

INFOWATCH

InfoWatch Traffic Monitor

Administration Guide

08/24/2026

© JSC “InfoWatch”

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

http://www.infowatch.com

TABLE OF CONTENTS

1 Introduction 7
1.1 Who Should Read this Guide 7
1.2 Set of Documents 7
1.3 Technical Support 7
2 Traffic Monitor Overview 8
2.1 InfoWatch Traffic Monitor Features 8
2.1.1 In Stream/At The Gateway Traffic Interception 8
SMTP Traffic Interception Scheme 8
POP3 Traffic Interception Scheme 11
HTTP Traffic Interception Scheme 12
HTTPS Traffic Interception Scheme 15
ICQ Traffic Interception Scheme 17
NRPC Traffic Interception Scheme 18
IMAP4 Traffic Interception Scheme 19
2.1.2 Processing Traffic, Received from Third-party Systems 19
2.2 InfoWatch Traffic Monitor Subsystems (Red Hat Enterprise Linux) 20
2.3 Licensing 21
3 System Installation Types 26
4 Configuring System After Installation 27
4.1 Changing the Preset Password 27
4.2 Configuring protection against password guessing 29
4.3 Preliminary Settings 30
4.3.1 Configuring Time Synchronization 30
4.3.2 Configuring Sphinx for Distributed Installation 31
4.4 General Settings 31
4.4.1 Configuring Server to Work with SPAN, or Port Mirroring Technology 31
Configuring Traffic Monitor Server as Sniffer 32
Configuring Traffic Monitor Server to Receive Copy of Traffic from Sniffer 33
Creating Traffic Monitor Cluster 34
4.4.2 Intercepting Traffic, Transmitted via ICAP Protocol 35
Configuring ICAP 36
Recommendations on SQUID Configuration 37
Recommendations on configuring UserGate 42

Disabling ICAP ... 45
4.4.3 Configuring Licensing Server (in case of Cluster) ... 45
4.5 Configuring Traffic Interception ... 46
4.5.1 Configuring SMTP Traffic Interception ... 47
SPAN, or Port Mirroring ... 47
Receiving Copies from Mail Server ... 48
Inline Mode ... 48
Configuring Mail Servers for SMTP Traffic Interception ... 56
4.5.2 Configuring POP3 Traffic Interception ... 62
4.5.3 Configuring HTTP Traffic Interception ... 62
SPAN, or Port Mirroring ... 62
Inline Mode ... 63
4.5.4 Configuring HTTPS Traffic Interception ... 63
Inline Mode ... 63
4.5.5 Configuring ICQ Traffic Interception ... 64
SPAN, or Port Mirroring ... 64
4.5.6 Configuring NRPC Traffic Interception ... 64
SPAN, or Port Mirroring ... 64
4.5.7 Configuring IMAP4 Traffic Interception ... 64
4.5.8 Receiving Objects Intercepted by InfoWatch Device Monitor ... 65
4.6 Process autorun ... 65
4.6.1 Check of Process Autorun ... 65
4.6.2 Enabling and Disabling Process Autorun ... 68
4.7 Remote database interaction module ... 70
4.7.1 Configuring Data Collection in a Branch Network ... 70
4.7.2 Configuring the Client of the Remote Database Management Module ... 71
4.7.3 Configuring the Server of the Remote Database Management Module ... 72
4.8 Configuring OCR Extractors ... 72
4.8.1 Interception channels ... 73
4.8.2 Supported OCR extractors ... 74
Tesseract settings ... 75
Content AI ContentReader Engine settings ... 75
4.9 Configuring Notifications for Users and Employees ... 77
4.10 Limiting the number of events that can be found ... 78
4.11 Service-to-service cooperation setup (Consul service) ... 78
4.11.1 Starting and stopping the service ... 78
4.11.2 Registering services in Consul ... 79
4.11.3 Distributed installation ... 80
4.11.4 Network rules configuration to access Consul ... 82
4.11.5 consul.json configuration file and iwtm-consul.service unit file ... 83
4.12 Secure Deployment Recommendations ... 85

4.12.1 Components ports ... 86
4.13 Configuring Verdict Management ... 91
5 Settings for automatic deletion of Data Discovery events ... 93
6 Monitoring ... 94
6.1 Monitoring Subsystem for Distributed Architecture ... 94
6.1.1 Configuring Connection to Device Monitor ... 94
6.1.2 Configuring Indicators Manually ... 95
6.1.3 Configuring Addresses of Time Synchronization Server for Monitoring Subsystem ... 95
6.1.4 Configuring Notifications ... 95
7 Using a database unloading for automatic recipient validataion ... 97
8 Database Administration ... 99
8.1 Oracle ... 99
8.1.1 Tablespaces in InfoWatch Traffic Monitor database ... 99
General information ... 99
Storing ... 101
Archiving ... 102
Deleting ... 102
8.1.2 Managing Daily Tablespaces ... 102
Configuring Location of Files within File System ... 102
Configuring Storage Modes for Tablespace Files ... 104
Archiving Daily Tablespaces ... 106
Restoring Daily Tablespaces ... 110
Deleting Daily Tablespaces ... 111
Managing Daily Tablespaces with the Console Utility ... 114
8.1.3 Load statistics of Daily Tablespaces ... 116
Scenarios of script execution ... 117
8.1.4 Database Backup ... 121
Creating Database Backup ... 121
Restoring the Database from the Backup ... 129
8.1.5 Database Routinely Maintenance ... 133
8.1.6 Database Logging ... 134
Rotation of database logs ... 134
8.2 PostgreSQL ... 135
8.2.1 Tablespaces in InfoWatch Traffic Monitor database ... 136
General information ... 136
Storing ... 137
Archiving ... 138
Deleting ... 138

8.2.2 Managing Daily Tablespaces ... 138
Configuring Location of Files in File System ... 138
Configuring Storage Modes for Tablespace Files ... 140
Archiving Daily Tablespaces ... 143
Restoring Daily Tablespaces ... 147
Deleting Daily Tablespaces ... 148
Managing Daily Tablespaces with the Console Utility ... 151
8.2.3 Load statistics of Daily Tablespaces ... 152
Scenarios of script execution ... 154
8.2.4 Database Backup ... 157
Creating Database Backup ... 158
Restoring Database from Backup ... 164
8.2.5 Database Server Routinely Maintenance ... 167
8.2.6 Database logging ... 168
Rotation of database logs ... 169

9 Administrating the Server End of InfoWatch Traffic Monitor ... 170

9.1 Traffic Monitor Server Processes ... 170
9.1.1 List of Traffic Monitor Server End Processes ... 170
9.1.2 Setting Traffic Monitor Server End Configuration Files ... 176
9.1.3 Using Traffic Monitor Server End Processes ... 176
9.1.4 SSL Thrift Encryption ... 178
Preparing a key and certificates ... 179
Editing configuration files ... 181
9.2 Configuring OCR ... 182
9.2.1 Enabling OCR technology when implementing the System ... 183
9.2.2 Configuring OCR on several nodes ... 183
9.2.3 Configuration File ocr_custom.xml ... 183
9.3 Configuring Settings for Processing Enclosed Archives ... 185
9.3.1 The extractors.xml Configuration File ... 185
9.3.2 The extractors_customization.xml Configuration File ... 189
9.4 Configuring Settings of Search Using Wildcards ... 191
9.5 Configuring Integration with Data Analysis Service ... 192
9.6 Configuring Connection with Data Storage ... 195
9.7 Configuring Sending Events to Platform ... 197
9.7.1 Switching the way of sending events ... 197
9.7.2 Configuring real-time pushing ... 199
9.7.3 Configuring scheduled events sending ... 199
9.8 Logging System Work ... 199
9.9 File Queues ... 201

9.10 Recovering the System after Failures 203
9.11 Managing Languages Including Morphological Support 204
9.11.1 Adding New Language for Events Search. Morphology and Adding Terms. 204
9.11.2 Updating Installed Language Including Morphological Support 206
9.11.3 Deleting Search Language and Terms 206
9.12 Configuring Forwarding Data to SIEM 206
9.12.1 Configuring SIEM Side 207
Table Representation of TM Events 207
User Audit Table View 213
9.12.2 Configuring TM Side 218
Managing Siem User 218
Forwarding Logs to SIEM 220
Log Management for TM DB User Sessions 220
9.12.3 Type of Logs, Transmitted to SIEM 221
9.13 Deleting Temporary Files 221
10 Working in Traffic Monitor via Administration Centre Web Interface (Platform) 223
11 Configuring Single Sign-On in InfoWatch products 225
12 Interaction with external systems 227
13 Appendix A. Username and Password Creation Recommendations 228
14 Appendix B. Monitoring Indicators 230

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.

In addition to the primary System User Guide and Administration Guide, a Knowledge Base is available at lk.infowatch.ru, which includes troubleshooting materials and answers to questions. If you do not have access to the Knowledge Base, please contact the technical support service of InfoWatch at support@infowatch.com.

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.

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

2 Traffic Monitor Overview

In this chapter:

- InfoWatch Traffic Monitor Features;
- InfoWatch Traffic Monitor Subsystems (Red Hat Enterprise Linux);
- Licensing.

2.1 InfoWatch Traffic Monitor Features

InfoWatch Traffic Monitor allows you to control corporate network information flows 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);
- Traffic intercepted by Device Monitor agents on workstations (see in *InfoWatch Device Monitor. User Guide*);
- 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.

SMTP Traffic Interception Scheme

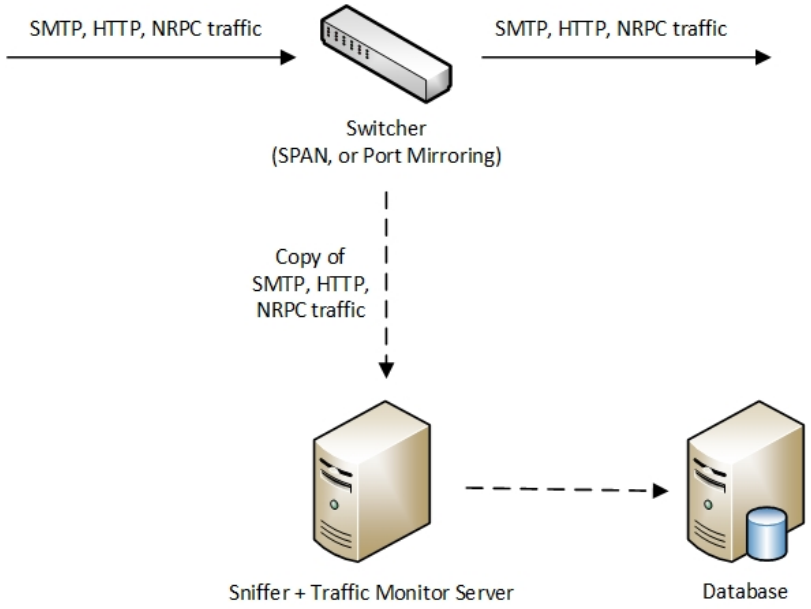
Method 1:

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:

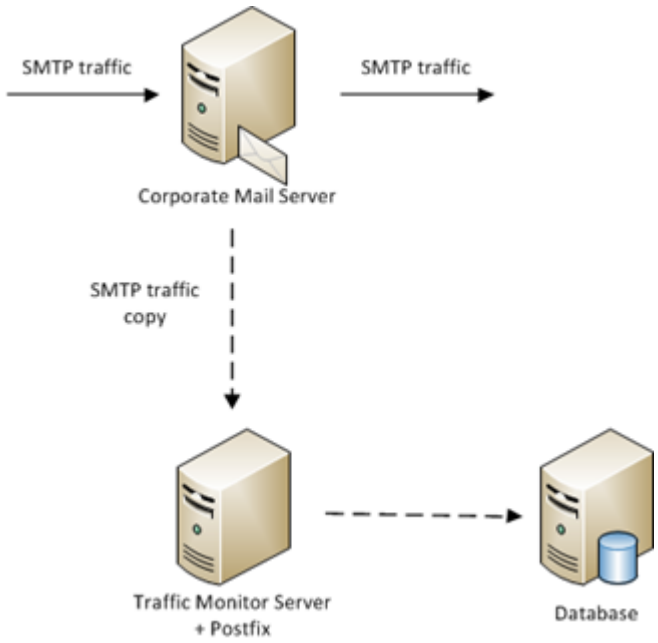
- This method allows to analyze traffic safely even in the isolated network segment. System can never influence analyzed traffic, regardless of Server state.
- SMTP traffic of external servers is being analyzed as well

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 Traffic Monitor 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 *Receiving Copies from Mail Server*.

Advantages:

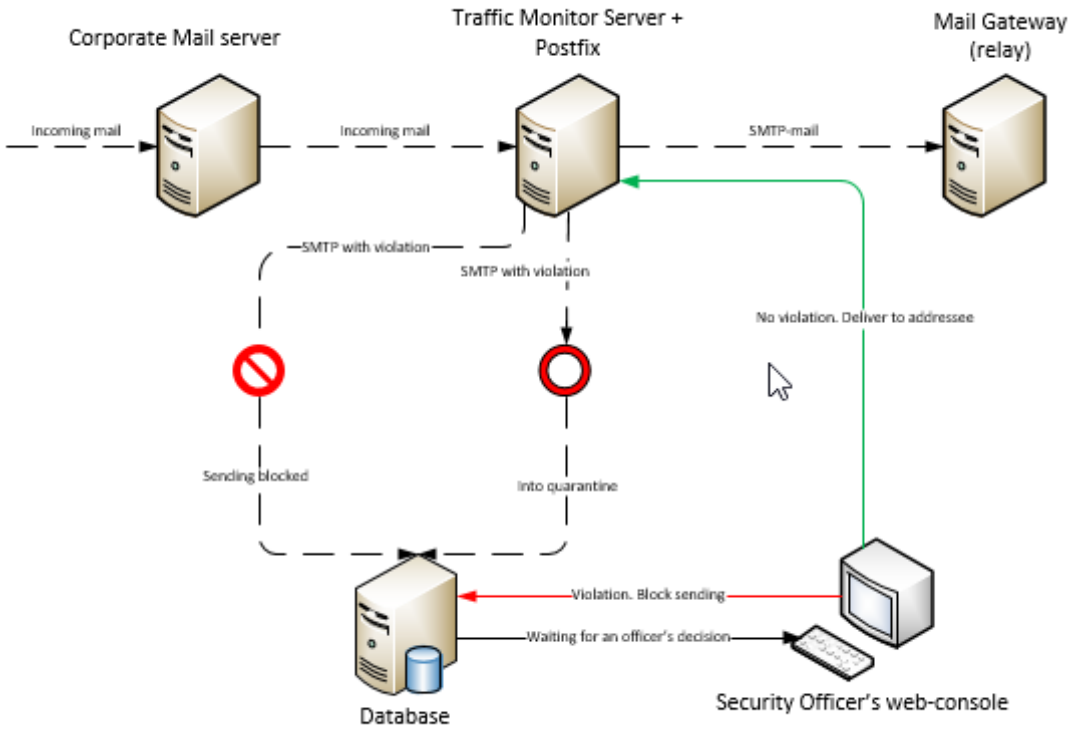
- Apart from external, it allows analyzing company's internal communications;
- When MS Exchange 2007 or newer is used there is functionality to analyze communications of a certain user group;
- Guarantees entire mail analysis.

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:

Traffic Monitor server uses configured Postfix mail server and functions as an SMTP retranslator.



For more information on the 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 Traffic Monitor server inaccessibility, users cannot send mail, in case server reservation has not been provided (for example, through MX-records).

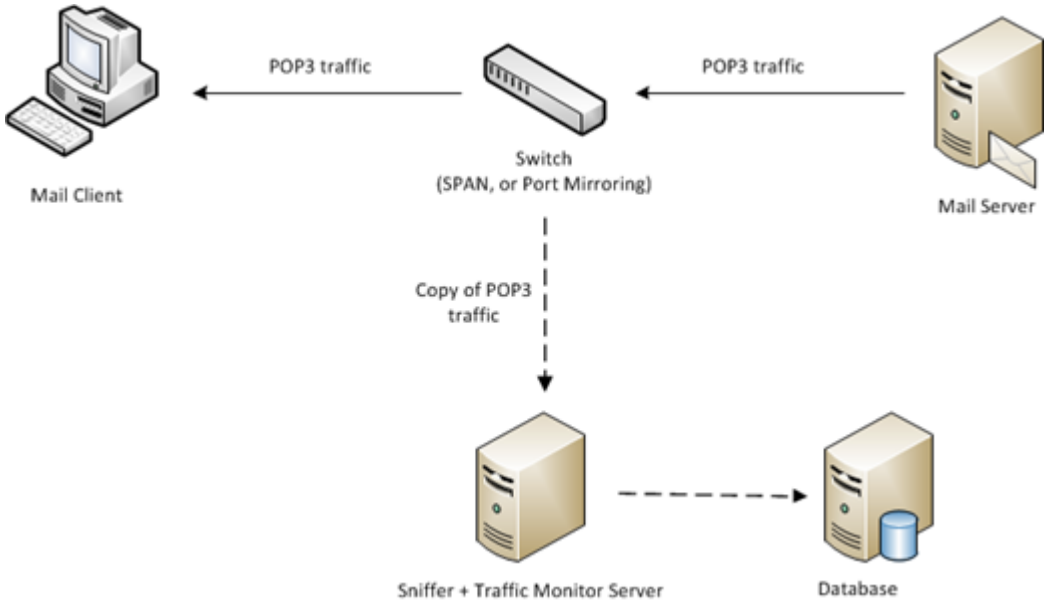
POP3 Traffic Interception Scheme

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

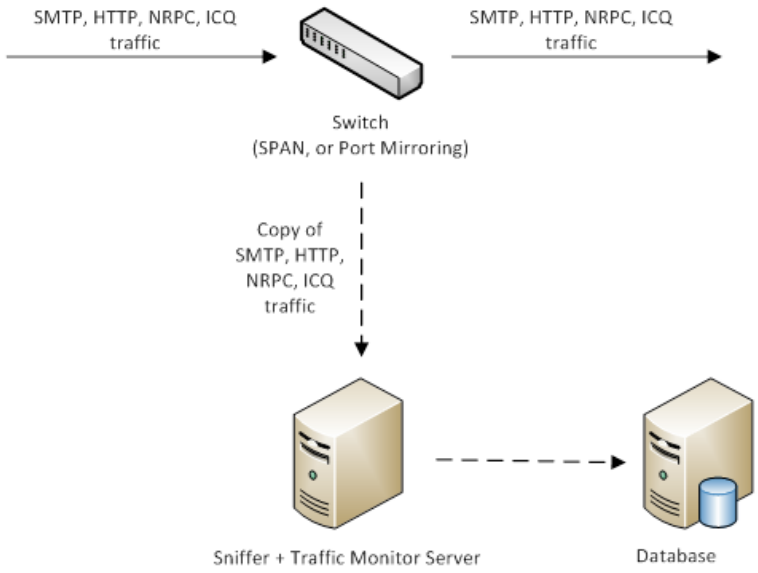
Method 1:

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, or 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 Traffic Monitor server.

Special case 1:

In case Traffic Monitor server is located in virtual environment, in addition to switch port setup, to analyze 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:

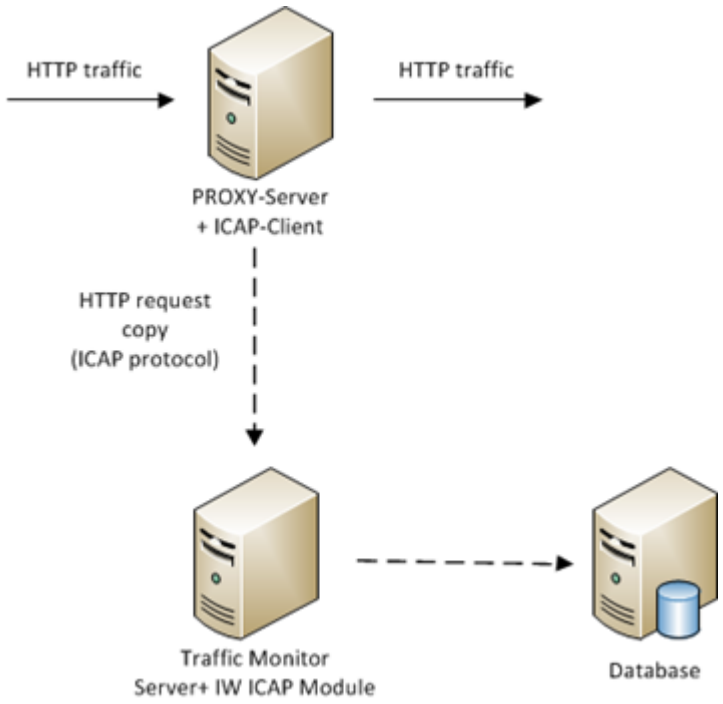
Traffic copy, which is transmitted via ICAP protocol, is intercepted from corporative proxy server.

Traffic Monitor Server is positioned as an ICAP server. 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.

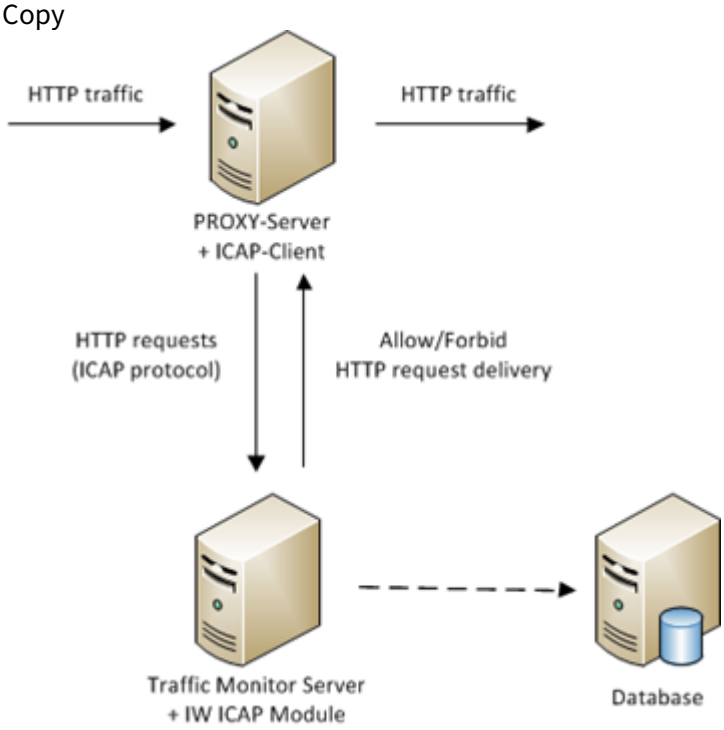
The following proxy servers support this option:

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

> **Note:**
>
> To work with other proxy servers maintaining ICAP is possible, but this requires 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:

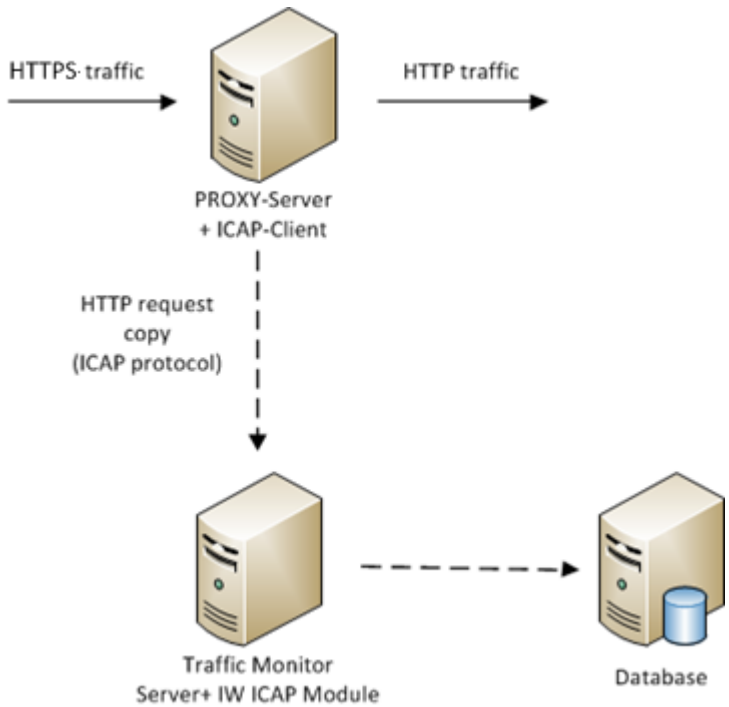
Corporate proxy-server carries out certificate replacement and HTTPS traffic parsing. After parsing HTTPS traffic, the proxy server sends traffic as HTTP to Traffic Monitor Server via ICAP protocol.

The following proxy servers support this option:

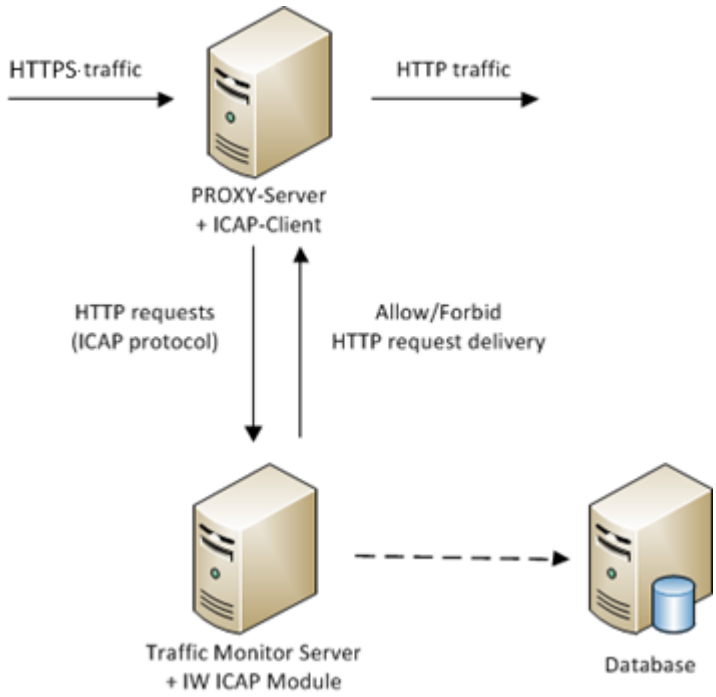
- SQUID (given that the package has been compiled including ICAP support)
- Zimbra Proxy (as a part of Zimbra ZCS)

> **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 *Inline Mode*.

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:

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 Traffic 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.

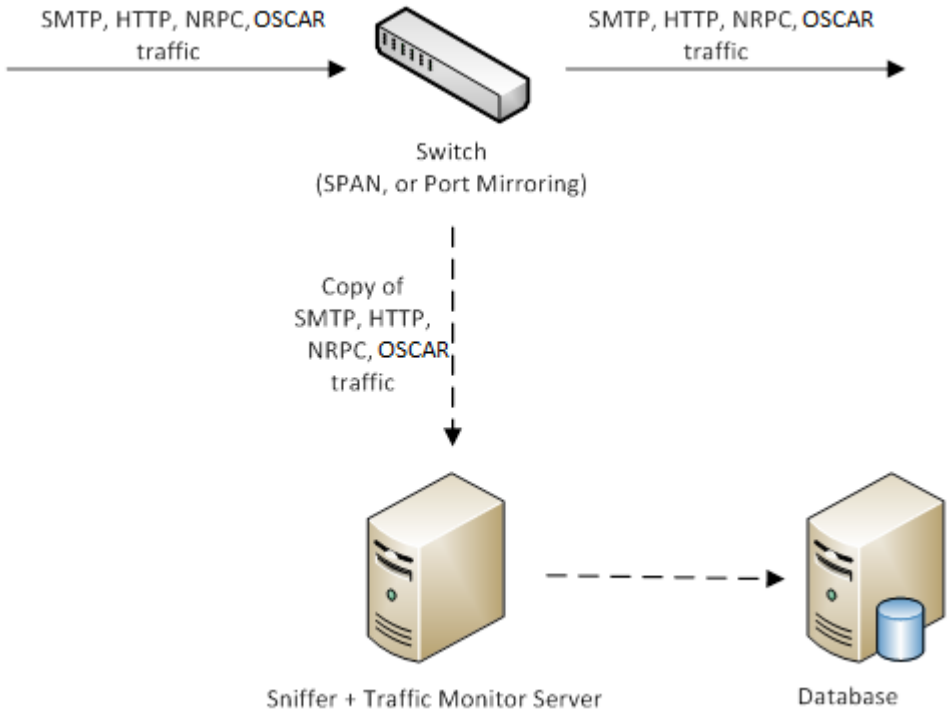
> **Note:**
>
> Direct file transfer is not supported. OSCAR protocol assumes that Traffic Monitor gets the file hosting service reference, from which the file can be loaded.

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 Traffic Monitor server.

NRPC Traffic Interception Scheme

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

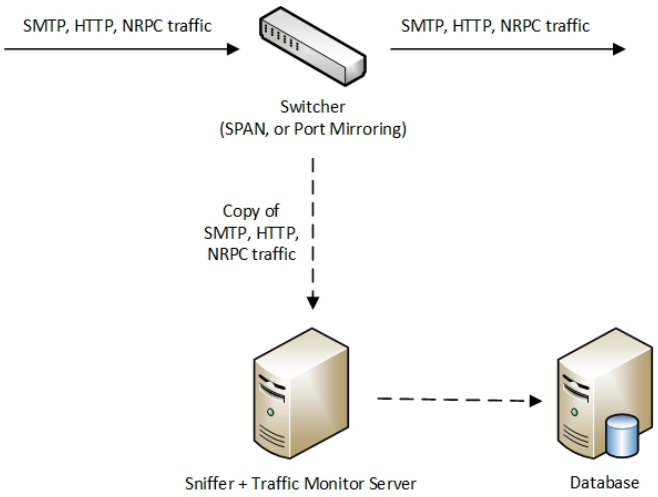
Method 1:

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 Traffic Monitor server.

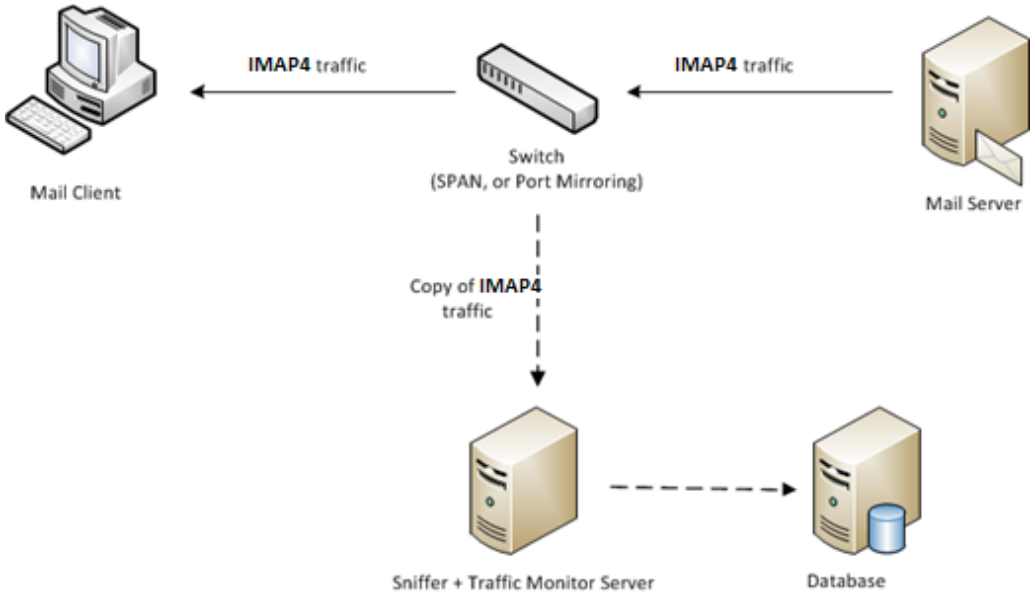
IMAP4 Traffic Interception Scheme

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 *Configuring Server to Work with SPAN, or Port Mirroring Technology*.

2.1.2 Processing Traffic, Received from Third-party Systems

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

- **InfoWatch Lotus Domino Adapter**. Find the recommendations for installation and administration in the document *InfoWatch Lotus Adapter. Installation and Configuration Guide*;
- **InfoWatch MS Lync Adapter**. Find the recommendations for installation and administration in the document *InfoWatch MS Lync Adapter. Installation and Configuration Guide*;
- **InfoWatch TMG Adapter**. Find the recommendations for installation and administration in the document *InfoWatch TMG Adapter. Installation and Configuration Guide*;
- **InfoWatch Device Control Adapter**. Find the recommendations for installation and administration in the document *InfoWatch Device Control Adapter. Installation and Configuration Guide*;
- **InfoWatch Cisco UCM Adapter**. Find the recommendations for installation and administration in the document *InfoWatch Cisco UCM Adapter. Installation and Configuration Guide*;
- **InfoWatch Smart Logger II**. Find the recommendations for installation and administration in the document *InfoWatch Smart Logger II. Installation and Configuration Guide*;
- **InfoWatch HEML Adapter**. Find the recommendations for installation and administration in the document *InfoWatch HEML Adapter. A Guide for Installation, Configuration, and Running the Program*;

- **InfoWatch Sample Documents Autoupdate Adapter**. Find the recommendations for installation and administration in the document *InfoWatch Sample Documents Autoupdate Adapter. Setup and Configuration 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. Consisting of the following modules: • Sniffer module • ICAP module • Device Monitor module • Mail (SMTP) interception 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; • Vector images; • Blanks; • Stamps; • DB unloadings; • Graphical objects; • Autolinguist.
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, Samba DC and Domino Directory Integration module • Decision-Making module

InfoWatch Traffic Monitor subsystem	Purpose
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 internal one.
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

After the System has been installed, the license should be installed accordingly. For this purpose, request for license key file (see the document *InfoWatch Traffic Monitor. User Guide. Requesting License*).

The license is intended to specify the duration, number of users, number of interception modules and analysis modules, as well as the ability to integrate with external systems.

A commercial license key is a file in LIC format.

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

- If the license expires, interceptors stop working. To resume the System operation, the new license should be installed.
- 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!

About license validity check and license management, you may find in the document *InfoWatch Traffic Monitor. User Guide. Managing Licenses*.

Modules used in the product are listed below.

Interception modules designed by InfoWatch		
Subsystem	Event type	Protocol
TM	E-Email	POP3 IMAP SMTP NRPC
	Web message	HTTP HTTPS
	Web email	HTTP HTTPS
	ICQ	OSCAR
	Data Discovery	-
DM	Email	POP3 IMAP Outlook SMTP
	Web message	HTTP HTTPS
	Web email	HTTP HTTPS
	Print	-
	Skype	SKYPE

Interception modules designed by InfoWatch		
Subsystem	Event type	Protocol
	XMPP	XMPP
	Mail.Ru Agent	MMP
	FTP	FTP
	Clipboard	-
	Screenshots	-
	Removable devices	-
	Network resources	-
	Terminal session	-
	Cloud storage	HTTPS
	Telegram	-
	Keyboard input	-
	VK (VKontakte)	HTTPS
	Facebook	HTTPS
	WhatsApp	-
Adapters	MS Lync	SIP
	Email (Lotus)	NRPC
	Web message (ICAP)	ICAP
	Web email (ICAP)	ICAP

External interception modules	
Event type	Protocol
Email	POP3 MAPI SMTP/ESMTP IMAP NRPC
Web email	HTTP HTTPS ICAP
ICQ	OSCAR
Mail.ru agent	MMP
Skype	Skype
XMPP	XMPP
MS Lync	SIP
Web message	HTTP HTTPS ICAP
FTP	FTP
Removable devices	-
Print	-
SmartLogger	XMPP

Analysis modules:

1. Linguistic analysis
2. Sample documents detector
3. Vector images detector
4. Text objects detector
5. DB unloadings detector
6. Form detector
7. Graphical analysis
8. Stamps detector
9. Autolinguist

Additional possibilities:

1. Modules of sample unloadings update;
2. Export to external analysis systems.

> **Note:**
>
> The technology of blocking leakage channels on workstations based on analysis results is not licensed.

3 System Installation Types

The deployment scheme is chosen based on estimated hardware workload and implementation goals (for details, see the document *InfoWatch Traffic Monitor. Installation Guide. System Deployment Schemes and Installation Types*). The following installation modes are supported:

- *All-in-one Standard* - the base type of installation, when all System components are installed on the same computer together with PostgreSQL DBMS. For details, see the document *InfoWatch Traffic Monitor. Installation Guide. All-in-one Installation Mode of TM Enterprise and TM Standard*;
- *All-in-one Enterprise* - System installation type with advanced features including PostgreSQL and Oracle DBMS, scalability, fine control of workstations. For details, see the document *InfoWatch Traffic Monitor. Installation Guide. All-in-one Installation Mode of TM Enterprise and TM Standard*;
- *Distributed Installation of TM Enterprise (Traffic Monitor Server + Database)* - System installation type for operation under heavy workload and with a large amount of data. For details, see the document *InfoWatch Traffic Monitor. Installation Guide. Distributed Installation of TM Enterprise*.

Important!

If the System is installed on different servers (and when building a server cluster), pay attention to the following:

- you should configure network parameters of Sphinx searching engine (see *Configuring Sphinx for Distributed Installation*)
- some server processes (**iw_adlibitum, iw_bookworm, iw_deliver, iw_licensed, iw_indexer, iw_is, iw_image_autoling, iw_text_autoling**) and user console processes (**iw_kicker, iw_configerator**) should be run on the cluster in a single copy (see *List of Traffic Monitor Server End Processes*)

Depending on the purchased license, each installation type may include installation of the following interceptors:

- InfoWatch Device Monitor which is intended to configure security schemes, computer monitoring system, access to the company computers, etc. (see the document *InfoWatch Device Monitor. Installation, Configuration and Administration Guide*).
- Adapters - interception modules intended for integration with third-party systems.

4 Configuring System After Installation

After installing the System, configure the following settings for proper System operation:

- Configuring Time Synchronization - enables automatic time synchronization on servers;
- Configuring Sphinx for Distributed Installation - settings required for 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 description when and how to enable/disable autorun for these processes;
- Configuring OCR Extractors - the order of installing packages required for text recognition in intercepted events;
- Configuring 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 events that can be found - changing the 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 (for details, see the document *InfoWatch Device Monitor. Installation, Configuration and Administration Guide*);
- Configuring Data Collection in a Branch Network - the settings of configuration files services, responsible for collecting data in a branch network;
- Service-to-service cooperation setup (Consul service) - the settings of configuration files services, managing The System processes;
- Detecting Workstations to Install the Agents on - scanning the network in order to detect workstations outside Active Directory (for details, see the document *InfoWatch Device Monitor. User Guide*).

We recommend:

- changing passwords pre-configured in the System, as information security rules require (for details, see *Changing the Preset Password*);
- configuring protection against guessing passwords during authorization in Traffic Monitor and Device Monitor consoles (for details, see *Configuring protection against password guessing*);
- configuring a firewall to prevent unauthorized access to the System components (for details, see *Secure Deployment Recommendations*).

4.1 Changing the Preset Password

For accounts in the System, a standard password is preset – xxXX1234 (for more details, see the article *InfoWatch Traffic Monitor. Installation Guide. Pre-installed Server Parameters*). During the operation of the System, it must be replaced, following information security requirements. Stable and secure operation of the System requires storing passwords in a secure place, inaccessible to others. The standard password is changed in the System configuration files. To replace the preset password with a new one:

Stop process Traffic Monitor:

1. Stop process Traffic Monitor:

```
iwtm stop
```

2. Run command:

```
egrep -lir --include=\*.{cfg,conf,pgpass} --exclude-dir=\*{etc_conf_backup,config_merge}\*
'xxXX1234' /  | xargs -l sed -i -e 's/xxXX1234/<new_pass>/g'
```

where `<new_pass>` is the new password.

3. Make sure the new password is set in all configuration files:

```
egrep -lir --include=.{cfg,conf,pgpass} --exclude-dir={etc_conf_backup,config_merge}*
'<new_pass>' /
```

4. Change the password to connect to the database. For this:

For PostgreSQL:

a. Connect to PostgreSQL DBMS:

```
psql postgres iwtm
```

b. Get a list of users:

```
\du
```

c. Change all users passwords, including the user `postgres`:

```
alter user <iw_user> with password '<new_pass>';
```

where `<iw_user>` is the selected database user, `<new_pass>` is the new password for this user.

d. Disconnect from the PostgreSQL DBMS:

```
\q
```

For Oracle:

a. Connect to the Oracle DBMS:

```
sqlplus iwtm@iwtm
```

b. Enter the preset password.

c. Get a list of users:

```
select * from dba_users
```

d. Change user passwords:

```
ALTER USER user IDENTIFIED BY new_pass
```

where `user` is the selected database user, `new_pass` is the new password for this user.

e. Disconnect from the Oracle DBMS:

```
exit
```

5. Start process Traffic Monitor:

```
iwtm start
```

Requirements for passwords

The password may include the following symbols:

- Capital Latin characters (A-Z);
- Lowercase Latin characters (a-z);
- Arabic numerals (0-9);
- Special symbols: "@", "%", ":", "^", "-", "_", "+", "/", ".", ",".

4.2 Configuring protection against password guessing

To protect the System, the following feature is enabled: in the case of repeated unsuccessful authorization attempts, user login is blocked. Protection against password guessing is configured in the database.

By default, the protection is disabled.

Protection for InfoWatch Traffic Monitor and InfoWatch Device Monitor is configured separately.

To enable protection for Traffic Monitor server:

1. Connect directly to the database which is used by the Traffic Monitor server.
2. Find the table `SETTING`.
3. Find 3 parameters responsible for protection configuration:
   - **`web_logon_attempts_count`** - the number of unsuccessful login attempts allowed;
   - **`web_logon_blocking_period`** - the time for which the login will be blocked, in seconds;
   - **`web_logon_attempts_period`** - the period of unsuccessful login attempts, in seconds.
4. Set the values for all three parameters in accordance with security requirements.

> **Warning!**
>
> In case any parameter's value is incorrect or equal to 0, the protection is to be disabled.

5. To apply the settings, save changes in the database. You need no restart the server as protection settings change dynamically.

If login is blocked, a new event is created in the audit log (the **Log** button in the Navigation pane) where the unlocking time is specified.

When the blocked user tries to log into the System again, he/she will be notified that the number of failed login attempts has been exceeded.

An example of protection settings for Traffic Monitor:

- `web_logon_attempts_count - 5`
- `web_logon_blocking_period - 300`
- `web_logon_attempts_period - 120`

How these settings work: if during 2 minutes (120 seconds), the user makes 5 unsuccessful login attempts, then login for this user is blocked for 5 minutes (300 seconds). The countdown period of unsuccessful attempts starts from the first attempt. If during 120 seconds the user makes only 4 unsuccessful login attempts, then the next attempt will relate to a new period.

4.3 Preliminary Settings

Upon System installation the following settings must be performed:

- Configuring Time Synchronization;
- Configuring Sphinx for Distributed Installation.

4.3.1 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 `chronyd` service:
   `systemctl stop chronyd`
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 NTP, use `chronyd -q 'server <IP> iburst'` command (where IP is the address of server to be checked), for example:
   ```
   chronyd -q 'server 10.10.0.98 iburst'
   2024-09-11T10:30:17Z chronyd version 4.3 starting (+CMDMON +NTP +REFCLOCK
   +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH +IPV6 -DEBUG)
   2024-09-11T10:30:17Z Initial frequency -19.107 ppm
   2024-09-11T10:30:22Z System clock wrong by 8551737.490761 seconds (step)
   2024-12-19T09:59:19Z chronyd exiting
   ```
6. Configure the synchronization specifying NTP synchronization server in **/etc/chrony.conf** file. Add entry (specify IP address of your NTP server):
   `server 10.10.0.98 iburst`
7. Run `chrony` service:
   `systemctl start chronyd`
8. Check the current state of `chrony` service with the command:
   `systemctl status chronyd`
9. Enable automatic time synchronization:
   `chronyc -N sources`

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================
^* 10.10.0.98                    4   6    37    19    -14us[ -102us] +/-   39ms
```

4.3.2 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** when using Indexer template. For information on installation, see the document *InfoWatch Traffic Monitor. Installation Guide. System Deployment Schemes and Installation Types*).

A distributed installation is an installation scheme when Traffic Monitor components are installed on different servers.

> **Note:**
>
> If you use several servers, specify the server IP address where **sphinx** service is running (a server with Indexer template). IP address is specified in `hostname` parameter within `search` section of **web.conf** configuration file on the server with Web console template used.

4.4 General Settings

The chapter contains information on configuring the System and its components:

- Configuring Server to Work with SPAN, or Port Mirroring Technology;
- Intercepting Traffic, Transmitted via ICAP Protocol;
- Configuring Licensing Server (in case of Cluster).

4.4.1 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 1).
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 (**Interceptors** template key):
    a. Configure Server to work as Sniffer (see *Configuring Traffic Monitor Server as Sniffer*, variant 2).
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 (**Database** and **Indexer** templates key).
2. On the computer, where Sniffer will be running (**Interceptors** template key):
    a. Configure it to work as Sniffer (see *Configuring Traffic Monitor Server as Sniffer*, variant 2).
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 the connection alive (in seconds) if no packages are transmitted. The recommended value – `600`.
`LiveInSec` (subsection `Timeouts`)	Timeout (in seconds) when the status of the connection must change to *ESTABLISHED*. If the status is not changed, the 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 the 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:

```
iwtm stop
```

2. Configure process autostart:
    - Variant 1. Traffic copy interception and analysis are performed on the same computer. Traffic Monitor Server will receive traffic copy from a switch (Sniffer function), analyze received data and upload it to the database (Traffic Monitor Server function). Enable **iw_sniffer** process autostart:

```
iwtm enable iw_sniffer
```

- Variant 2: Traffic copy interception and analysis are performed on different computers. Configured Traffic Monitor Server example will act only as Sniffer (traffic interception).
  a. Enable **iw_sniffer** process autostart:

  ```
  iwtm enable iw_sniffer
  ```

  b. Disable other processes autostart.

  > **Note:**
  >
  > For more information on enabling and disabling autostart, see *Enabling and Disabling Process Autorun*.

3. In **/opt/iw/tm5/etc/sniffer.conf** file, section `iscp`, configure traffic interception parameters:
   - `ListenHost –` IP-address on which the **iw_proxy** process receives incoming connections from **iw_sniffer**;
   - `ListenPort –` Port via which the **iw_proxy** process receives incoming connections from **iw_sniffer** (4301 by default).
4. Start Traffic Monitor processes:

   ```
   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 and configure the following settings:

1. Enable autostart for required traffic interceptors (setup for SMTP, HTTP(S), ICQ traffic:

   ```
   iwtm enable iw_proxy_http iw_proxy_smtp iw_proxy_icq
   ```

   For NRPC traffic interceptor autostart configuration description, see *SPAN, or 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 is being 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, which are used to call the **iw_sniffer** process.

> **Note:**
>
> To configure interaction with the computer used to run the **iw_sniffer** process, 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 on each TM server instance that will be included in the cluster:

1. In the **sniffer.conf** configuration file, make sure that the `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 the values of `Host` and `Port,` on which the **iw_sniffer** process is running.
   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:

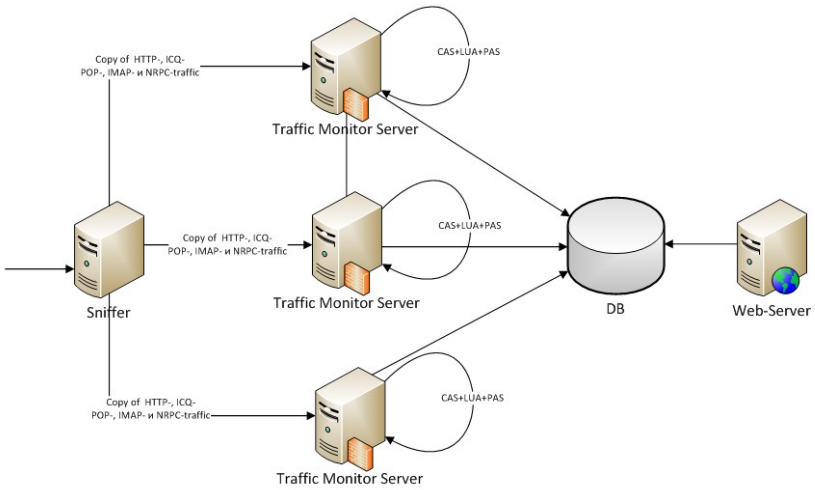
   ```
   "iscp": {
   "ListenArea": "icq",
   "Host": 10.20.30.40,
   "Port": 4301
   }
   ```

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. In this case, all Traffic Monitor Server instances are used one in a turn.
   - `IpPref` – the traffic is distributed between several instances of Traffic Monitor server with **iw_proxy** based on an IP address of the client. In this case, 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.



4.4.2 Intercepting Traffic, Transmitted via ICAP Protocol

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

In this scheme, automatically installed modules are used on the Traffic Monitor server:

- **iw_icap_buf**, which receives large data in parts, combines these parts and send data to **iw_icap** for analysis;
- **iw_icap**, which processes intercepted data received through a proxy server or data processed by **iw_icap_buf** module.

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

Warning!

Traffic Monitor Server and proxy with ICAP client must be located in the same subnetwork.

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

Important!

The **iw_icap_buf** supports buffering of file uploads to file exchangers: filetrance.tander.ru, Yandex.Disk (disk.yandex.ru), Mail.ru Cloud (cloud.mail.ru), Google Drive (drive.google.com), BOX (box.com), DropBox (www.dropbox.com), OneDrive (onedrive.live.com). When uploading files to another file storage, buffering is not supported.

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

- **Copy** mode – a 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 the Traffic Monitor system. Depending on the fact if there is a 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;
- Recommendations on SQUID Configuration;
- Disabling ICAP.

Configuring ICAP

The IW ICAP module is automatically installed with Traffic Monitor server (**All-in-one** installation or **Interceptors** template options). Autostart of the **iw_icap** process on TM Server is enabled by default.

HTTP and HTTPS traffic is intercepted with the same System resources, but the configuration of external mechanisms configuration differs (see below).

To enable interception of HTTP(S) traffic transferred via ICAP, you need to configure parameters of intercepting HTTP and HTTPS requests on a proxy server.

Warning

On each workstation, configure the browser so that HTTP(S) traffic should pass through the SQUID proxy server. For more information on how to configure this, see the documentation for your browser.

The following ICAP configuration options are possible:

1. For the traffic to be transmitted in "Copy" mode:
   a. In the **luaengined.conf** configuration file, which is located in the `/opt/iw/tm5/etc` directory, in the `Icap` property of the `TransportModes` section, specify a valid FQDN name of the TM server (for example, `tm-server1.local`). The value of the mode should be:

`Copy`. You can specify multiple pairs of values:
`"Icap": [{"Server": "tm-server1.local", "Mode": "Copy"}, {"Server":"tm-server2.local", "Mode": "Copy"}]`

b. Save changes in the **luaengined.conf** file.

2. For the traffic to be transmitted irrespective of the verdict:
   a. In the code specified above, set the mode value to `Transparent`.
   b. Save changes in the **luaengined.conf** file.
3. For the traffic to be transmitted in the "Block" mode:
   a. In the code specified above, set the move value to `Normal`.
   b. Save changes in the **luaengined.conf** file.
4. In the **icap.conf** configuration file, which is located in the `/opt/iw/tm5/etc` directory, set the value for `AsyncCheck` parameter of the `Icap` section as follows:
   - `true` – the "Copy" mode
   - `false` – the "Block" mode
5. Save the configuration file.
6. Restart the Traffic Monitor server:
   `iwtm restart`

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

> **Note:**
>
> This setting depends on the modification of the proxy server. You can find actual information in the documentation for your proxy server.
>
> See *Recommendations on SQUID Configuration*.

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 RPM package or an archive (that should be then unpacked) from a repository or from CD/DVD. In our example we use the `squid-3.4.0.2-2.el6.x86_64.rpm` RPM package.

To install an RPM 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, do the following:

1. To 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
```

2. To configure working on ICAP **UserGate Web Filter** server, in the `squid.conf` configuration file, add the following:

```
icap_enable on
icap_preview_enable on
icap_preview_size 4096
icap_send_client_ip on
icap_service service_req reqmod_precache bypass=0 icap://10.0.3.10:1344/request
adaptation_access service_req allow all
icap_service service_resp respmod_precache bypass=0 icap://10.0.3.10:1344/response
adaptation_access service_resp allow all http_port 8080 transparent
```

   where `10.0.3.10` is the **UserGate Web Filter** server address.

   Important!

   UserGate Web Filter server does not support `icap_preview_enable off` mode. Working with HTTPS traffic is not supported at the moment.

3. Restart Squid:

```
sudo service squid3 restart
```

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.

To configure SSL-Bump mode, perform the following actions:

1. Disable the SELinux access control system. For this:

a. Run the command:
`sudo sed -i 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config`
b. Restart the server using the command:
`reboot`
c. Check status of the SELinux system using the command:
`sestatus`
As a result, you will see the message:
`SELinux status: disabled`

2. Create a catalogue to store SQUID certificates:
`mkdir /etc/squid/ssl_cert`
3. Generate a root certificate for browsers of workstations whose traffic will be intercepted:
`openssl req -new -newkey rsa:2048 -days <number of days> -nodes -x509 -keyout /etc/squid/ssl_cert/IW.key -out /etc/squid/ssl_cert/IW.crt`
`openssl x509 -in /etc/squid/ssl_cert/IW.crt -outform DER -out /etc/squid/ssl_cert/IW.der`
4. Copy the file with extention **.der** to the workstations and install it as a trusted certificate to computer storage.
5. Configure browsers of the workstations to use new proxy server SQUID.
6. Generate a parameter file for the Diffie-Hellman algorithm:
`openssl dhparam -outform PEM -out /etc/squid/ssl_cert/IW_dhparam.pem 2048`
7. Make the **squid** user an owner of the `/etc/squid/ssl_cert` directory and, to ensure security, change file permissions:
`chown -R squid:squid /etc/squid/ssl_cert && chmod 400 /etc/squid/ssl_cert/IW*`
8. Identify the SQUID version used on your server. For this, run the command:
`squid -v`
Information about used version will be displayed in the following format:
`Squid Cache: Version <version>`
9. Stop SQUID:
`systemctl stop squid`
10. If you use SQUID proxy server version 3, perform the following actions:
a. Create a database for substitute certificates and make the **squid** user its owner:
`mkdir -p /var/lib/squid`
`rm -rf /var/lib/squid/ssl_db`
`/usr/lib64/squid/ssl_crtd -c -s /var/lib/squid/ssl_db`
`chown -R squid:squid /var/lib/squid`
b. In the `/etc/squid/squid.conf` configuration file, comment out the `http_port` setting and add the following certificate generation parameters:
`#http_port 3128`
`http_port 3128 tcpkeepalive=60,30,3 ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=20MB cert=/etc/squid/ssl_cert/IW.crt key=/etc/squid/ssl_cert/IW.key cipher=HIGH:MEDIUM:!LOW:!RC4:!SEED:!IDEA:!3DES:!MD5:!EXP:!PSK:!DSS options=NO_TLSv1,NO_SSLv3,NO_SSLv2,SINGLE_DH_USE,SINGLE_ECDH_USE tls-dh=prime256v1:/etc/squid/ssl_cert/IW_dhparam.pem`
`sslproxy_flags DONT_VERIFY_PEER`
`sslproxy_cert_error allow all`
`always_direct allow all`
`ssl_bump client-first all`
`ssl_bump server-first all`
`ssl_bump none all`

`sslcrtd_program /usr/lib64/squid/ssl_crtd -s /var/lib/squid/ssl_db -M 20MB`

11. If you use SQUID proxy server version 4 or later, perform the following actions:
    a. Create a database for substitute certificates and make the **squid** user its owner:
    ```
    mkdir -p /var/lib/squid
    rm -rf /var/lib/squid/ssl_db
    /usr/lib64/squid/security_file_certgen -c -s /var/lib/squid/ssl_db -M 20MB
    chown -R squid:squid /var/lib/squid
    ```
    b. In the `/etc/squid/squid.conf` configuration file:
        i. Add the following lines before the first `http_access` rule:
        ```
        acl intermediate_fetching transaction_initiator certificate-fetching
        http_access allow intermediate_fetching
        ```
        ii. Comment out the `http_port` setting and add the following certificate generation parameters:
        ```
        #http_port 3128
        http_port 3128 tcpkeepalive=60,30,3 ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=20MB tls-cert=/etc/squid/ssl_cert/IW.crt tls-key=/etc/squid/ssl_cert/IW.key cipher=HIGH:MEDIUM:!LOW:!RC4:!SEED:!IDEA:!3DES:!MD5:!EXP:!PSK:!DSS options=NO_TLSv1,NO_SSLv3,SINGLE_DH_USE,SINGLE_ECDH_USE tls-dh=prime256v1:/etc/squid/ssl_cert/IW_dhparam.pem
        sslproxy_cert_error allow all
        ssl_bump stare all
        sslcrtd_program /usr/lib64/squid/security_file_certgen -s /var/lib/squid/ssl_db -M 20MB
        sslcrtd_children 8
        ```
12. Start SQUID:
    ```
    systemctl start squid
    ```

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 operating system and SQUID version. For example, in Debian OS with SQUID version 3 installed, they are located in catalogue: `/usr/lib/squid3`, in Red Hat Enterprise Linux: `/usr/lib64/squid`. To see what authentication methods are supported by SQUID, third-party modules placement and other parameters, use command `squid -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 using `auth_param` parameter. Client will alternately attempt to use authentication schemes in the order they have been set in the `squid.conf` configuration file. Newly configured authentication scheme enters into force after SQUID service restart. To change existing schemes without service restart, use `squid -k reconfigure` command.

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]
```

To control internet access:

1. In the beginning of the `/etc/squid/squid.conf` configuration file, add the `auth_param` authentication setting according to the scheme:
   ```
   auth_param authentication_scheme scheme_parameters [parameters_value]
   ```
2. Create an access control list that will use the configured authentication module. In the configuration file, the access control list is designated as `acl` . In `selection_type` field, the access control list must have `proxy_auth` , `proxy_auth_regex` or `external` value using `%LOGIN` variable. For example:
   ```
   acl auth proxy_auth REQUIRED
   ```
3. Set access permission in `http_access` parameter for the specified access control list. For example:
   ```
   http_access allow auth
   ```

> **Note:**
>
> For the details about configuring user authentication, see documentation for SQUID proxy server.

Example of configuring Basic authentication:

On the server with installed SQUID, perform the following actions:

1. Add the following lines into the beginning of the `/etc/squid/squid.conf` configuration file:
   ```
   auth_param basic program /usr/lib64/squid/basic_ldap_auth -R -b "dc=<second-level domain name>,dc=<top-level domain name>" -D "<user name>@<Active Directory domain>" -w "<user password>" -f "sAMAccountName=%s" <IP address of the Active Directory domain controller>
   auth_param basic children 10
   auth_param basic realm Squid proxy-caching web server
   auth_param basic casesensitive off
   auth_param basic credentialsttl 1 minute
   acl auth proxy_auth REQUIRED
   http_access allow auth
   ```
2. To enable logging of events in debug mode, in the `/etc/squid/squid.conf` configuration file add the `-d` parameter to the first string. For example:
   ```
   auth_param basic program /usr/lib64/squid/basic_ldap_auth -R -d -b "dc=<second-level domain name>,dc=<top-level domain name>" -D "<user name>@<Active Directory domain>" -w "<user password>" -f "sAMAccountName=%s" <IP address of the Active Directory domain controller>
   ```
   Debug events will be written to the `/var/log/squid/cache.log` file.
3. Restart SQUID, running the command:
   ```
   service squid restart
   ```

Recommendations on configuring UserGate

As an ICAP-client, UserGate allows you to transmit HTTP/HTTPS traffic, SMTP and POP3 mail traffic to Traffic Monitor ICAP server. To set up interaction between UserGate and ICAP server:

1. Create an ICAP-server:
   i. Go to **Security policies** → **ICAP servers**.
   ii. Click **Add** and create one or more ICAP servers by filling in the fields:

Field	Description
Name	ICAP server name
Description	ICAP server description (optional)
Address	IP address of the ICAP server
Port	ICAP server TCP port, the default value is 1344
Message maximum size	Defines maximum size of a message (in KB) to be transmitted to ICAP server. The size should be greater than 0. **Example:** `35840`
ICAP server accessibility checking period	Sets the time in seconds after which UserGate sends OPTIONS request to the ICAP server to check if the server is available. Specify the value from 100 up to 600 seconds. **Example:** `100`

Field	Description
Skip if error occurs	If the option is enabled, UserGate does not send data to the ICAP server when the server is unavailable (does not respond to OPTIONS request). Enabling this option is not needed
Reqmod path	You can enable Reqmod mode by selecting the **Enable** flag. Then specify **path on ICAP server to work in Reqmod mode** in the format: `icap://icap-server:port/path` - specifying the full URI for the `reqmod` mode **Example**: `icap://FQDN:1344/reqmod`
Respmod path	Enabling the Respmod mode is not required
Respond with username	Set the **Enable** flag to enable sending user names to the ICAP server. Then specify **Headline** value that will be used for sending user names to the ICAP server. The default value is `X-Authenticated-User` If necessary, select the **Encode in base64** option to encode user names in base64. This can be needed if usernames contain characters of national alphabets
Respond with IP address	If the **Enable** flag is on, then sending user's IP address to the ICAP server is enabled. Then specify **Heading** that will be used for sending user's IP address to the ICAP server. The default value is `X-Client-Ip` Enabling this option is not needed
Respond with MAC address	If the **Enable** flag is on, then sending user's MAC address to the ICAP-server is enabled. Then specify **Heading** that will be used for sending user's MAC address to the ICAP-server. The default headline is `X-Client-Mac` Enabling this option is not needed

2. Create a balancing rule for ICAP servers (optional):
    a. Go to **Network policy** → **Load balancing**.
    b. Select **Add** → **ICAP Balancer** and fill in the fields:

Field	Description
Enable/Disable	Enables or disables the rule

Field	Description
Name	Rule name
Description	Rule description
ICAP servers	List of ICAP servers created in the previous step between which the load will be distributed

3. Create an ICAP rule:
    a. Go to **Security policies -> ICAP Rules**.
    b. Click **Add** and fill in the fields:

Field	Description
Enable/Disable	Enables or disables the rule
Name	Rule name
Description	Rule description
Operation	Possible options: • **Skip** - not send data to the ICAP server. By creating this rule, administrator can explicitly exclude specific kind of traffic from transmission to the ICAP server; • **Transmit** - send data to the ICAP server and wait for response. This is a standard operating mode for ICAP servers; • **Transmit and ignore** - send data to the ICAP server and ignore its response. In this case, no matter what the ICAP server responce would be, data sent to user will not be modified, but the ICAP server will receive a full copy of user's traffic.
ICAP servers	The list of ICAP servers created at the previous step between which the load will be distributed
Source	Traffic source zone and/or list of traffic source IP addresses
Users	The list of users and groups, the rule applies to. The following user types can be used: **Any**, **Unknown**, **Known**. To apply the rules to specific users or to the **Known** type, set up user identification
Destination	Traffic destination zone and/or lists of traffic destination IP addresses
MIME-type content	MIME-type lists. There is a possibility to manage video and audio content, images, executables, and other types. The administrator can also create custom groups of MIME-types

Field	Description
Categories	Lists of UserGate URL filtering categories
URL	URL lists
HTTP-method	A method used in HTTP requests. As a rule, POST or GET method is used
Service	Possible options: • **HTTP** - web traffic • **SMTP** - mail traffic. Emails will be sent to the ICAP server as a corresponding MIME type • **POP3** - mail traffic. Emails will be sent to the ICAP server as a corresponding MIME type

Warning!

ICAP rules are applied from top to bottom in the order they are listed in the console. Only the first rule for which the conditions defined in the rule are matched, is applied. This means that specific rules should be placed above general ones. Use **Up**/**Down** arrow buttons to change the order of applying rules.

Disabling ICAP

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

1. Stop Traffic Monitor processes:
   `iwtm stop`
2. Disable autostart for **iw_icap** process:
   `iwtm disable iw_icap`
3. Start Traffic Monitor processes:
   `iwtm start`
4. Check the state of Traffic Monitor processes:
   `iwtm status`

After you have disabled the module, restore original settings of the proxy server.

4.4.3 Configuring Licensing Server (in case of Cluster)

To receive correct data from interceptors in full, you need to configure the licensing server. It should run on the main Traffic Monitor server and be disabled on all other cluster nodes.

For this, take the following steps (on the node):

1. Stop **iw_licensed** service:
   `iwtm stop licensed`
2. Disable autostart of **iw_licensed** service:
   `iwtm disable iw_licensed`

And on the main Traffic Monitor server:

1. Enable autostart of **iw_licensed** service:
   `iwtm enable iw_licensed`
2. Run **iw_licensed** service:
   `iwtm start licensed`

To install, delete, request a license, or check its validity, please see the *InfoWatch Traffic Monitor. User Guide. Managing Licenses*.

4.5 Configuring Traffic Interception

The System can intercept data transferred via the following protocols:

Protocol	Description
SMTP (Simple Mail Transfer Protocol)	Mail protocol, which is used by mail clients for sending 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. For sending emails, the 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 website. You can realize interception of all transmitted data on the Internet (visited pages, portals, received 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.
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. **Important!** ICQ traffic will be intercepted if a specific server that supports OSCAR protocol is used for ICQ.
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 a mailbox. For example, access to processing events, located on the server, as if they were located on local receiver computer, without the 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 email clients.

Depending on intercepted traffic type and the interception method, the System can be configured as follows:

- Configuring SMTP Traffic Interception;
- Configuring POP3 Traffic Interception;
- Configuring HTTP Traffic Interception;
- Configuring HTTPS Traffic Interception;
- Configuring ICQ Traffic Interception
- Configuring NRPC Traffic Interception;
- Configuring IMAP4 Traffic Interception;
- Receiving Objects Intercepted by InfoWatch Device Monitor.

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 you configure traffic interception, you should 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.

4.5.1 Configuring SMTP Traffic Interception

The section contains information on how to configure interception of SMTP traffic:

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

You can find a detailed description of SMTP traffic interception scheme in the *SMTP Traffic Interception Scheme* article.

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. Enable the autorun option for `iw_proxy_smtp` process which is responsible for intercepting SMTP traffic:
   ```
   iwtm enable iw_proxy_smtp
   ```
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_x2db** (see *Enabling and Disabling Process Autorun*).

4. To avoid duplication of intercepted data, disable **iw_smtpd** process (see *Enabling and Disabling Process Autorun*).

Receiving Copies from Mail Server

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

Integration of Traffic Monitor Server with Postfix 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 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 the database.

To configure receiving copies from a mail server:

1. Make sure that **iw_smtpd** process autostart is enabled (see *Process autorun*).
2. On the mail server, configure forwarding of blind copies of SMTP messages to Traffic Monitor Server. Find a setup example for Microsoft Exchange Server 2007 and 2010 in *Forwarding Blind Carbon Copies with Microsoft Exchange Server 2007 and 2010*.
3. Configure the embedded Postfix server (see *Configuring Postfix Server in Traffic Monitor*).
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_luaengined**, **iw_cas**, **iw_pas**, **iw_x2x**, **iw_x2db**, **iw_tech-tools** (see *Process autorun*).
5. Make sure that the value of the `"TransportModes"/" Sm tp"` parameter in the **/opt/iw/tm5/etc/luaengined.conf** is `Copy` or empty.

All emails received according to the rule of shadow copy or journal rule will contain a permanent recipient, for example, "`iwtm-mon@local`". To remove it, configure the `SmtpTmBccList` parameter in the **luaengined.conf** file.

> **Important!**
>
> If MS Exchange uses a journal rule, then, for correct processing of such emails, enable the setting in Traffic Monitor. For this, in the `messed.conf` configuration file, specify:
>
> `"ExchangeJournalReports": true,`
>
> To apply the changes, restart the service **iw_messed**.

Inline Mode

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

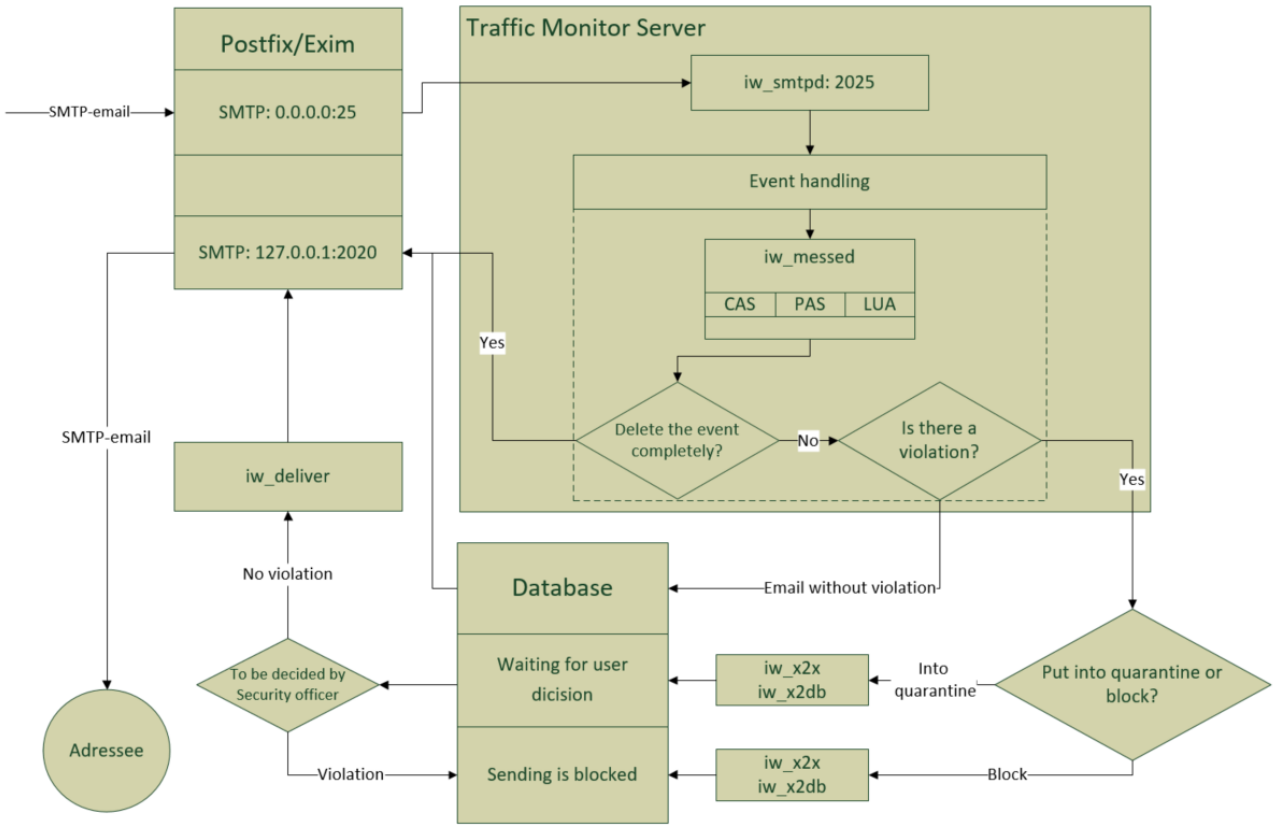
Integration of Traffic Monitor mail server with the mail server is implemented in the following way. Postfix mail server, which is embedded in the Traffic Monitor system, receives incoming SMTP messages via port **25**. SMTP messages are then transmitted to the **iw_smtpd** process via port **2025**. The System creates events for each email. Events are placed in the Traffic Monitor Database except when the *Delete event completely* action is selected in the transfer rule of the policy. In this case, the event is not placed in the Database and the email is sent to the recipient without analysis in Traffic Monitor.

In the **Inline** mode, SMTP traffic is analysed by Traffic Monitor and:

- If there is no violation, SMTP traffic is sent to the recipient or to the next relay server in the company's mail system by means of the embedded Postfix server. Delivery works as follows: the **iw_messed** process sends emails to port **2020** of the Postfix mail server. The Postfix mail server either delivers emails to recipients directly or transmits them to the next mail relay server;
- If there is a violation and policies contain the *Quarantine* verdict, then the System sets the *Quarantine* verdict to the email. The email will be delivered only if the Security officer sets the *No violation* user decision and allows the delivery in the Management Console (see the document *InfoWatch Traffic Monitor. User Guide*). Delivery works as follows: the **iw_deliver** process transmits emails to port **2020** of the Postfix server that is embedded in the System. The Postfix mail server either delivers emails to recipients directly or transmits them to the next mail relay server. You can also configure the System to automatically block quarantined event after a specified timeout;
- If there is a violation and policies contain the *Block* verdict, then the System sets the *Block* verdict to the email. In this case, the email will not be delivered.

You can also configure the System to:

- Automatically block events with the *Quarantine* verdict, see *Automatically Blocking Events with the Quarantine Verdict*.
- Suspend the sending of an email until it is confirmed by the employee who has sent it, see *Suspending Email Sending until Employee Confirmation*.



To configure the inline mode for SMTP interceptor:

1. On the corporate mail server, configure Traffic Monitor as a relay server.

> **Note:**
>
> If the company uses more than one mail server, each server should be configured to send messages to the embedded Postfix server.
>
> The configuration process may differ depending on the mail server which is 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*).
4. Stop the **iwtm** service:

```
iwtm stop
```

5. Open `/opt/iw/tm5/etc/luaengined.conf` for editing.
6. In `Smtp` property of `TransportModes` section, specify TM server name with interceptor (for example, `tm-server1`) and mode value `Normal` (*Block* mode):

```
"Smtp": [{"Server": "tm-server1", "Mode": "Normal"}]
```

> **Important!**
>
> In case of distributed installation, the mode is defined by the local **iw_luaengined** process or the one located on another node. That is why on each node in the `/opt/iw/tm5/etc/luaengined.conf` file in the `Smtp` property of the `TransportModes` section you need to specify several pairs of valid FQDN names of TM servers and required modes. For example:
>
> ```
> "Smtp": [{"Server": "tm-server1.local", "Mode": "Copy"}, {"Server":"tm-server2.local.ru", "Mode": "Normal"}]
> ```
>
> Note that the `iwssid.lua` and `luaengined.conf` files should be the same on all the nodes.

7. Save the file.
8. Start the **iwtm** services:

```
iwtm start
```

For the traffic to be transmitted in spite of a verdict given:

1. In the code in step 6 above, set the `Transparent` value for the `TransportMode` parameter.
2. Save the file.
3. Restart the System:

```
iwtm restart
```

Delivering SMTP emails with processing errors sent in "inline mode"

SMTP emails processing of which caused errors are to be put into the error queues: **queue/x2x-errors** and **queue/errors**. Delivering SMTP emails (including the ones with *Quarantine* verdict assigned) is performed by **iw_rammer** daemon from error queues. After that the queues are to be refined. The System extracts the sender and recipient's addresses (if provided) from an XML file. Otherwise, the email cannot be delivered. When sending an email to Security officer, the sender and recipient's addresses are specified within the configuration file **/opt/iw/tm5/etc/rammer.conf**. The email attachment contains XML and DAT object files. Email sending to the addressee as well as notification for Security officer is performed via Postfix mail server (port **2020**). Notification is to be delivered to Security officer via event email and the sender is specified from initial message. Connection data (address and port), as well as the addressee and sender addresses, are set within the **rammer.conf** configuration file (for details, see the document *InfoWatch Traffic Monitor. Configuration Files Guide. rammer.conf*).

SMTP email is to be delivered when meeting each of the following terms:

1. If it wasn't delivered in a regular mode (by **iw_messed** daemon);
2. If *Block* mode is assigned when processing the email and when the email got into error queue;
3. If the email wasn't qualified as a *Blocked* one.

Forced delivery measure is **/opt/iw/tm5/bin/rammer_tool** utility. To view the list of available settings, enter in the command line:

```
/opt/iw/tm5/bin/rammer_tool --help
```

Automatically Blocking Events with the Quarantine Verdict

You can configure the System to assign the *Blocked* verdict to quarantined events after a specified timeout. For this open `opt/iw/tm5/etc/web.conf`, in `autoForbid` → `quarantined` section change the `timeout` parameter value (in minutes). The value by default is 0, i.e. the System does not block quarantined events.

When changing the timeout, you may also need the following settings:

- Parameter `batchSize` – the number of events processed at a time. The default value is 5000. To edit the value, go to the file `opt/iw/tm5/etc/web.conf`, section `autoForbid` → `quarantined`;
- Cron task launching schedule. To edit the schedule, go to the file `etc/cron.d/web_cron`. By default, the task is launched every 4 hours and looks like this:

```
*/* 4 * * * iwtm /opt/iw/tm5/www/backend/protected/yiic autoforbid quarantined
```

Note:

The System uses the cron task to assign the verdict *Blocked* to the set number of events with the expired timeout.
For example, 1 hour waiting period is specified and the cron task runs every 4 hours. In this case, the events which have been quarantined for at least 1 hour will have their verdicts automatically changed within 4 hours.

We do not recommend to set the cron task execution frequency to less than 30 minutes.

A value of **batchSize** that is too large can affect system load.

Suspending Email Sending until Employee Confirmation

The System has a mechanism that prevents the accidental sending of confidential information. The System suspends the sending of an email until it is confirmed by the employee who has sent it.

Details of the process:

1. The System intercepts the email containing confidential information and places it in quarantine.
2. The employee receives an email notification about the suspended sending and a link to the confirmation page.
3. The employee clicks the link and either confirms the email or permanently blocks it:
    - If confirmed, the System forwards the email to the recipient;
    - If the email is not confirmed within the specified waiting period, the System automatically blocks it.

The System can also send the notifications about blocking/unblocking emails.

Note:

The System user (Security officer) can also block or confirm the email in the Traffic Monitor Management Console. If the Security officer changes the verdict before the employee does, the selection of actions on the confirmation page will become unavailable.

The default waiting period is 24 hours. For details on changing the waiting period, see below.

You can configure:

- Notification templates, see *InfoWatch Traffic Monitor. User Guide. Configuring Notifications;*
- Confirmation page display (change the text, accent colour, logo, contact information, web page address);
- Confirmation waiting period.

Configuring the confirmation page

To configure the confirmation page display (change the accent colour, add a logo and contact information):

1. In the directory `/opt/iw/tm5/www/frontend/tmng/tmng/custom/`, create a file **justify.json**.
2. From the file **justify.json.example** that is placed in the same directory, copy the block with the parameters to **justify .json**. Make sure you do not copy the commented block to the file.
3. If you need to add a logo, place the file with the image in the directory `/opt/iw/tm5/www/frontend/tmng/tmng/custom/`.
4. In the file **justify.json**, edit the parameter values as per the table. All parameters are optional and can be deleted.

Parameter	Description
`accentColor`	Accent colour of the page in the HEX format.

Parameter	Description
	Example: `#3f51b5`

`phones`	List of the contact phone numbers/email addresses. You can enter several parameters in the form of a string array. Use comma as a separator.
	Examples:
	`["+1 (234) 56-789-01", "+1 (234) 56-789-02"]`
	`["support@support.example", "support1@support.example"]`

`emails`	
`securityContact`	Security service address that is displayed in the confirmation text. Default value: `security@infowatch.ru`
`logo`	Path to the file with the logo. Specified relative to the directory `/opt/iw/tm5/www/frontend/tmng/`. Supported file formats: SVG, PNG, JPEG, AVIF, WebP. Example: `/tmng/custom/logo.svg`
`texts`	Customizable page text. See the description below.

5. Save the changes.

Configuring the confirmation page text

The section `texts` contains the subsections `ru` and `en`, each containing the parameters:

- `alert` – text of a notification that the email needs to be confirmed to be sent. Displayed in a separate block under the page header.
- `description` – the main text of the notification page. Displayed under the "Confirm sending" header and right over the confirmation/blocking buttons.

In the texts `alert` and `description`, the following parameters are used by default:

Parameter	Description
`date`	Email sending date. Configured automatically based on the event data.
`time`	Email sending time. Configured automatically based on the event data.
`subject`	Email subject. Configured automatically based on the event data.
`expiry`	Date and time when the confirmation waiting period expires. Configured automatically based on the email sending date and time, as well as the waiting period.

Parameter	Description
`contact`	Security service contact. The value configured by the `securityContact` variable is used. If there is no variable `securityContact`, the default value is used: `security@infowatch.ru`

If needed, you can reorder the parameters in text any way you want, as well as delete the parameters you don't need.

Configuring the confirmation page address
You can change the confirmation page address: the address of another server with an installed and configured Nginx will be displayed instead of the Traffic Monitor address.
To do this:

1. On any server with Nginx, create a file `/etc/nginx/conf.d/confirmation_page.conf`.
2. Paste the following content to the file:

```
server {
    listen 80;

    # The domain where the page will be available
    server_name <domain_name>;

    # When using the HTTPS protocol
    #listen 443 ssl;

    # If needed, specify the location of the SSL-key and the certificate
    #ssl_certificate     <certificate_location>;
    #ssl_certificate_key <key_location>;

    charset utf-8;

    # Proxying settings
    proxy_http_version 1.1;
    proxy_ssl_server_name on;

    # Connection timeouts with the target server
    proxy_connect_timeout 10s;
    proxy_send_timeout 60s;
    proxy_read_timeout 60s;

    # Transfer of information about the initial request
    proxy_set_header X-Real-IP         $remote_addr;
    proxy_set_header X-Forwarded-For   $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Forwarded-Host  $host;

    # Transfer of API service headers
    proxy_set_header X-API-PERSONALHASH $http_x_api_personalhash;
    proxy_set_header X-API-VERSION      $http_x_api_version;
```

```
    # Proxying API requests to the main Traffic Monitor server
    location ~ ^/(justify|xapi|)(/|$) {
        # Specify the domain name or the IP address of the server
        proxy_pass https://<сервер_Traffic_Monitor>
    }

    location ~* \.(?:css|js|png|jpg|jpeg|gif|svg|ico|woff2?|ttf|eot|json)$ {
        # Specify the domain name or the IP address of the server
        proxy_pass https://<сервер_Traffic_Monitor>
    }

    # Ban on all other requests
    location / {
        return 404;
    }
}
```

3. Fill in the following parameters:
   - `server_name` – domain name or the IP address of a server with Nginx that is displayed as an address of the confirmation page;
   - `proxy_pass` (occurs twice) – the actual Traffic Monitor address (domain name or IP-address).
4. To work over the HTTPS protocol, uncomment the strings:
   - `listen 443 ssl;`
   - `ssl_certificate     <certificate_location>;`
   - `ssl_certificate_key <key_location>;`

   In the variables `ssl_certificate` and `ssl_certificate_key`, specify the location of the SSL certificate and the key.
5. On the Traffic Monitor server in the `/opt/iw/tm5/etc/web.conf` configuration file, parameter `justify_host`, specify the address of the server with Nginx.
   For example:

```
justify_host: "http://domainname.ru" or justify_host: "https://203.0.113.0"
```

Configuring the confirmation waiting period

To edit the period when the System waits for the confirmation from the user/Security officer before permanently blocking the email, in the file `opt/iw/tm5/etc/web.conf`, section `autoForbid`, subsection `justify`, change the value of the parameter `timeout` (in minutes). The default value is 1440 minutes (24 hours).

When changing the waiting period, you may also need the following settings:

- parameter `batchSize` – the number of events processed at a time. The default value is 5000. To edit the value, go to the file `opt/iw/tm5/etc/web.conf`, section `autoForbid`, subsection `justify`;
- cron task launching schedule. To edit the schedule, go to the file `etc/cron.d/web_cron`. By default, the task is launched every 4 hours and looks like this:

```
*/* 4 * * * iwtm /opt/iw/tm5/www/backend/protected/yiic autoforbid justify
```

Note:

The System uses the cron task to assign the verdict *Blocked* to the set number of events with the expired waiting period.
For example, 1 hour waiting period is specified and the cron task runs every 4 hours. In this case, the events for which 1 hour has already passed since the confirmation request was sent will have their verdicts automatically changed within 4 hours.

We do not recommend to set the cron task execution frequency to less than 30 minutes.
A value of `batchSize` that is too large can affect system load.

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.

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 the **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 the IP address of the 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 the 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 the 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!**
>
> The 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 a 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 a 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** checkbox. 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 the **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 is 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** checkbox.
6. Click **OK**.

Important!

If MS Exchange uses a journal rule, then, for the correct processing of such emails, enable the setting in Traffic Monitor. For this, in the `messed.conf` configuration file, specify:

```
"ExchangeJournalReports": true,
```

To apply the changes, restart the service **iw_messed**.

Configuring Blind Carbon Copies with ZCS Zimbra

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`

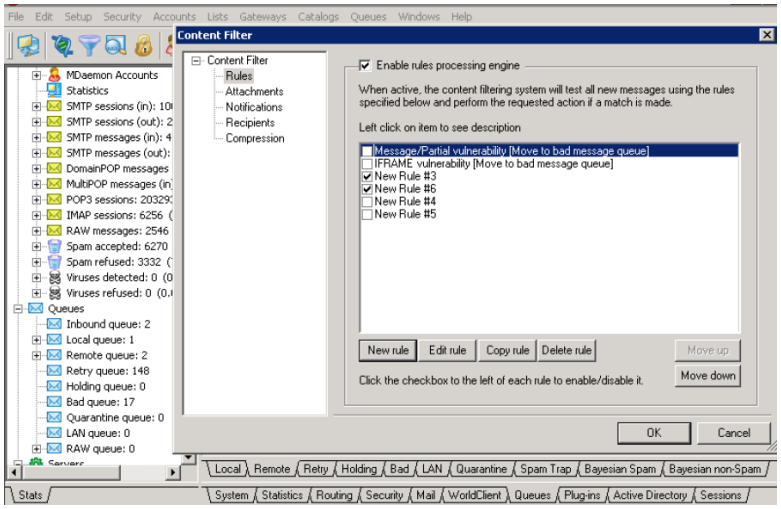
Configuring BCC

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

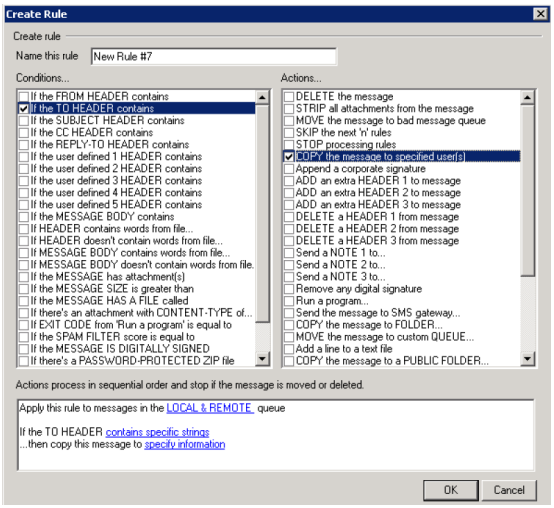
Forwarding BCC with MDaemon

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 method and on how the Traffic Monitor 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	Traffic Monitor server is installed separately from the database	Required
	All components are installed on the same server	Configured by default
Traffic Monitor intercepts and delivers SMTP traffic by means of integration with Postfix	Traffic Monitor server is installed separately from the database	Required
	All components are installed on the same server	Configured by default
The System receives a copy of SMTP traffic via Sniffer		Not required
Interception of SMTP traffic is not required (for example, Traffic Monitor is used only as Sniffer)		Not required

For proper interaction between 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 on behalf of the `root` user:

   ```
   su – root
   ```

2. Apply these settings in the `main.cf` file:
   a. Set the value for `inet_interfaces` parameter as recommended on the Postfix site. In most cases, you should specify `all` as `inet_interfaces` parameter value.
   b. Set the value of the `message_size_limit` parameter (`5000000` by default) to be higher than what is set on the corporate mail server. Otherwise, senders may receive messages from Postfix that emails cannot be sent.
   c. Make sure that `mynetworks` parameter contains the correct name of the subnet where mail servers are located.
   d. In case Traffic Monitor participates in delivering SMTP traffic (see *Inline Mode*), configure the `relayhost` parameter. As its value, enter the IP address of the corporate mail server to which SMTP emails will be sent after analysis in Traffic Monitor and a password to access the mail server. For example:

      ```
      relayhost = [smtp.organization.ru]:port
      ```

3. Apply the settings in the `master.cf` file:
   a. Add the following line to enable sending mail to Traffic Monitor for analysis:

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

> **Note:**
>
> When the System is installed with the installer, this setting is applied automatically.

b. In case Traffic Monitor participates in delivering SMTP traffic (see *Inline Mode*), write the following lines to the end of the file:

```
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=<fully_qualified_domain_name_of_the_server>
```

> **Important!**
>
> Lines that specify the service options should begin with a space. For example:
>
> " `-o <option_specification>` "

4. Check that the syntax in configuration files is correct:

```
postfix check
```

5. Restart Postfix:

```
systemctl restart postfix
```

6. Check the availability of the Postfix mail server via port 25 with the following command:

```
telnet <TM_IP> 25
```

where `<TM_IP>` is the IP address of the Traffic Monitor server on which Postfix has been configured.
In response to this command, the following message should be displayed:

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

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

If you cannot establish the connection, perform step-by-step checks of the subnet and port settings depending on your network configuration.

> **Important!**
>
> Traffic Monitor installed on a server running Alt Server 10 does not support interception of emails with UTF-8 encoded headers. To set it up, reinstall the Postfix server with the `libicu-devel` package. To learn more, see the Postfix site.

4.5.2 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.

4.5.3 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 *Configuring Server to Work with SPAN, or Port Mirroring Technology*).
2. Enable autostart of HTTP traffic interceptor:
```
iwtm enable iw_proxy_http
```

3. Make sure, that autostart of all processes, which participate in traffic interception and analysis, is enabled:
iw_sniffer, iw_warpd, iw_cas, iw_x2db (see *Enabling and Disabling Process Autorun*).

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*).

4.5.4 Configuring HTTPS Traffic Interception

For this traffic interception method, see in *HTTPS Traffic Interception Scheme*.

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.

4.5.5 Configuring ICQ 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 *Configuring Server to Work with SPAN, or Port Mirroring Technology*).
2. Enable autorun of ICQ traffic interceptor:

```
iwtm enable iw_proxy_icq
```

4.5.6 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 *Configuring Server to Work with SPAN, or Port Mirroring Technology*).
2. Open **capstack.conf** configuration file, which is located in `/ort/iw/tm5/etc` directory.
3. Make sure, that `Usedprocessors` section has NRPC traffic interceptor enabled:
   `"UsedProcessors": {`
   `"nrpc": true,`
4. Make sure, that `Processors` section has NRPC traffic transmission enabled:
   `"processors": {`
   `"nrpc": {`
   `"TrackExternal": true,`
   `"TrackInternal": true`
   `},`
5. Save changes in the **capstack.conf** file.
6. Enable autostart for **iw_capstack** process:
   `iwtm enable iw_capstack`
7. Restart **iw_capstack** process:
   `iwtm restart capstack`

4.5.7 Configuring IMAP4 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 `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.

4.5.8 Receiving Objects Intercepted by InfoWatch Device Monitor

1. Install and configure Traffic Monitor Server part (see document *InfoWatch Traffic Monitor. Installation Guide. Installing Traffic Monitor Server and Database*).
2. Setup event transmission from Device Monitor to Traffic Monitor server (see document *InfoWatch Device Monitor. User Guide. Device Monitor Server Settings. Connecting to Traffic Monitor Server*).
3. Setup object analysis parameters (see document *InfoWatch Traffic Monitor. User Guide. Technologies Section*).

4.6 Process autorun

This section contains features of System's processes autostart:

- Check of Process Autorun;
- Enabling and Disabling Process Autorun.

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

4.6.1 Check of Process Autorun

Important!

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

Note:

For instructions on enabling and disabling process autorun, see *Enabling and Disabling Process Autorun*.

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

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

Process	By default autorun is enabled
`iw_adlibitum`	Yes **Note:** The process should operate only on the main server
`iw_agent`	Yes
`iw_analysis`	Yes
`iw_kicker`	Yes **Note:** The process should operate only on a server with the web console
`iw_blackboard`	Yes
`iw_bookworm`	Yes **Note:** The process should operate only on the main server
`iw_capstack`	No
`iw_cas`	Yes
`iw_configerator`	Yes **Note:** The process should operate only on a server with the web console
`iw_deliver`	Yes **Note:** The process should operate only on the main server
`iw_icap`	Yes
`iw_is`	Yes **Note:** The process should operate only on the main server
`iw_indexer`	Yes **Note:** The process should operate only on the main server
`iw_image_autoling`	Yes **Note:** The process should operate only on a server with the web console
`iw_text_autoling`	Yes **Note:** The process should operate only on a server with the web console
`iw_licensed`	Yes **Note:** The process should operate only on the main server
`iw_luaengined`	Yes

Process	By default autorun is enabled
`iw_messed`	Yes
`iw_pas`	Yes

`iw_proxy_http`
`iw_proxy_icq`
`iw_proxy_smtp`
	No

`iw_qmover_client`	No
`iw_qmover_server`	No
`iw_sample_compiler`	Yes
`consul`	Yes
`iw_smtpd`	Yes
`iw_sniffer`	No
`iw_system_check`	Yes
`iw_tech_tools`	Yes
`iw_updater`	Yes
`iw_warpd`	Yes
`iw_x2x`	Yes
`iw_x2db`	Yes
`iw_xapi_xapi` `iw_xapi_puppy`	Yes
`iw_space_manager`	Yes **Note:** The process should operate only on the main server
`iw_attributor`	No
`iw_rest2push`	No **Note:** You have to start the process manually. For details, see *Enabling and Disabling Process Autorun*

In order to check which processes are configured to start automatically, use the command:

```
iwtm status
```

This will display a list of all Traffic Monitor process with their statuses. In `enabled state` field, find autorun status:

- `loaded (enabled)` if autorun is enabled;
- `loaded (disabled)` if autorun is disabled;
- `loaded (static)` if service is in static mode, i.e. it runs according to its settings;
- `masked (masked)` or `masked (bad)` if service is masked, i.e. autorun is disabled.

In order to check autorun status for a specific service, use the command:

```
iwtm status <process_name>
```

> **Note:**
>
> To delete all `iw_kicker` processes from the server, delete `iwtm-web-meta` package:
>
> ```
> rpm -e iwtm-web-meta
> ```

4.6.2 Enabling and Disabling Process Autorun

In order to enable/disable process autorun, use the commands:

- **Enabling process autorun**

  ```
  iwtm enable <process_name>
  ```

- **Disabling process autorun**

  ```
  iwtm disable <process_name>
  ```

- **Enabling autorun for several processes**

  ```
  iwtm enable <process1_name> <process2_name> ... <processN_name>
  ```

- **Disabling autorun for several processes**

  ```
  iwtm disable <process1_name> <process2_name> ... <processN_name>
  ```

- **Enabling autorun for all processes**

```
iwtm enable all
```

- **Disabling autorun for all processes**

```
iwtm disable all
```

Example of enabling/disabling `iw_proxy` service:

The `iw_proxy` service includes three components: `iw_proxy_http`, `iw_proxy_icq` and `iw_proxy_smtp`. For this reason:

1. For each process of the service, enable/disable autorun:
   - **Enabling autorun**

```
iwtm enable iw_proxy_http iw_proxy_icq iw_proxy_smtp
```

   - **Disabling autorun**

```
iwtm disable iw_proxy_http iw_proxy_icq iw_proxy_smtp
```

2. Restart the processes of `iw_proxy` service:

```
iwtm restart iw_proxy_http iw_proxy_icq iw_proxy_smtp
```

All Traffic Monitor processes with the `loaded ( enabled)` status can run automatically, while processes with the `masked (masked )` status can only be started manually.

In order to configure the process autorun:

1. Go to the directory with unit files, `/usr/lib/systemd/system`.
2. Edit the process unit file and save your changes. For details, see *InfoWatch Traffic Monitor. Configuration Files Guide*. *Traffic Monitor configuration and unit files description*.
3. Reload the configuration:

```
systemctl daemon-reload
```

4. Add the configured process to autorun:

```
iwtm enable <process_name>
```

5. Start the process:

```
iwtm start <process_name>
```

6. Check if the process is started with one of the following commands:

- **Command to check status of a specific process**

```
iwtm status <process_name>
```

- **Command to check status of all services**

```
iwtm status
```

In `Active` field or in the line corresponding to the process, find the process status:

- `active (running)`;
- `inactive (dead)`.

4.7 Remote database interaction module

In case the System deployment scheme is chosen in a way, that database, receiving intercepted objects is located on a remote server, you need to install a remote database interaction module.

The 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 *InfoWatch Traffic Monitor. Installation Guide. Distributed Installation of TM Enterprise*).

The standard process of data transmission to a database is **iw_x2db** (see *List of Traffic Monitor Server End Processes*). Using a remote database integration module with a remote database provides an additional opportunity to configure:

- the speed of files transmission to file queue;
- schedule of the width of the file transmission channel.

Configuration 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.

4.7.1 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 the 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 the documents *InfoWatch Traffic Monitor. Configuration Files Guide. qmover_client.conf and iw_qmover_client.service* and *InfoWatch Traffic Monitor. Configuration Files Guide. qmover_server.conf and iw_qmover_server.service*).

4.7.2 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
`ListenerIP`	Server IP address (**qmover_server** service)
`Port`	Server port (central office)
`NookDir`	**qmover_server** service working catalogue
`ChannelWidth`	Channel bandwidth, speed of data downloading to Traffic Monitor (Kbps). Can be implicitly limited with `WindowSize` parameter

2. Restart Traffic Monitor:
   `iwtm restart`

Configuring processes autorun

- Enable autorun for **iw_qmover_client** process.
- Disable autorun for **iw_x2db**, **iw_x2x**, **iw_deliverd** and **iw_adlibitum** processes.

For more information on disabling and enabling processes autorun see *Enabling and Disabling Process Autorun*.

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> <bandwidth>`
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	
	Per cent 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
```

4.7.3 Configuring the Server of the Remote Database Management Module

Configuration setting

Configure the following client settings in the configuration file **/opt/iw/tm5/etc/qmover_server.conf**. The directory where the objects queue is stored is /opt/iw/tm5/queue/db. For this:

1. Specify the IP address of a client (branch office) in the `ip` parameter.
2. Specify the port, where the server listens for objects coming from clients in the `port` parameter.

> **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 Process Autorun*.

4.8 Configuring OCR Extractors

OCR for different interceptors is configured in the configuration files:

- **To enable OCR for analysis of intercepted images**, use the `/opt/iw/tm5/etc/warpd.conf` file. In the `Warp` section, set the value of the `EnableOCR` parameter to `true`.
- **To enable OCR for analysis of images loaded as sample documents**, use the `/opt/iw/tm5/etc/ sample_compiler.conf` file. Set the value of the `EnableOCR` parameter to `true`.

To configure OCR for different interception channels, use the `/opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml` file. Setting levels are listed by priority, from lowest to highest.

- Level of a service;
- Level of the event type for a particular service;
- Level of a protocol for a particular event type.

For details, see *Configuring OCR*.

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

```
iwtm restart
```

> **Note:**

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

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.

4.8.1 Interception channels

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

Service	Event type	Protocol
Email	Email	POP3 SMTP IMAP MAPI NRPC
	Web email	HTTP HTTPS
Messenger	Skype	SKYPE
	ICQ	OSCAR
	XMPP	XMPP
	MS Lync	SIP
	Telegram	-
	VK (VKontakte)	HTTPS
	Facebook	HTTPS
	WhatsApp	WhatsApp
Internet activity	Web message	HTTP HTTPS

Service	Event type	Protocol
File exchange	FTP	FTP
	External devices	-
	Cloud storages	HTTPS
Printer and MFD	Print	-
Storage	Data Discovery	-
Recording media	Photo	-

4.8.2 Supported OCR extractors

During Traffic Monitor installation, both extractors are installed to the server end of the System, and one of them is chosen for usage:

- Content AI ContentReader Engine 12;
- Tesseract 4.1.1.

In case you selected Content AI ContentReader Engine, configure the license manually.

Functional differences of extractors are listed in the table below:

Functionality	Content AI ContentReader Engine	Tesseract
Recognition of image rotation angles	0 (+/-20) , 90 (+/-20), 180 (+/-20) and 270 (+/-20) degrees	-
Recognition of colour images	+	-
Image correction	+	-
Recommended image resolution	300 DPI for text with a font size from 10pt 400-600 DPI for text with a font size of 9pt and less	300 DPI for text with a font size from 10pt 400-600 DPI for text with a font size of 9pt and less

Note:

To avoid deviation from recommended image resolution, when using Content AI ContentReader Engine the parameter `AutoOverwriteResolution` (`true` by default) is used, which allows to specify the image resolution automatically.

Tesseract settings

Select the extractor

To configure the System to use Tesseract:

1. Delete the `/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
```

Change image size limits

To change size limit for images that can be sent:

1. Go to `/ opt/iw/tm5/etc/image2text_ts.conf` directory.
2. Edit the `MaxSizeInKb` (maximum size) and `MinSizeInKb` (minimum size) parameters. By default, their values are 1536 KB and 40 KB respectively.

Enable OCR only for cloud storage events

To enable OCR only for cloud storage events:

1. Open the `/opt/iw/tm5/etc/config/bookworm/services.xml` file and find `mnemo` and `key` parameters, which are suitable for cloud storage.
   For example:

```
object_type mnemo="cloud_storage"

key="AA9DFB259F0DFEE040BADC95815E13A200000000"
```

2. Copy the values of the `key` and `mnemo` parameters and paste them into `/opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml` file.

Content AI ContentReader Engine settings

Configure license

To configure Content AI ContentReader Engine license:

1. In the `/opt/iw/tm5/etc/image2text_fre.conf` configuration file, edit values of the fields as follows:
   - Enter serial number in the `SerNum` field;
   - Enter password in the `Pwd` field.

2. Copy the license file (`.LocalLicense` format) to the `/var/lib/Content_AI/SDK/12/Licenses` directory.
3. Make sure that `iwtm` user can access the downloaded file.
4. Restart the `iw_warpd` service.

Select the extractor

To configure the System to use Content AI ContentReader Engine:

1. Delete the `/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
```

Activate fast mode of document processing

Content AI ContentReader Engine can operate in two modes:

- *Balanced mode* provides the best quality of images processing (default mode). You can configure the user profile of the mode in `/opt/iw/tm5/etc/CRProfile.ini` file;
- *Fast mode* provides the fastest images processing, 64 pages can be loaded at a time while document synthesis. You can configure the user profile of the mode in `/opt/iw/tm5/etc/CRProfile_fast.ini` file. If required, configure the mode manually.

The following options are enabled while *Fast mode* is on:

- Fast mode of page orientation detection (the quality lowers);
- Standard analysis of page, no sample selection;
- Ignoring the shadows;
- Detecting tables during analysis;
- Fast objects extraction (the quality lowers).

The following options are disabled while *Fast mode* is on:

- Balanced mode;
- Processing images as photos;
- Compressing images;
- Using image binarization;
- Detecting font parameters;
- Removing garbage from image;
- Removing texture from temporary image;
- Detecting porous text;
- Detecting whole text on image, including text within image;
- Extracting whole text from image;
- Detecting headlines;
- Detecting footnotes;
- Detecting table of contents;
- Detecting running titles;
- Detecting pages of document.

To activate the fast mode of document processing, in `"Profile":"etc/CRProfile_fast.ini"` parameter of the configuration file `/opt/iw/tm5/etc/image2text_fre.conf` , indicate the path to the file with user profile configuration, then save the changes.

Warning!

Speed optimization of images processing cannot be applied for scanned copies of schemes, location maps, monochrome images.

Change image size limits

To change size limit for images that can be sent:

1. Go to `/opt/iw/tm5/etc/image2text_fre.conf` directory.
2. Edit the `MaxSizeInKb` (maximum size) and `MinSizeInKb` (minimum size) parameters. By default, their values are 1536 KB and 40 KB respectively.

Enable OCR only for cloud storage events

To enable OCR only for cloud storage events:

1. Open the `/opt/iw/tm5/etc/config/bookworm/services.xml` file and find `mnemo` and `key` parameters, which are suitable for cloud storage.
   For example:

   ```
   object_type mnemo="cloud_storage"

   key="AA9DFB259F0DFEE040BADC95815E13A200000000"
   ```

2. Copy the values of the `key` and `mnemo` parameters and paste them into `/opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml` file.

4.9 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).

4.10 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.

4.11 Service-to-service cooperation setup (Consul service)

To register the services, monitor the accessibility and detect Traffic Monitor components the decentralized fault-tolerant discovery service Consul is used. The Consul agent:

- is installed on each host and is a significant part of cluster activity;
- revealing the services, collecting the services state data, realizing DNS, API HTTP and RPC CLI interfaces;
- can be started in one of two modes: client and server one.

Consul is used in all types of installation. Information on System installation is available in *InfoWatch Traffic Monitor. Installation Guide. System Deployment Schemes and Installation Types*.

When using All-in-One installation mode, the configuration parameters to connect to the Consul service are set automatically during the installation. The only exception is the distributed installation, when Traffic Monitor and the database are installed on different servers (when the System is installed on more than one node and has more than one network interface). See how to configure in *Configuring Consul and creating a cluster* article.

The service operation settings are to be done within the configuration file located by the following path: `/opt/iw/tm5/etc/consul/consul.json`. The full description of parameters is available at the page *consul.json configuration file and iwtm-consul.service unit file*.

4.11.1 Starting and stopping the service

To start the Consul service, use one of the following commands:

- `service iwtm-consul start`
- `systemctl start iwtm-consul.service`

To stop the Consul service, you can use the following commands:

- `service iwtm-consul stop`
- `systemctl stop iwtm-consul.service`

If necessary, you can start the Consul agent **manually**:

```
consul agent -data-dir=<path> -bind=<bind_addr> -bootstrap -server -ui
```

where:
- `<path>` is a path to the directory with service data (e.g., `/opt/iw/tm5/var/consul`);
- `<bind>` is the network interface address.

If the System has more than one network interface, specify one of the following parameters:
- `-bind=<ip-address>`;
- `-config-file` or `-config-dir` – the path to the configuration file (e.g.: `/opt/iw/tm5/etc/consul`).

If several configuration files are loaded, their options are merged.

4.11.2 Registering services in Consul

You can register a service in Consul in 2 ways:

- using HTTP API or agent's configuration file, in the case, when service can communicate to Consul independently;
- registering service as an external component.

Services with obligatory registry in Consul	Services installed on nodes with Consul Server or Consul Client
iw_adlibitum	iw_adlibitum
iw_agent	iw_agent
Iw_analysis	Iw_analysis
iw_blackboard	iw_bookworm
iw_bookworm	iw_capstack
iw_capstack	iw_cas
	iw_configerator

Services with obligatory registry in Consul	Services installed on nodes with Consul Server or Consul Client
iw_cas	iw_icap
iw_icap	iw_indexer
iw_deliver	iw_licensed
iw_indexer	iw_kicker
iw_licensed	iw_luaengined
iw_luaengined	iw_messed
iw_messed	iw_pas
iw_pas	iw_proxy_http
iw_proxy_http	iw_proxy_icq
iw_proxy_icq	iw_proxy_smtp
iw_proxy_smtp	iw_qmover_server
iw_qmover_server	iw_sample_compiler
iw_sample_compiler	iw_system_check
iw_system_check	iw_smpd
iw_smtpd	iw_tech_tools
iw_tech_tools	iw_updater
iw_updater	iw_warpd
iw_warpd	iw_xapi_xapi
iw_xapi_xapi	iw_xapi_puppy
iw_xapi_puppy	iw_x2x
iw_x2x	iw_x2db
iw_x2db	Web (backend)

After the registration, Traffic Monitor services and Consul interact the following way:

- registration using Consul client;
- establishing TCP connection or returning HTTP code;
- deregistration.

4.11.3 Distributed installation

Important!

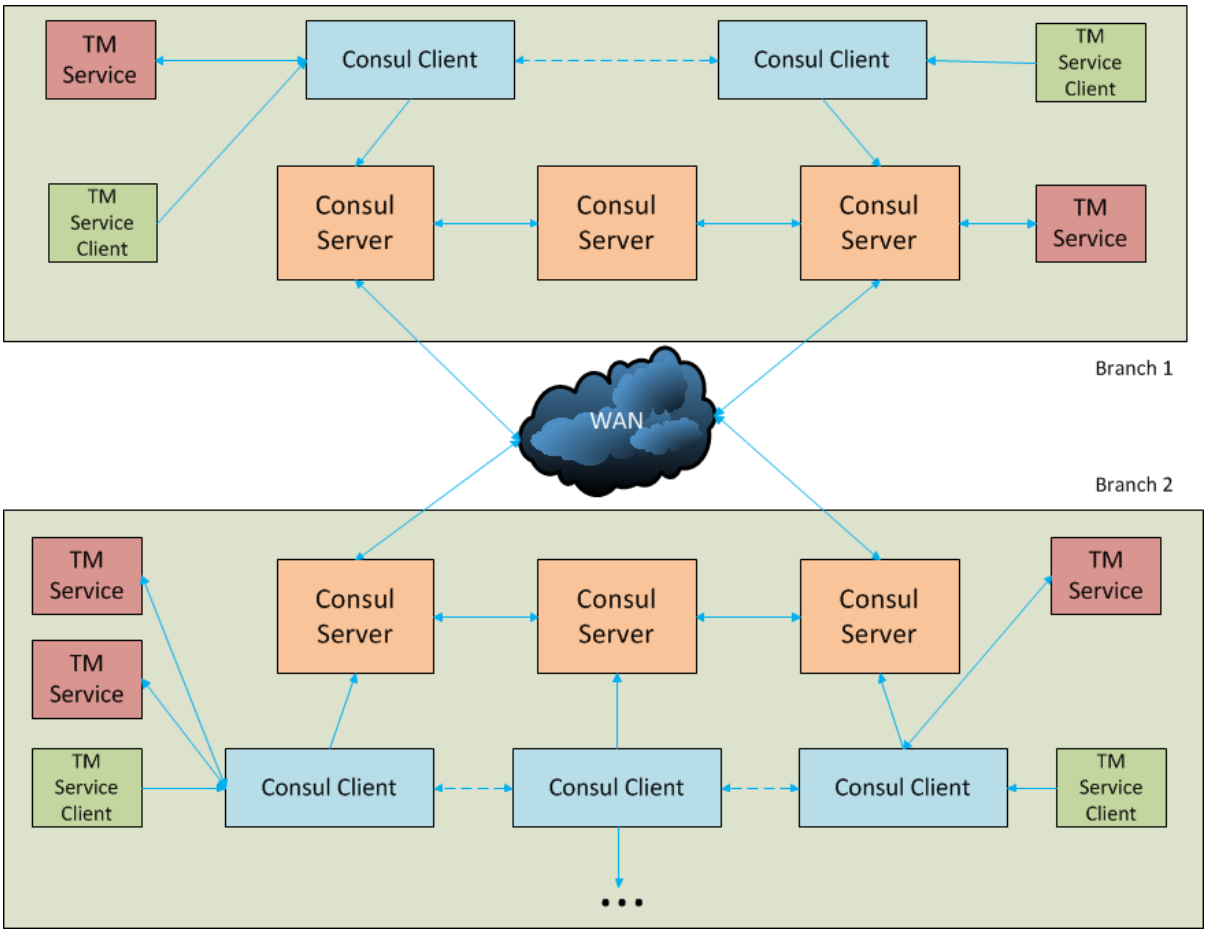
To use the Consul service, the full-mesh network topology ("each-to-each" connection) should be implemented for all the agents within the cluster and for servers, when combining them into WAN.

Clustering

The client collects the node- and service-related data and sends it to the server. System components searching for services send the request to the agent started on a local workstation, which resends the request to an available server. If the server is unable to respond to the request, it can send the request to a different data center (a branch) and retrieve the response.

Servers compose a cluster and define independently the leading server, responsible for elements coordination within the cluster. The first/the only one server is usually started in bootstrap mode (assigning the leader manually). When starting the agent, to connect to cluster it is enough specifying one server of this cluster. While configuring it in `retry_join` option, it is recommended specifying all the servers of the cluster. A quorum to hold the operations and to provide the consistency is required in each data center. If there are few data centers, a separate cluster to be created in each of them. Data centers are not isolated from each other due to service detection task. An agent within one data center can get information from a separate data center.

The Consul network can use one server, but to avoid data loss it is recommended using from three to seven servers within the data center.



Example:

A cluster consisting of three nodes (servers) continues operating when one server is out of operation.

Below are the examples of using the interface command line:

Command	Description
`consul members`	Displays the list of cluster members
`consul catalog services -node <node_name>`	Displays the list of cluster servers on a specific computer
`consul operator raft list-peers -stale=true`	Displays the list of all the servers regardless of the cluster

Connecting to cluster

You may register extra nodes on the cluster using one of the following ways:

- Enter the command:

  ```
  consul join <ip-address>
  ```

  Please make sure that, within `consul.json` configuration file, all the servers and Consul clients have the same parameters `datacenter` and `encrypt` (see *consul.json configuration file and iwtm-consul.service unit file*)
- In `consul.json` configuration file, in `retry_join` parameter specify the list of servers to be joined

4.11.4 Network rules configuration to access Consul

To set up the network exchange the following ports between all Consul agents (servers and clients) should be accessible.

Port by default	Interface	Supported protocols	Description
8300	Server RPC	TCP	Used by servers to process incoming queries from other agents
8301	Serf LAN	TCP, UDP	Used by agents to process data flows within local network
8302	Serf WAN	TCP, UDP	Used by servers to exchange data with other servers via WAN
8400	CLI RPC	TCP	Used by all the agents to process RPC from CLI
8500	HTTP API	TCP	Used by clients to interact with HTTP API interface
8600	DNS	TCP, UDP	Used to allow DNS queries

4.11.5 consul.json configuration file and iwtm-consul.service unit file

Contents of **`consul.json`** configuration file

Content	Description
`{`	
`"bootstrap_expect": 1,`	Number of servers expected in cluster (for server mode only)
`"server": true,`	Start of agent in server mode (`false` – client mode)
`"datacenter": "iwtm",`	Title for datacenter
`"data_dir": "/opt/iw/tm5/var/consul",`	Directory to store the Consul service data
`"encrypt": "4RTZ5ttYY6RwIYX28XWNPw==",`	Secret key shared between cluster agents
`"log_level": "WARN",`	Level of logging
`"enable_syslog": true,`	Let logging in `syslog`
`"disable_update_check": true,`	Prohibit to check updates for Consul
`"leave_on_terminate": false,`	If true, then receiving SIGTERM, sends an exit message and leaves the cluster in standard mode. Default values: for server – `false` , for client – `true`
`"skip_leave_on_interrupt": true,`	If false, then receiving the signal of interruptions (e.g, SIGINT) leaves the cluster in standard mode. Default values: for server – `true` , for client – `false`
`"rejoin_after_leave": true,`	If `true` , then joins to cluster upon startup
`"limits": {`	Limit section
`"http_maxconns_per_client": 500`	Maximum number of HTTP(S) connections from one client
`},`	

Content	Description
`"retry_join": "0.0.0.0",`	In case of distributed installation contains the list of servers, which should be connected to
`"ui_config": {`	Web interface configuration section
`"enabled": false`	Access to web interface (prohibited by default)
`},`	
`"client_addr": "0.0.0.0"`	IP of a client with open web interface access
`}`	

Contents of **`iwtm-consul.service`** unit file

Code	Description
`[Unit]`	Section defining daemon metadata and its settings for interaction with other daemons
`Description=Consul Service discovery agent`	Daemon name
`Requires=network-online.target`	Services cannot operate without `network-online.target`
`After=network-online.service`	Daemons that will be run before the current daemon is started
`[Service]`	Daemon start setting section
`StandartOutput=syslog`	Redirecting standard output to `syslog`
`StandartError=syslog`	Redirecting standard error to `syslog`
`Type=simple`	Daemon start type. `simple` – daemon starts and switches to waiting mode on the console
`User=iwtm`	User name on behalf of which daemon is started
`Group=iwtm`	User group name

Code	Description
`SyslogIdentifier=iwtm-consul`	Defines process name for log prefix rows, which are sent to logging system or to core log buffer
`PermissionsStartOnly=true`	Starting commands from ExecStartPre on behalf of the **`root`** user
`ExecStartPre=/opt/iw/tm5/bin/consul validate /opt/iw/tm5/etc/consul`	Full path and command arguments which should be completed before starting the main process
`ExecStart=/opt/iw/tm5/bin/consul agent $OPTIONS -config -dir= /opt/iw/tm5/etc/consul`	Full path and command arguments which should be completed to start daemon. The command is to be run on behalf of the user defined in `User`
`ExecReload=/bin/kill -s SIGHUP $MAINPID`	The command restarts daemon configuration, if it is accessible. The command is to be run on behalf of the user defined in `User`
`KillSignal=SIGINT`	The command stops daemon's work forcefully
`TimeoutStopSec=5`	Period of time within which the system waits for daemon to stop, before labeling it as inaccessible or stopped forcefully
`[Install]`	Defining daemon's behaviour, if it is enabled or disabled
`WantedBy=multi-user.target`	Start this daemon, when the system is loading in a multi-user mode

4.12 Secure Deployment Recommendations

Traffic Monitor components use various network ports on the System servers.

> **Note:**
>
> For more information about component sets and templates on the System servers, see *InfoWatch Traffic Monitor. Installation guide. System Deployment Schemes and Installation Types*.
>
> For information about Traffic Monitor servers processes, see *Traffic Monitor Server Processes*.

To prevent unauthorized access to the components, it is recommended to configure a firewall. Only the connections that are necessary for the operation of the components should be allowed.

4.12.1 Components ports

Port	Interaction between components		Port's Function
	Source	**Target**	
Unique ports necessary for Traffic Monitor work			
TCP 9100	Device Monitor server	Traffic Monitor server	Transfer of shadow copies from Device Monitor for analysis
	Data Discovery server	Traffic Monitor server	Transfer of objects from Data Discovery for analysis
TCP 40731	Traffic Monitor Server with the "Interceptors" component	Data Storage server	Transfer of data for storing in Data Storage
	Traffic Monitor Server with the "Web-console" component	Data Storage server	Receiving data from Data Storage to access them in the web interface
TCP 30050	Traffic Monitor Server	Data Analysis Service server	Text data protoclustering using Data Analysis Service
TCP 9101	Server with a special connector	Traffic Monitor server	Transfer of objects for analysis using Push API Special connector using the Push API program interface can be created for transferring objects from servers via unsupported protocols, e.g. designed by client
	Lotus Domino adapter	Traffic Monitor server	Transfer of objects for analysis using Lotus Domino adapter
	MS Lync adapter	Traffic Monitor server	Transfer of objects for analysis using MS Lync adapter
	Smart Logger adapter	Traffic Monitor server	Transfer of objects for analysis using Smart Logger adapter
	MS ActiveSync adapter	Traffic Monitor server	Transfer of objects for analysis using ActiveSync adapter

Port	Interaction between components		Port's Function
	Source	Target	
Ports necessary for Traffic Monitor work in case of distributed installation			
TCP 1521	Traffic Monitor server	Traffic Monitor server DB	Connection to the Oracle Traffic Monitor database
TCP 5433	Traffic Monitor server	Traffic Monitor server DB	Connection to the PostgreSQL Traffic Monitor database
TCP 2025	Traffic Monitor server	Traffic Monitor server	SMTPD service
TCP 4301/2525/6338/6559	Traffic Monitor server	Traffic Monitor server	Sniffer service
TCP 8300	Traffic Monitor server	Traffic Monitor server	Consul (RPC) service
TCP 8301	Traffic Monitor server	Traffic Monitor server	Consul (Serf LAN) service
UDP 8301	Traffic Monitor server	Traffic Monitor server	Consul (Serf LAN) service
TCP 8302	Traffic Monitor server	Traffic Monitor server	Consul (Serf WAN) service
UDP 8302	Traffic Monitor server	Traffic Monitor server	Consul (Serf WAN) service
TCP 8400	Traffic Monitor server	Traffic Monitor server	Consul (CLI RPC) service
TCP 8500	Traffic Monitor server	Traffic Monitor server	Consul (HTTP API) service
TCP 8600	Traffic Monitor server	Traffic Monitor server	Consul (DNS interface) service
TCP 9997	Traffic Monitor server	Traffic Monitor server	Consul service connection to ICAP

Port	Interaction between components		Port's Function
	Source	Target	
TCP 9998	Traffic Monitor server	Traffic Monitor server	Consul service connection to Analysis
TCP 9999	Traffic Monitor server	Traffic Monitor server	Consul service connection to Messed
TCP 9090	Traffic Monitor server	Traffic Monitor server	Bookworm service
TCP 9091	Traffic Monitor management console	Traffic Monitor server	Sample Compiler service
TCP 9093	Traffic Monitor server	Traffic Monitor server	Blackboard service
TCP 9095	Traffic Monitor server	Traffic Monitor server	Licensed service
TCP 9096	Traffic Monitor server	Traffic Monitor server	Adlibitum service
TCP 9097	Traffic Monitor management console	Traffic Monitor server	System Check service
TCP 9099	Traffic Monitor server	Traffic Monitor server	Agent service
TCP 9102	Traffic Monitor server	Traffic Monitor server	Tech Tools service
TCP 9250	Traffic Monitor server	Traffic Monitor server	X2X service
TCP 9306	Traffic Monitor management console	Traffic Monitor server DB	Indexing service
TCP 9310	Traffic Monitor management console	Traffic Monitor server DB	Indexing service

Port	Interaction between components		Port's Function
	Source	Target	
TCP 9987	Traffic Monitor server	Traffic Monitor server	CAS service
TCP 9988	Traffic Monitor server	Traffic Monitor server	Luaengined service
TCP 9989	Traffic Monitor server	Traffic Monitor server	PAS service
TCP 16888	Traffic Monitor server	Traffic Monitor server	Qmover service
TCP 9103	Traffic Monitor server	Traffic Monitor server	Image_autoling service
TCP 9104	Traffic Monitor server	Traffic Monitor server	Text_autoling service
TCP 1111	Traffic Monitor server	Traffic Monitor server	Prometheus service (monitoring)
TCP 1112	Traffic Monitor server	Traffic Monitor server	Node-exporter service (monitoring)
TCP 1113	Traffic Monitor server	Traffic Monitor server	Consul-exporter service (monitoring)
TCP 1114	Traffic Monitor server	Traffic Monitor server	Postgres-exporter service (monitoring)
TCP 1115	Traffic Monitor server	Traffic Monitor server	Alert-manager service (monitoring)
TCP 1116	Traffic Monitor server	Traffic Monitor server	Statsd-exporter service (monitoring)
TCP 1117	Traffic Monitor server	Traffic Monitor server	Gearman-exporter service (monitoring)
TCP 1118	Traffic Monitor server	Traffic Monitor server	Process-exporter service (monitoring)
Standard ports for InfoWatch products interaction			

Port	Interaction between components		Port's Function
	Source	Target	
TCP 443	Device Monitor Server	Traffic Monitor server DB	Receiving Traffic Monitor policies
	Vision Server	Traffic Monitor server DB	Connection with Traffic Monitor DataExportAPI
	Activity Monitor Server	Traffic Monitor server DB	
	Prediction Server	Traffic Monitor server DB	
	Data Explorer Server	Traffic Monitor server DB	
TCP 5433	Traffic Monitor server	Remote DB server	The remote Traffic Monitor database in case of using it
Ports for integration with external services			
TCP 2025/587	Mail server	Traffic Monitor server	Simple Mail Transfer Protocol (SMTP)
	Traffic Monitor server	Mail server	
UDP 53	Traffic Monitor server	DNS server	Domain Name System (DNS)
UDP 123	Traffic Monitor server	NTP server	Network Time Protocol (NTP)
TCP 389	Traffic Monitor server	AD server	Lightweight Directory Access Protocol (LDAP)
	Device Monitor server	AD server	
TCP 636	Traffic Monitor server	AD server	Lightweight Directory Access Protocol (LDAPS)
TCP 3268	Traffic Monitor server	AD server	Microsoft Global Catalog

Port	Interaction between components		Port's Function
	Source	Target	
TCP 3269	Traffic Monitor server	AD server	Microsoft Global Catalog (LDAPS)
UDP 514	Traffic Monitor server	SIEM server	Integration with SIEM via the syslog protocol
TCP 1521	SIEM server	Traffic Monitor server DB	Integration with SIEM (Oracle Traffic Monitor DB)
TCP 5433	SIEM server	Traffic Monitor server DB	Integration with SIEM (PostgreSQL Traffic Monitor DB)
TCP 1344	Proxy server	Traffic Monitor server	Internet Content Adaptation Protocol (ICAP)
Remote management and administration			
TCP 22	Automated workplace	Traffic Monitor server	Configuring the server via SSH protocol
TCP 443	Automated workplace	Traffic Monitor Management console	Connection to Traffic Monitor Management console
TCP 3000	Automated workplace	Traffic Monitor server	Connection to the Grafana console (monitoring system)

4.13 Configuring Verdict Management

By default, you cannot manage verdict for Copy rules in Data protection policies, and value of **Assign verdict to event** field of **Action if rule triggered** block is set to *Allow*.

If you want the System to assign another verdict to an event in case of a triggered rule, **enable verdict management**:

1. Connect to the database used by Traffic Monitor server.
2. Open `setting` table of the database.
3. Change the value of `allow_change_verdict_copy` parameter from `0` to `1`.

In Management Console, in the Copy rule for which you need to configure the verdict, you will be able to select a value of **Assign verdict to event** field: *Allow*, *Block* or *Quarantine*.

To disable verdict management, set `0` for `allow_change_verdict_copy` parameter.

Note:

In case you specify a verdict and then disable verdict management in `setting` table, changing verdict for this rule will be unavailable.

5 Settings for automatic deletion of Data Discovery events

Traffic Monitor applies a special anti-garbage filter to Data Discovery events. **By default**, the filter deletes Data Discovery events if they haven't triggered any policy or no protected objects have been found in them.

You can configure deletion of Data Discovery events in the `/opt/iw/tm5/etc/luaengined.conf` configuration file.

The anti-garbage filter modes are defined by the `DeleteDDEventsWithoutPolicy` parameter:

- `true`, to save only those events to the Traffic Monitor database that have triggered a policy,
- `false` (selected by default), to save only those events that contain protected objects or have triggered a policy.

If you do not want the anti-garbage filter to delete Data Discovery events, then in the `DisableDeleteDDEventsForServers` parameter, specify Data Discovery servers that should be added to exceptions.

To apply changes:

1. Save the file.
2. Restart the `iw_luaengined` service: `iwtm restart luaengined`

Example:
You do not want the anti-garbage filter to apply to events from MainDD and DDcompany servers. For other servers, you want to save only those events that contain triggered policies.

Parameter values for the luaengined.conf example configuration file:

```
"DeleteDDEventsWithoutPolicy": true,
"DisableDeleteDDEventsForServers": ["MainDD", "DDcompany"],
```

6 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 installer. For more details on the installation see *InfoWatch Traffic Monitor. Installation and Configuration Guide* document.

If InfoWatch Traffic Monitor system is deployed on few servers using the installer and installation templates, the monitoring subsystem will be automatically configured and detectors will be in accordancy with the templates used.

You can also use *Configuring Indicators Manually*.

6.1 Monitoring Subsystem for Distributed Architecture

> **Warning!**
>
> If InfoWatch Traffic Monitor system is deployed on few servers using installer and installation templates, the monitoring subsystem will be automatically configured in accordance with installation templates used.

Monitoring configuration includes the following tasks:

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

6.1.1 Configuring Connection to Device Monitor

To configure connection to Device Monitor server:

1. Edit `/opt/iw/tm5/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 `/opt/iw/tm5/etc/nagios/iwmon/iwmon-services-dm.cfg` file uncomment `service` section.
- In `/opt/iw/tm5/etc/nagios/iwmon/iwmon-commands.cfg` file uncomment `Check Dm server` section.
- Restart nagios process:
  `systemctl restart iwtm-nagios`

6.1.2 Configuring Indicators Manually

Enabling and disabling indicators is being performed in the following file of the `/opt/iw/tm5 /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.

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:

```
systemctl restart iwtm-nagios
```

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 `/opt/iw/tm5/etc/nagios/iwmon/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 Notifications

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

For e-mail notifications to be sent only for selected indicators:

1. Go to the Nagios subsystem directory:
   `cd /opt/iw/tm5/etc/nagios/iwmon`
2. Open the **iwmon-services.cfg** configuration file:
   `mcedit /opt/iw/tm5/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 sending notifications;
   - 0 – to disable sending notifications.
     If there is no `notifications_enabled` parameter in the configuration file, add this parameter manually.

- Save changes.
- Set up a connection to one of the mail servers:
  - the built-in local Traffic Monitor mail server with anonymous access (Posfix or Exim) OR

- an external mail server without encryption.

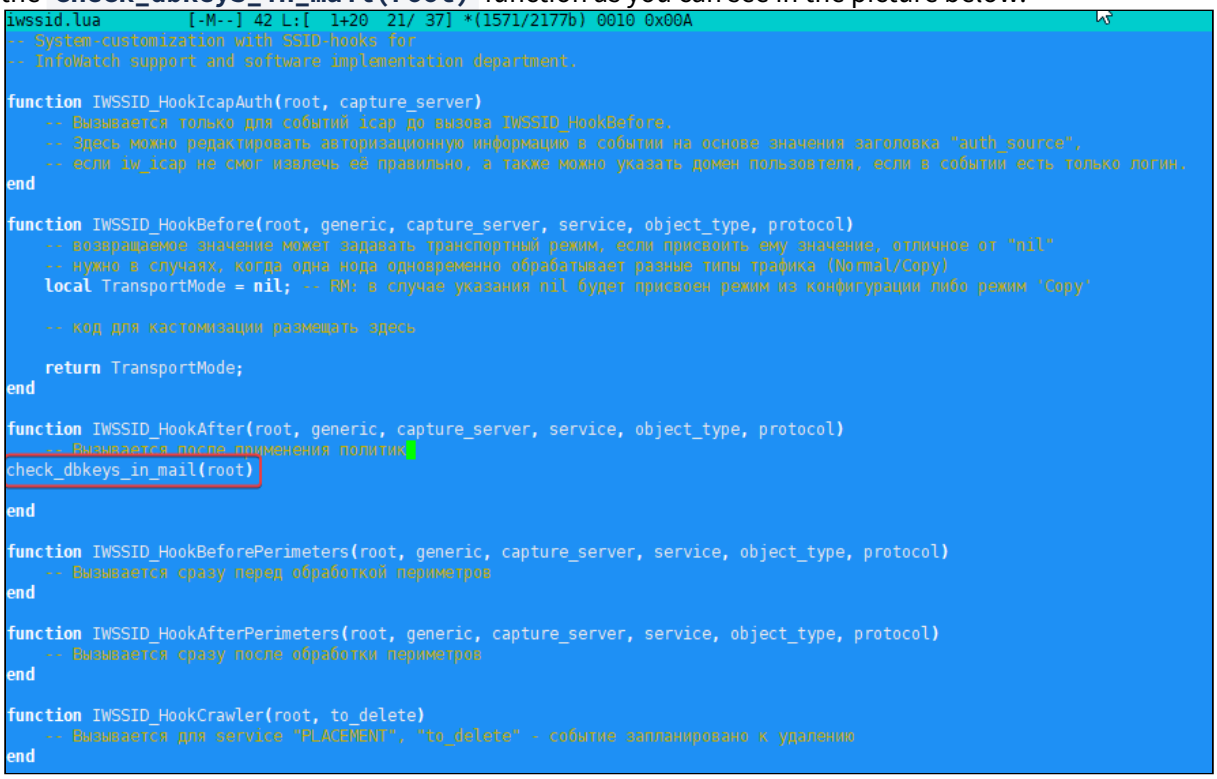
7 Using a database unloading for automatic recipient validataion

Traffic Monitor can use a database unloading to control sending data by email. The database unloading must meet the requirements (see *InfoWatch Traffic Monitor. User Guide. Recommendations on Preparing Unloadings*). The last column of each row in the unloading must contain the email address to which data of this row is allowed to be sent. The fields of the last column are considered keys and the unloading is not indexed by them. This solution allows you to protect a large amount of data without manually creating a lot of protected objects and policies. In the *Blocking* transport mode (the in-line mode), Traffic Monitor allows you to block sending emails with protected data or send them to quarantine.

By default, after Traffic Monitor installation, this functionality is disabled.

To enable the ability to use the database unloading for recipient validation:

1. In the `/opt/iw/tm5/etc/scripts/iwssid.lua` file, add a command to call the `check_dbkeys_in_mail(root)` function as you can see in the picture below.



2. After you save changes, check permissions with the command:

```
ls -la /opt/iw/tm5/etc/scripts/iwssid.lua
```

Example where the correct permissions are displayed:

```
-rw-r--r--. 1 iwtm iwtm 2181 jul 24 09 : 43 /opt/iw/tm5/etc/scripts/iwssid.lua
```

3. If the permissions have been changed and do not match the example above, use the following command to edit the permissions:

```
chown -R iwtm:iwtm /opt/iw/tm5/etc/scripts/iwssid.lua
```

4. Restart Traffic Monitor services with the command:

```
iwtm restart
```

Important!

Please, keep in mind that parameters of the `cas.conf` configuration file affect the operation with database unloadings:

- `MinWords` (`10` by default). The System creates an event with a violation if an email with an impermissible recipient contains at least 10 words, including words which satisfy detection conditions. Otherwise, the System does not detect a protected object and creates an event without a violation;
- `MaxCheckLimit` (`0` by default). If the value is greater than zero, the System continues searching until it finds the specified maximum number of lines with unique keys (or number of unique lines in case the unloading does not contain keys). The parameter is available only for *All words in one cell following each other in any order* search type and if optimization if disabled (`"StopOnLimitExceed": false`).

For details, see *InfoWatch Traffic Monitor. Configuration Files Guide*.

To disable the functionality:

1. In the `/opt/iw/tm5/etc/scripts/`**`iwssid.lua`** file, delete the command that calls the **`check_dbkeys_in_mail(root)`** function.
2. Restart Traffic Monitor services with the command:

```
iwtm restart
```

8 Database Administration

This chapter contains information on administrating:

- Oracle;
- PostgreSQL.

DB statistics information is available in *Compiling DB statistics* KB article.

8.1 Oracle

This chapter contains instructions on Oracle administration:

- Tablespaces in InfoWatch Traffic Monitor database;
- Managing Daily Tablespaces;
- Load statistics of Daily Tablespaces;
- Database Backup;
- Database Routinely Maintenance;
- Database Logging.

> **Note:**
>
> To change the DB user password, see the *Changing the Preset Password* article.

8.1.1 Tablespaces in InfoWatch Traffic Monitor database

General information

InfoWatch Traffic Monitor data are stored in DB as tablespaces (TS). There are two types of Traffic Monitor tablespaces:

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.)

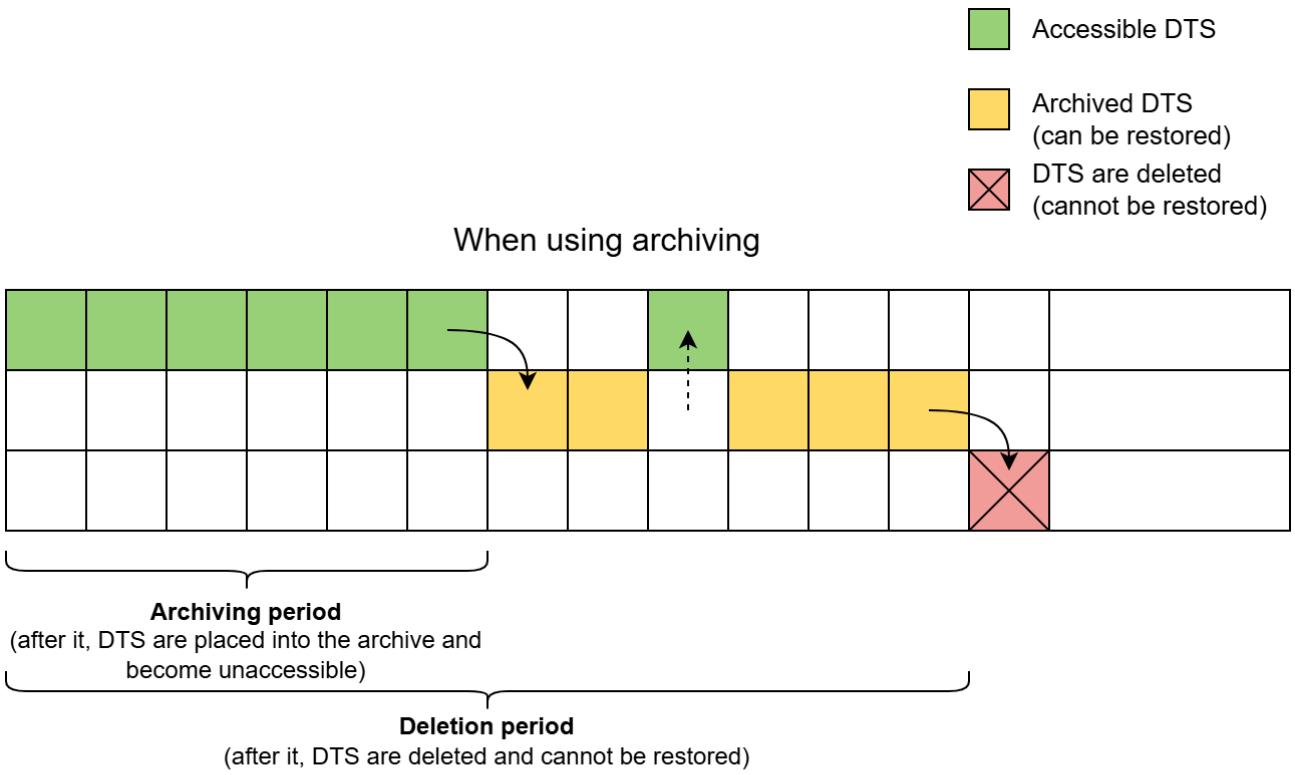
All data about the objects intercepted on a particular day (according to UTC+0) is stored in three daily tablespace (DTS) of the folowing types:

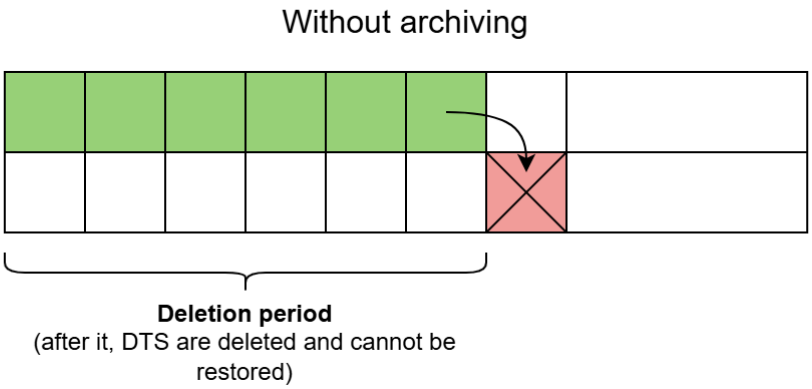
- Events without violations;
- Events with violations;
- Other (screenshots).

Daily tablespaces are created every day in such a way that the database always has DTS for the next six days, excluding the current day. All DTS automatically get the *IWTM_YYYYMMDD_X* name, where X is the DTS number (the TBS_ID value from the TBS_LIST table). The tablespace type is defined by the TBS_TYPE value: 0 – No Violations, 1-Violation, 2 - Other (screenshots).

Lifecycle of DTS can be divided into 3 stages:

1. **Ordinary storing**
   Initially, DTS are stored in the database and are in operational access. If you use Data Storage, then the event contents from this DTS such as attachments, screenshots, audio files, and so on, are stored there.
2. **Storing in an archive** (optional)
   If you need to store events for a long time, but do not need operational access to them, you can archive them before deleting.
   For this, enable automatic archiving of DTS. After the **archiving period**, they will be archived and will become unavailable. If neccesary, you can restore them (the dashed arrow on the diagram).
3. **Deleting**
   To avoid disk overflow, you can delete DTS which you do not need to store.
   For this, enable automatic deleting of DTS. After the **deletion period**, they will be deleted without the possibility of restoring.





By default, automatic archiving and deletion are disabled. You can enable them during the installation or after it. Also, you should set the DTS **archiving period** and/or the DTS **deletion period**. For details, see articles on archiving and deletion.
Configure **archiving period** and **deletion period** so that you always have enough free space on the disks, which store DTS, and they do not overflow.

If you need to archive/restore/delete a single DTS, you can do it manually in the Traffic Monitor web interface. See *InfoWatch Traffic Monitor. User Guide. Managing tablespaces*.
If the web interface is unavailable, use the **iw_space_manager** service utility for this (see *Managing Daily Tablespaces with the Console Utility*). Last operate with DTS manually in the database.

Storing

The main tablespace is stored in the `/u02/oradata` catalogue by default.
The daily tablespaces are stored in the `/u02/oradata1` catalogue by default.
For details on placing DTS, see *Configuring Location of Files within File System*.

On storage modes, see *Configuring Storage Modes for Tablespace Files*.

Archiving

Archiving process consists of:

- disconnecting DTS from the database;
- moving DTS to the specified catalogue (by default: `/u02/arch`).

You should place this catalogue on the separate disk to free up space on the hard drive with operational data and avoid its overflow.
When using Data Storage, binary data of the archived DTS will be moved to the Data Storage slow disk.

During archiving, data is not compressed. So, on the allocated disk, it will take about the same place. You can estimate the size of the disk for archived DTS based on how much place DTS take in operational access in their storage directories (by default: `/u02/oradata1` in the DB and `/opt /dsdata/_seaweedfs` in Data Storage).

Archiving is described in details in the *Archiving Daily Tablespaces* section.

To access the archived DTS data, you need to restore it. See *Restoring Daily Tablespaces*.

Deleting

When automatic deletion is enabled, the System deletes DTS older than the deletion period. You specify its value separately for each DTS type: events without violations, events with violations, other (screenshots).

For details on deletion methods, see *Deleting Daily Tablespaces*.

8.1.2 Managing Daily Tablespaces

In this section:

- Configuring Location of Files within File System;
- Configuring Storage Modes for Tablespace Files;
- Archiving Daily Tablespaces;
- Restoring Daily Tablespaces;
- Deleting Daily Tablespaces;
- Managing Daily Tablespaces with the Console Utility.

Configuring Location of Files within File System

By default, the installation program (see *InfoWatch Traffic Monitor. Installation Guide*) sets the usage of one directory for storing daily tablespaces: `/u02/oradata1`.

> **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

Configuring Storage Modes for Tablespace Files

There are three modes of storing data in DB:

- **Normal** – switching to the following partition (when it is specified) happens after the previous one is overflow.
- **Fast/Slow disks** – dividing pools into fast and slow ones. Recent data are to be kept in fast pool. In a number of days specified, the System relocate them to the slow ones. Slow pool operates in Normal mode.
- **Rotate** – switching to the following partition happens every day once the previous one is overflow.

You select storage mode when installing Traffic Monitor. By default, the installer offers you **Normal** mode. You can change the storage mode later.

By default, DTS are stored in the `/u02/oradata1` directory.

> **Note:**
>
> Modes described in this article relate to data stored in DB only. Changing mode does not affect data stored in Data Storage.

Fast/slow disks Mode

The System moves data from the fast disk to the slow one every night. If you are switching from **Normal** mode to **Fast/slow** mode, you store a large amount of DTS on your old partition, and you specify the old partition as a fast disk, then data transfer may take a long time.
If you will use the old disk as a fast one, before switching mode make sure that the following conditions are met:

- The new partition size is not less than the old one size. So, there is enough space for transferring all DTS from the old partition;
- There is free space in the old partition not less than the largest tablespace that will be transferred to the slow disk.

The System creates DTSs every day in such a way that the database always has DTS for the next six days, excluding the current day. So, if when switching from **Normal** mode to **Fast/slow** mode, you specify a new partition as a fast disk, then, for first seven days, the System will save events to the already created DTS on the slow disk. In this case, the System will create new DTSs on the fast disk.

For configuring **Fast/slow** mode, we will use the new patrtition `/u03/oradata/` as a slow disk and the old partition `/u02/oradata1/` as a fast one.

To configure "Fast/slow" storage mode (fast and slow drives):

1. Edit the `/etc/fstab` file to automatically mount a new partition to `/u03:`
   `/dev/sdd1 /u03/ ext4 defaults 1 2`
2. Create the `oradata` folder:
   `mkdir /u03/oradata`
3. Change user:
   `chown -R oracle:oinstall /u03`
4. Log into the database:
   `su - oracle`
   `sqlplus iwtm@iwtm`
5. Specify the storage period on fast drives:
   `exec pkg_part.set_fast_days(7);`
6. Specify the path to the fast drive:
   `exec pkg_part.set_fast_path('/u02/oradata1/',1);`
7. Specify the path to the slow drive:
   `exec pkg_part.set_df_path('/u03/oradata/',1);`
8. If needed, you can use several slow drives. The data will be recorded to the next slow drive when the previous is full. To add the slow drives specify a new path:
   `exec pkg_part.set_df_path('/u03/oradata2/',2);`
9. Specify the total amount of slow drives:
   `exec pkg_part.set_df_path_cnt('2') ;`
10. Change the mode to fast-slow drives:
    `exec pkg_part.set_filesys_type('fast/slow');`
    The data will be transferred from fast drives to slow ones during night job.
11. Apply changes:
    `commit;`
12. To run the process of moving files manually:
    `exec iwtm.pkg_part.move_fast_tablespaces_to_slow();`

> **Note:**
>
> Few slow drives can be used in the System.

> **Note:**
>
> In **Fast/slow** mode, the screenshot tablespaces are stored in slow partitions only.

Rotate Mode

To configure "Rotate" storage mode (everyday rotation):

1. Mount the partition and make sure that it can be mounted automatically on reboot
2. Create the `oradata` folder:
   `mkdir /u03/oradata`
3. Change user:
   `chown -R oracle:oinstall /u03`

4. Log into the database:
   `su - oracle`
   `sqlplus iwtm@iwtm`
5. Add a path to the second partition:
   `exec pkg_part.set_df_path('/u03/oradata/',2);`
6. Specify a new number of paths:
   `exec pkg_part.set_df_path_cnt(2);`
7. Apply changes:
   `commit;`
8. Switch to **rotate** mode:
   `exec pkg_part.set_filesys_type('rotate');`

```
 SQL>select * from setting where setting like 'df_path%';
select * from setting where setting like 'df_filesys%';

setting | value | editable
------------+---------------+----------
df_path1 | /u02/oradata1/ | 1
df_path2 | /u03/oradata/ | 1
df_path_cnt | 2 | 1
df_filesys_type | rotate | 1
```

> **Note:**
>
> Parameters of modes are stored in the `setting` table of the database. Their specifics are described in the Knowledge Base article *Tablespaces data storage settings. Data storage partition*.

Archiving Daily Tablespaces

Archiving process consists of disconnecting DTS from the database and moving them to the specified catalogue (by default: `/u02/arch`). You should place this catalogue on the separate disk to free up space on the hard drive with operational data and avoid its overflow. You can restore this data if necessary.

In the System, there are following ways of archiving DTS:

- Automatically after the specified period is expired (see *Automatic Archiving of Daily Tablespaces*);
- Manual archiving of single DTS:
  - In the Traffic Monitor web interface. See *InfoWatch Traffic Monitor. User Guide. Managing tablespaces*;
  - Using the console utility of the **iw_space_manager** service (see *Managing Daily Tablespaces with the Console Utility*);
  - In the database (see *Manual Archiving of Daily Tablespaces in the Database*).

If you need to archive a single DTS, we recommend to do it in the Traffic Monitor web interface. If the web interface is unavailable, use the **iw_space_manager** service utility. Last use manual archiving of DTS in the database.

Archiving when using Data Storage

If you use Data Storage, then, when archiving DTS, binary data will be moved to the Data Storage slow disk.
If the slow disk is not connected, then, in Traffic Monitor web interface, archived daily tablespace will have the "*Archived*" status. But in this case, binary data of DTS will be stored on the fast disk of the Data Storage server,

inside the directory for placing binary data. You specify this directory when installing the storage (by default: `/opt/dsdata/_seaweedfs`).

You specify the path to the slow disk when installing Data Storage. For details, see *InfoWatch Traffic Monitor. Installation Guide. Installing Platform*.
To add the path to the Data Storage slow disk after installing the storage:

1. Create a directory and mount the slow disk to it:

   ```
   mkdir -p /mnt/slowdisk
   mount /dev/<your_slowdisk> /mnt/slowdisk
   ```

2. Set a user and access permissions for the directory, where you have mounted the slow disk:

   ```
   chown 1000 /mnt/slowdisk
   chmod 700 /mnt/slowdisk
   ```

3. Open the Data Storage deployment for editing. For this use the command:

   ```
   kubectl -n infowatch edit deployment datastorage-<node_label>
   ```

   where `<node_label>` (hereafter) is the label of the node where the storage is installed. For the central node or, if the storage is installed not in the cluster of Platform products, use the label `central`. For the office node, the label is specified during installation (`office` by default).
4. Add the following lines to the `containers` -> `volumeMounts` section:

   ```
       - mountPath: /var/lib/dataslow
         name: datastorage-dataslow-host-volume-<node_label>
   ```

5. Add the following lines to the `volumes` section:

   ```
       - hostPath:
           path: /mnt/slowdisk
           type: ""
         name: datastorage-dataslow-host-volume-<node_label>
   ```

6. Save the changes and exit the editor.

Automatic Archiving of Daily Tablespaces

By default, automatic DTS archiving is disabled. To make the System archive DTS according to schedule, enable this function and set the time after which DTS must be archived. Details are described further.
Every day, at 00:00 server time, the **iw_space_manager** service procedure will archive DTS that satisfy the following condition:

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

So, all DTS older than the specified value will be archived.

Warning!

If months or years are used as the time interval, we recommend using the maximum value of the interval in calculations. For a month – 31 days. For a year – 366 days. For example, to archive DTS older than 4 years, specify the interval 366 * 4 = 1464 days.

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

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

The `Oracle` user should be an owner of the catalogue.

In case the catalogue has been set improperly, reset it with 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;
/
```

- 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;
/
```

- 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 automatic archiving 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. This number should be smaller than the set number of days before deleting the daily tablespace (see *Deleting Daily Tablespaces*).

Manual Archiving of Daily Tablespaces in the Database

It is recommended to archive single DTS via web interface or using the **iw_space_manager** utility.

The order of archiving daily tablespaces manually in the database is described below.

> **Important!**
>
> In this method of archiving, data stored in the Data Storage are not archived.

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 scheme from which it was disconnected (even if this scheme was updated). The restoration of the tablespace after total database scheme reinstallation is impossible.

In the System, there are the following ways of restoring DTS:

- In the Traffic Monitor web interface. See *InfoWatch Traffic Monitor. User Guide. Managing tablespaces*;
- Using the console utility of the **iw_space_manager** service. See *Managing Daily Tablespaces with the Console Utility*;
- In the database – this method is described below. It is recommended to use this method last.

Moving data files

To restore a daily tablespace, 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 a daily tablespace during `IWTM_ADD_PARTS` and `IWTM_DELETE_TABLESPACES` jobs. This may cause the data loss.

When the System restores an archived tablespace, by default it moves its data files to a standard directory for tablespaces. In case you need the System to store files in the archive storing directory (for example, to increase recovery performance thereby), go to `setting` table in the database and replace the value of `move_restore_datafile` parameter with `0`.

1. On behalf of the owner of the database scheme, 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

In the System, there are the following ways of deleting DTS:

- Automatic, according to schedule. Described below.
- Manual deleting of single DTS:

- In the Traffic Monitor web interface. See *InfoWatch Traffic Monitor. User Guide. Managing tablespaces*;
- Using the console utility of the **iw_space_manager** service. See *Managing Daily Tablespaces with the Console Utility*;
- In the database. Described below.

We recommend using scheduled deletion. Otherwise, disk overflow can occur or the big amount of data for deletion can build up. It will result in increasing the time for running this procedure in future and consequently increasing the idle time of the Traffic Monitor Server.

> **Warning!**
>
> Deleting tablespaces cannot be undone. If you complete the operation, you will not be able to restore the deleted data.
> The System deletes both DTS data from the storage directory (by default, `/u02/oradata1`, or `/u02/arch` for the archived ones) and information on DTS from the database. If you use Data Storage, data from it will be deleted as well.
>
> While deleting tablespaces, access to the corresponding tables is closed. For this reason, log files of the **iw_deliver**, **iw_x2db**, **iw_updater** processes may contain database access errors. Once tablespaces are deleted, these processes automatically restore access to the database.

Automatic deletion

By default, automatic DTS deletion is disabled. To make the System delete DTS according to schedule, enable this function and set the time after which DTS must be deleted. Details are described further.
Every day, at 00:00 server time, the **iw_space_manager** service procedure will delete DTS that satisfy the following condition:

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

So, all DTS older than the specified value will be deleted.

> **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 DTS older than 4 years, specify 366*4=1464 days interval.

Enabling automatic deletion

Automatic deletion according to schedule is configured separately for each DTS type.
To enable it, set the deletion `delete_enabled` flag and specify the period of storing DTS `delete_period`.
For this, run the following scripts on behalf of the database scheme owner:

- For DTS storing objects with the *Violation* status:

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

```
end;
/
```

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

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

- 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 automatic deletion is enabled (to disable, specify 0 instead of 1);
D is a number of days at the end of which the DTS will be deleted by the System. This number should be larger than the set number of days before archiving daily tablespaces (see *Automatic Archiving of Daily Tablespaces*).

Deleting daily tablespaces with a script

As well, you can configure automatic deletion of daily tablespaces, use the **/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-oracle.sh** script. You can use the following commands:

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

Example:

To enable automatic deletion of the DTS, that store objects with the *"No violation"* status and are older than 15 days, run the commands:

```
/opt/iw/tm5/bin/dbconf-iwdrop-oracle.sh set noviolation 15 [-v]
/opt/iw/tm5/bin/dbconf-iwdrop-oracle.sh enable noviolation [-v]
```

Manual deletion in the database

If you need to immediately launch the procedure of automatic DTS deletion (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 on behalf of the database scheme owner:

```
begin
     iwtm.pkg_part.delete_tablespaces();
end;
/
```

As a result, the System will delete DTS for which scheduled deletion is enabled and the period of storing is specified.

The command above affects data in DB only. If you use Data Storage, launch the procedure of automatic DTS deletion using the **iw_space_manager** service:

```
iw_space_manager cron
```

To delete one DTS by its identifier (ID), run the following script:

```
begin
     iwtm.pkg_part.delete_tablespace(ID);
end;
/
```

This command affects data in DB only. If you use Data Storage, delete DTS using the **iw_space_manager** service:

```
iw_space_manager tbs:delete <tbs_id>
```

Managing Daily Tablespaces with the Console Utility

To manage daily tablespaces via the command line, use the console utility that calls the **iw_space_manager** service. The service is available for the **iwtm** user and is enabled by default.

When using Data Storage, the **iw_space_manager** service archives/restores/deletes binary data from the storage as well.

Commands and parameters of the service:

Command	Description
`tbs:archive [options] [--] <id>`	Starts archiving a daily tablespace with its ID specified. An example on how to archive a daily tablespace with ID=123: `iw_space_manager tbs:archive 123`
`tbs:create <type> <capture>`	Creates a daily tablespace with the following data specified: • type: 0 – no violation, 1 – violation, 2 – screenshots • creation date in the YYYY-MM-DD format An example on how to create a new daily tablespace with violations on September 1, 2023: `iw_space_manager tbs:create 1 2023-09-01`
`tbs:delete [options] [--] <id>`	Deletes a daily tablespace with its ID specified
`tbs:get [options]`	Gets the list of existing daily tablespaces. Additional parameters: • `--limit=LIMIT` – sets the maximal number of items to display on the screen • `--offset=OFFSET` – hides the first N items (N=0 by default) • `--order=ORDER` – sorts the daily tablespace list by: ASC – daily tablespace name, DESC – daily tablespace creation date An example on how to get a list of 20 daily tablespaces sorted by the creation date: `iw_space_manager tbs:get -- limit=20 --order=DESC`
`tbs:restore [options] [--] <id>`	Restores an archived daily tablespace with its ID specified. An example on how to restore a daily tablespace with ID=123 from an archive: `iw_space_manager tbs:restore 123`
	With all the commands listed above, you can use the following common parameters: • `-f, --force` – runs the command without the validation check in case of a database emergency. Enables you to perform operations on tablespaces where date of event interception coincides with today's date; • `--used-configs` – runs the command with the parameters from the configuration file; • `-p, --configpath [=CONFIGPATH]` – displays the configuration file path. By default, it is `opt/iw/tm5/etc` ; • `--force-config-load` – force loads the configuration file even if the query parameters are specified.

To get logs and debug messages, run the service with the parameters below:

- `-v` – displays usual logs;
- `-vv` – displays logs with extended detalization;
- `-vvv` – displays logs with full detalization.

To get a list of available commands, run the command:

```
iw_space_manager list
```

8.1.3 Load statistics of Daily Tablespaces

To analyze a load of daily tablespaces, you can use the `/opt/iw/tm5/bin/dbtools/tablespace_stat_oracle/tablespace_stat_oracle.sh` script. With its help, you can get the statistics on TBS content for the selected period. The script executes one of the six scenarios and in each case it collects different information. The scenarios are described in more detail *below*.

To display the information on the script usage:

1. Go to the directory where the script is located by running the command:
   `cd /opt/iw/tm5/bin/dbtools/tablespace_stat_oracle/`
2. Run the script without parameters by running the command:
   `./tablespace_stat_oracle.sh`

As a result, you will see the help information:

```
tablespace_stat.sh: usage: [ report_number ] [ -e ]

report_number:
1 - Period stats
2 - Period stats with count of objects
3 - Statistics on a given tbs id by event type
4 - Period stats by event type
5 - Period stats by person
6 - Statistics on a given person id

-e, --export : for export to csv
```

To use the script:

1. Go to the directory where the script is located by running the command:
   `cd /opt/iw/tm5/bin/dbtools/tablespace_stat_oracle/`
2. Run the script by running the command:
   `./tablespace_stat_oracle.sh <scenario_number> <-e>`
   where the scenario number is a digit from 1 to 6;
   `-e` or `--export` is a key that you can specify to unload the results of script execution in .csv format. The results will be displayed in the command line window, as well.
   Example of a command running the script:
   `./tablespace_stat_oracle.sh 1`
3. Specify the parameters depending on a scenario:
   - For scenarios 1, 2, 4, 5, 6 – a period for which the statistics should be displayed:
     a. Specify the lower bound of the period in the dd.mm.yyyy format and press **Enter**;
     b. Specify the upper bound and press **Enter**;

     > **Note:**
     >
     > If you do not specify values for bounds and just press **Enter** twice then, by default, statistics for last two weeks will be displayed.
     > If you specify only the lower bound then information for the period from the specified date to the current one will be displayed.

   - For scenario 3 – ID of the tablespace;
   - For scenario 6 – person's ID.

In case of unloading the results of script performing, the file is saved in the directory where the script is located. The file has the following name:
`report_<scenario_name>_<date>.csv`
where `<scenario_name>` has a value depending on the scenario number:

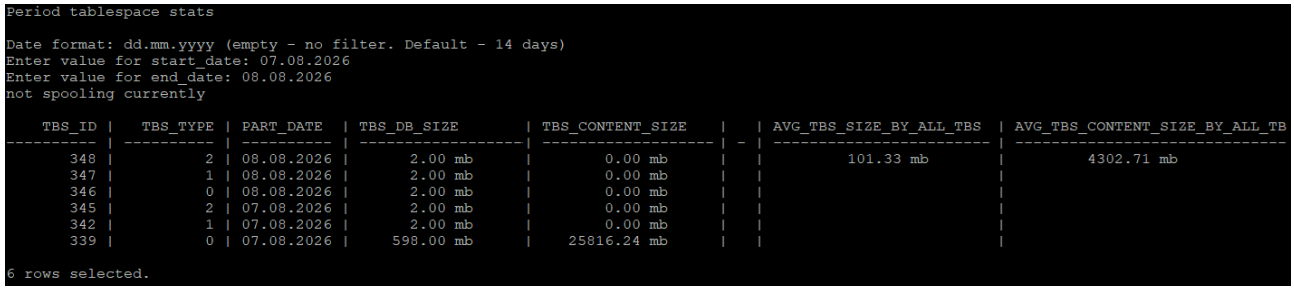
Scenario number	Scenario name	Short description
1	tbs_stat_period	Statistics for the period of time
2	tbs_stat_period_count	Statistics for the period of time including count of events in TBS
3	tbs_stat_by_tbs_id	Statistics on a particular TBS
4	tbs_stat_by_event_type	Statistics on event types for the period
5	tbs_stat_by_persons	Statistics on top-10 persons
6	tbs_stat_by_person_id	Statistics on a particular person

`<date>` - date of script execution. It has the `<yyyy-mm-dd_HH-mm-ss>` format.
Example of the unloading file name: `report_tbs_stat_period_count_2024-12-17_18-20-39.csv`

Scenarios of script execution

Scenario 1

As a result of scenario 1 execution, statistics on space that tablespaces take up for the period of time will be displayed.



```
Period tablespace stats

Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date: 07.08.2026
Enter value for end_date: 08.08.2026
not spooling currently

    TBS_ID |   TBS_TYPE | PART_DATE  | TBS_DB_SIZE       | TBS_CONTENT_SIZE    |   | AVG_TBS_SIZE_BY_ALL_TBS  | AVG_TBS_CONTENT_SIZE_BY_ALL_TB
---------- | ---------- | ---------- | ------------------| ------------------- | - | ------------------------ | ------------------------------
       348 |          2 | 08.08.2026 |       2.00 mb     |        0.00 mb      |   |         101.33 mb        |         4302.71 mb
       347 |          1 | 08.08.2026 |       2.00 mb     |        0.00 mb      |   |                          |
       346 |          0 | 08.08.2026 |       2.00 mb     |        0.00 mb      |   |                          |
       345 |          2 | 07.08.2026 |       2.00 mb     |        0.00 mb      |   |                          |
       342 |          1 | 07.08.2026 |       2.00 mb     |        0.00 mb      |   |                          |
       339 |          0 | 07.08.2026 |     598.00 mb     |    25816.24 mb      |   |                          |

6 rows selected.
```

The following information will be shown in columns:

TBS_ID	TBS identifier
TBS_TYPE	TBS type: 0 - No Violations 1 - Violation 2 - Other (screenshots)

PART_DATE	Date of TBS creation
TBS_DB_SIZE	TBS size in DB not including binary data
TBS_CONTENT_SIZE	Size of TBS binary data. If you use Data Storage, these data are stored there
AVG_TBS_SIZE_BY_ALL_TBS	Average size of one TBS for the specified period of time, not including binary data
AVG_TBS_CONTENT_SIZE_BY_ALL_TBS	Average size of binary data of one TBS for the specified period of time

Scenario 2

As a result of scenario 2 execution, statistics with count of objects on tablespaces for the period of time will be displayed.

```
Period tablespace stats with count of objects

Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date: 07.08.2026
Enter value for end_date: 08.08.2026
not spooling currently

    TBS_ID |   TBS_TYPE | PART_DATE  | TBS_STATUS    | COUNT_OBJECTS | TBS_DB_SIZE       | TBS_CONTENT_SIZE
---------- | ---------- | ---------- | ------------- | ------------- | ----------------- | ----------------------
       348 |          2 | 08.08.2026 | 0 - online    |             0 |       2.00 mb     |              0.00 mb
       347 |          1 | 08.08.2026 | 0 - online    |             0 |       2.00 mb     |              0.00 mb
       346 |          0 | 08.08.2026 | 0 - online    |             0 |       2.00 mb     |              0.00 mb
       345 |          2 | 07.08.2026 | 0 - online    |             0 |       2.00 mb     |              0.00 mb
       342 |          1 | 07.08.2026 | 0 - online    |             0 |       2.00 mb     |              0.00 mb
       339 |          0 | 07.08.2026 | 0 - online    |        100221 |     598.00 mb     |          25816.24 mb

6 rows selected.
```

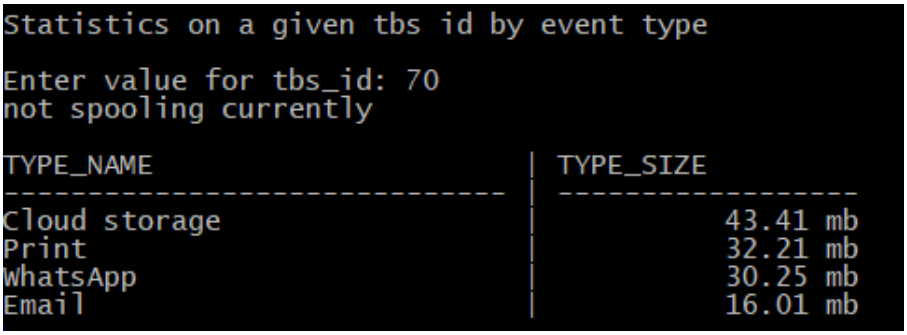
The following information will be shown in columns:

TBS_ID	TBS identifier
TBS_TYPE	TBS type: 0 - No Violations 1 - Violation 2 - Other (screenshots)
PART_DATE	Date of TBS creation
TBS_STATUS	TBS status: 0 - online (connected, in normal state) 3 - read only (only for reading) 5 - before exchange (before disconnecting for archiving) 7 - prepared offline (prepared to be disconnected for archiving) 9 - disconnected (disconnected before moving to archive) 10 - offline (archived and disconnected) 11 - plugged (plugged in before restoration) 13 - before update (before updating for restoration) 15 - after update (after updating for restoration)

	17 - before revert (before restoring from archive) 20 - restored (restored from archive)
COUNT_OBJECTS	Count of events in a TBS
TBS_DB_SIZE	TBS size in DB not including binary data
TBS_CONTENT_SIZE	Size of TBS binary data. If you use Data Storage, these data are stored there

Scenario 3

As a result of scenario 3 execution, statistics on a particular TBS will be displayed.

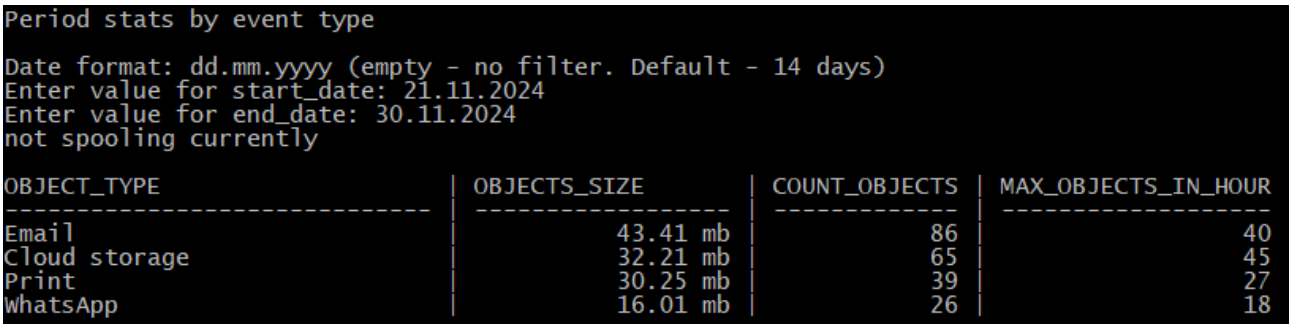


The following information will be shown in columns:

TYPE_NAME	Event type
TYPE_SIZE	Overall size of the events of the particular type in TBS

Scenario 4

As a result of scenario 4 execution, statistics on event types for the specified period of time will be displayed.



The following information will be shown in columns:

OBJECT_TYPE	Event type
OBJECTS_SIZE	Overall size of the events of the particular type
COUNT_OBJECTS	Count of the events of the particular type

MAX_OBJECTS_IN_HOUR	Maximum count of events per hour during the day

Scenario 5

As a result of scenario 5 execution, statistics on top-10 persons for the specified period of time will be displayed. Events with participation of top-10 persons take up the largest space in DB.

```
Period stats by persons

Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date:
Enter value for end_date:
not spooling currently

PERSON_ID                           | DISPLAY_NAME                  | OBJECT_COUNT | OBJECT_SIZE
------------------------------------ | ------------------------------ | ------------ | ------------------
B37174C262444412B7AC8ECDCA544BD200000000 | Ivanov Ivan                |            3 |            0.24 mb
099914C8CFD6416CB734C7721A2CF37600000000 | Petrov Petr                |            2 |            0.62 mb
554BEE71D78B49CE80DA30301022AC9400000000 | Margaret Smith             |            1 |            0.47 mb
```

The following information will be shown in columns:

PERSON_ID	Person ID
DISPLAY_NAME	Person display name
OBJECT_COUNT	Count of events
OBJECTS_SIZE	Overall size of the events with participation of the person

Scenario 6

As a result of scenario 6 execution, statistics on particular person for the specified period of time will be displayed.

```
Statistics on a given person id

Enter value for person_id: B37174C262444412B7AC8ECDCA544BD200000000
Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date:
Enter value for end_date:

Ivanov Ivan

OBJECT_TYPE                  | OBJECT_COUNT | OBJECTS_SIZE
------------------------------ | ------------ | ------------------
Электронная почта            |            3 |            0.24 mb
```

The following information will be shown in columns:

OBJECT_TYPE	Event type
OBJECT_COUNT	Count of events
OBJECTS_SIZE	Overall size of the events with participation of the person

8.1.4 Database Backup

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

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. You may also use this procedure to migrate the database from one server to another.

If, in addition to database, you use Data Storage, i.e. a storage of binary data, then back up the storage together with DB. This procedure is decribed together with DB backup creation.

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 Backup Storage;
- Creating Data Storage Backup.

Defining the Size of Backup

To define size of the future archive, it is necessary to find out summary size of catalogues of DB and Data Storage, if use you the storage.

To define the DB size:

1. On the computer, where the Oracle DB is installed enter the System as the **oracle** user.
2. Open Oracle SQL*Plus and log as **sysdba**:
   ```
   OS> sqlplus / as sysdba
   ```
3. If the system was installed using the installer, 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
   ```

To define size of data in the storage:

1. On the Data Storage server, enter the system as the **root** user.
2. Get the `/opt/dsdata/_seaweedfs` catalogue size:
   ```
   du -sx -BM /opt/dsdata/_seaweedfs
   ```

Checking the 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, the database and Data Storage are located on different computers.
   - Computers 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. Define 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:
   ```
   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 the installer, 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 installer 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

Create a list of files that need to be backed up. You will use this list 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 not required but we recommend doing this especially if there is little free space on IWTM server.

To stop IWTM system:

1. On each computer that hosts IWTM services, log in as **root**.
2. Stop all running Traffic Monitor Server services:
   `iwtm stop`

3. You can start services later (when backup is finished) using the following command:
   `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 Backup Storage

To copy database files:

1. Stop all Oracle services (see *Stopping Oracle Database*). To make sure that all services are stopped, run the following command:
   `ps aux | grep ora`
   If Oracle services are not stopped, backup files can be damaged and unsuitable for recovery.
2. On the computer that hosts the database, copy data from DB directories (see *Collecting a List of Files to Backup*) to previously created directories. You need to copy all the contents of the directories including links.
   If the system was installed using the installer and default parameters were left, the path should be as follows:
   a. copy contents of the **/u01/app/oracle/oradata/iwtm/** directory to the **/opt/IWTM_Backup_Files/IWTM** directory
   b. copy contents of the **/u02/oradata/** directory to the **/opt/IWTM_Backup_Files/Oradata** directory
   c. copy the **/u01/app/oracle/product/db_1/dbs/orapwiwtm** file to the **/opt/IWTM_Backup_Files/Recovery_Aid** directory

> **Important!**
>
> Use only the following devices as file storages:
>
> - an external drive with Ext4 or XFS file system
> - a remote block device connected via iSCSI or NFS protocol
> - a locally connected block device with Ext4 or XFS file system

Creating Data Storage Backup

In Data Storage, Traffic Monitor data are stored in buckets. To back up the storage of binary data, you need to back up these buckets. This procedure consists of the following steps:

1. Enabling functionality of backup

2. Getting a token to work with the Data Storage service
3. Getting a list of buckets for backup
4. Creating the backup task
5. Checking successful completion of backup

During the backuping process you need to send requests using the **curl** utility. When doing this, you can specify the following values as a server address `<ADDRESS>`:

- **localhost:40731**, if you send requests from the server where Data Storage is installed.
- **<server_IP_address>:40732**, if you send requests from another server.

Enabling functionality of backup

To enable creating a backup of Data Storage, you need to specify a directory for that.

We recommend to do it when you install the storage. For this, run the installer using the `--dsbackupspath` parameter with the directory for backups.
Example: `./setup.py install --dsbackupspath=/opt/dsbackups`

To specify the directory after installation, add it to the Data Storage deployment. For this:

1. On the Data Storage server, create a directory for storing a backup:

   ```
   mkdir /opt/dsbackups
   ```

2. Mount an external storage for backups into this directory. Requirements for the backup storage are described in the *Checking the Backup Storage* article.
3. Set a user and access permissions for the created directory:

   ```
   chown 1000 /opt/dsbackups
   chmod 700 /opt/dsbackups
   ```

4. Open the Data Storage deployment for editing. For this use the command:

   ```
   kubectl -n infowatch edit deployment datastorage-<node_label>
   ```

   where `<node_label>` (hereafter) is the label of the node where the storage is installed. For the central node or, if the storage is installed not in the cluster of Platform products, use the label `central`. For the office node, the label is specified during installation (`office` by default). The following actions depends on a text editor that you use. In our example, we use **vi**. To enter insert mode, press **i**.
5. Add the following lines to the `containers` -> `volumeMounts` section:

   ```
   - name: datastorage-databackups-host-volume-<node_label>
     mountPath: /var/lib/databackups
     mountPropagation: HostToContainer
   ```

   In this and the next step, indent with spaces and do not use a tab.
6. Add the following lines to the `volumes` section:

```
- name: datastorage-databackups-host-volume-<node_label>
  hostPath:
    path: /opt/dsbackups
```

7. Save the changes and exit the editor.
   For example, if you use the **vi** editor, press **Esc** and type `:wq`.

Getting a token to work with the Data Storage service

To work with the Data Storage service, you need to get a Bearer token for HTTP authorization. In requests to Data Storage, specify it in the Authorization header.
The token value can become outdated. So in response to a request, the service returns the 440 HTTP code. In this case, get the token again.

To get the token, send the following request to Data Storage:

```
curl -X GET -I --silent "http://<ADDRESS>/v2/logon?extAPIToken=<DS_user_token>" 2>&1 | grep
'^Authorization'
```

where `<ADDRESS>` is the server address. For details, see above.
`<DS_user_token>` is the Data Storage authorization token. The default value: `1exwo92iwpczl1hy6jxy`.
To learn more, see *Configuring Connection with Data Storage*.

As a result, you will see the Authorization header in the following format:
`Authorization: Bearer <token_value>`

Getting a list of buckets for backup

To get a list of identifiers of Data Storage buckets which store Traffic Monitor data, connect to the Traffic Monitor database and run the query:

```
select distinct(storage_bucket_id) from iwtm.tbs_list;
```

If you need to know a list of all existing Data Storage buckets (their bucketID identifiers), send the following request to the storage service:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets?filter=*" 2>&1
```

where `<AUTH_HEADER>` is the Authorization header received on the previous step;
`<ADDRESS>` is the server address. For details, see above.

Results in the JSON format may look as follows:

```
{
  "data": [
    {
      "backendType": "seaweedfs",
      "id": "barbucket",
      "isDumped": false,
      "isInaccurate": false,
      "isSlowDrive": false,
      "size": 27632
```

```
    },
    {
      "backendType": "seaweedfs",
      "id": "bazbucket",
      "isDumped": false,
      "isInaccurate": false,
      "isSlowDrive": false,
      "size": 27633
    },
    {
      "backendType": "file",
      "id": "oldbucket",
      "isDumped": false,
      "isInaccurate": false,
      "isSlowDrive": false,
      "size": 27634
    }
  ]
}
```


Also you can filter the bucket list with a regular expression using the **jq** utility. For example, the following request will find all buckets whose bucket ID value begins with the "bar" substring:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets?filter=*" 2>&1 | jq --raw-output
'.data.[] | select(.backendType=="seaweedfs") | select(.id|test("^bar")).id'
```

Creating the backup task

To create a task of bucket backup, send the following request:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?bucketID=<BUCKET_ID>"
```

where `<AUTH_HEADER>` is the Authorization header;
`<ADDRESS>` is the server address. For details, see above;
`<BUCKET_ID>` is the bucket identifier.

In response, the ID of the created task will be displayed:


```
{
  "taskID": "fe8163f2-a0fb-4990-8bb7-87aee5c425bc"
}
```


Also you can create a bucket backup task and get the ID of this task using the **jq** utility:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?bucketID=<BUCKET_ID>" |
jq --raw-output '.taskID'
```

Next, you can check successful completion of bucket backup using the task ID.

Checking successful completion of backup

To make sure that backuping completed successfully, check the status of the task. For this, send the request:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?taskID=<TASK_ID>"
```

where `<AUTH_HEADER>` is the Authorization header;
`<ADDRESS>` is the server address. For details, see above;
`<TASK_ID>` is the task identifier.

If succesfull, you will see names of data and index files created in the backup directory:

```
{
  "bucketID": "foobucket",
  "dataFilename": "foobucket_0.tar.gz",
  "indexFilename": "foobucket_extindex.tar.gz",
  "taskStatus": "Success"
}
```

In case of failure, the error description will be displayed:

```
{
  "bucketID": "foobucket",
  "error": "permission denied: cannot extract data tarball",
  "taskStatus": "Success"
}
```

Make sure that the task is completed and has one of the following statuses: Success, Canceled, Failed.

Also you can get the task status using the **jq** utility:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?taskID=<TASK_ID>" | jq
--raw-output '.taskStatus'
```

Restoring the Database from the Backup

To restore the database and/or Data Storage:

1. Choose the appropriate method of database recovery if necessary:
    - If the database was damaged due to the system failure or user error, restore the old database. For example, if an important file has been occasionally deleted, you can restore the database to the state when this file still existed. For details, see *Restoring at the Same Database*.
    - If the old database cannot be used any more, create a new database and recover data to it. See *Restoring at the New Database*.
2. Follow one of the scenarios below. You can find required instructions in the followinf articles: *Stopping IWTM System*, *Stopping Oracle Database* and *Restoring Data Storage*.

If you use Data Storage and it is not damaged then no action with the storage is required when restoring DB. Data Storage does not interact with the database directly.

To restore only DB:

1. Stop the Traffic Monitor services.
2. Restore the DB the chosen way.
3. Start the Traffic Monitor services.

To restore only Data Storage:

1. Stop the Traffic Monitor services.
2. Stop the database.
3. Restore Data Storage.
4. Start the database.
5. Start the Traffic Monitor services.
6. Make sure that Traffic Monitor is connected with Data Storage. If necessary, configure connection. For detailes, *Configuring Connection with Data Storage*.

To restore both DB and Data Storage:

1. Stop the Traffic Monitor services.
2. Restore Data Storage.
3. Restore the database.
4. Start the Traffic Monitor services.
5. Make sure that Traffic Monitor is connected with Data Storage. If necessary, configure connection.

> **Important!**
>
> If you need to update Traffic Monitor to a new version, you should first restore the database. Updating Traffic Monitor either before or during the database recovery is not supported.

Restoring at the Same Database

Below you can find instructions on how to restore data to a database that has the same directory structure as the one that was backed up.

To restore the database without 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. Delete all content of the **/u02/oradata/, /u02/oradata1/**, and **/u01/app/oracle/oradata/iwtm/** directories.
4. Copy the content of the **/opt/IWTM_Backup_Files/Oradata/** directory to the **/u02/** directory.
5. Copy the content of the **/opt/IWTM_Backup_Files/IWTM/** directory to the **/u01/app/oracle/oradata/iwtm/** directory.
6. Rename the **control01.ctl** file located in the **/opt/IWTM_Backup_Files/IWTM/** directory to the **control02.ctl** and copy it to the **/u01/app/oracle/oradata/iwtm/** directory.
7. Check permissions. Change them if necessary:
   ```
   OS> chown -R oracle:oinstall /u02/
   OS> chown -R oracle:oinstall /u01/app/oracle/oradata/iwtm/
   ```
8. 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.

Restoring Data Storage

Restoring the storage of binary data lies in restoring buckets from their backups. This procedure consists of the following steps:

1. Getting a token to work with the Data Storage service
2. Creating the task of restoring bucket
3. Checking successful completion of the task

When sending **curl** requests, you can specify the following values as a server address `<ADDRESS>`:

- **localhost:40731**, if you send requests from the server where Data Storage is installed.
- **<server_IP_address>:40732**, if you send requests from another server.

Getting a token to work with the Data Storage service

To work with the Data Storage service, you need to get a Bearer token for HTTP authorization. In requests to Data Storage, specify it in the Authorization header.
The token value can become outdated. So in response to a request, the service returns the 440 HTTP code. In this case, get the token again.

To get the token, send the following request to Data Storage:

```
curl -X GET -I --silent "http://<ADDRESS>/v2/logon?extAPIToken=<DS_user_token>" 2>&1 | grep '^Authorization'
```

where `<ADDRESS>` is the server address. For details, see above.
`<DS_user_token>` is the Data Storage authorization token. The default value: `1exwo92iwpczl1hy6jxy`.
To learn more, see *Configuring Connection with Data Storage*.

As a result, you will see the Authorization header in the following format:
`Authorization: Bearer <token_value>`

Creating the task of restoring bucket

To create a task of restoring bucket, send the following request:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?bucketID=<BUCKET_ID>"
```

where `<AUTH_HEADER>` is the Authorization header;
`<ADDRESS>` is the server address;
`<BUCKET_ID>` is the bucket identifier.

In response, the ID of the created task will be displayed:

```
{
  "taskID": "fe8163f2-a0fb-4990-8bb7-87aee5c425bc"
}
```

Also you can create the task of restoring bucket and get the ID of this task using the **jq** utility:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?bucketID=<BUCKET_ID>"
 | jq --raw-output '.taskID'
```

Next, you can check successful restoration of bucket using the task ID.

Important!

You can restore the bucket only if there is no one with the same ID in Data Storage.

Checking successful completion of the task

To make sure that restoration completed successfully, check the status of the task. For this, send the request:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?taskID=<TASK_ID>"
```

where `<AUTH_HEADER>` is the Authorization header;
`<ADDRESS>` is the server address.;
`<TASK_ID>` is the task identifier.

If succesfull, you will see the following response:

```
{
  "bucketID": "foobucket",
  "taskStatus": "Success"
}
```

Make sure that the task is completed and has one of the following statuses: Success, Canceled, Failed.

Also you can get the task status using the **jq** utility:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?taskID=<TASK_ID>" | jq
--raw-output '.taskStatus'
```

8.1.5 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 should 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:
   `iwtm stop`
   `service php-fpm stop`
   `service nginx stop`
3. Retrieve list of scheduled jobs from database server. For thisб 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:
    ```
    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.

8.1.6 Database Logging

Oracle DBMS operation in Traffic Monitor is logged with a script. This script allows you to set the logging level and export log data to a CSV file. The script uses settings of the current configuration file: `/opt/iw/tm5/csw/database.conf`. You should run the script from the directory where it is stored: **/** `opt/iw/tm5/csw/oracle/scripts/sys_log/sys_log.sh`.

The script includes the following commands:

- To set the logging level: `debug, info, warning, error –` run the command:
  `level`
  If you do not specify the second parameter, the current logging level is displayed.
- To export the log body (V_SYS_LOG representation) to a CSV file, run the command:
  `export`
  If necessary, you can set the number of lines to be exported:
  `export <the number of lines>`

On how logs are stored on the disk, see *Rotation of database logs*.

Rotation of database logs

Rotation of database logs is the process of archiving, storing, and deleting obsolete data in logs. This process is required to save space and free up disk space. In Traffic Monitor, rotation applies to:

1. Database logs:
   a. XML file that contains a log of errors and important messages. It is located in the `/u01/app/oracle/diag/rdbms/iwtm/iwtm/alert` folder. The file is stored for one year. Rotation applies to each 10 Mb of the file. The file is deleted automatically.

b. TRC and TRM files that contain detailed information about DB errors (trace files). They are located in the `/u01/app/oracle/diag/rdbms/iwtm/iwtm/trace` folder. Files are stored for 30 days and then they are automatically deleted.
c. `alert_iwtm.log` - a database log file in a text format. It is stored in the `/u01/app/oracle/diag/rdbms/iwtm/iwtm/trace` folder. Rotation applies to each 100 Mb of the file. The file is rotated by the **logrotate** service and is deleted when the number of files exceeds 1000.

2. Logs of **listener** network service:
   a. XML file that contains logs of the **listener** service. The file is located in the `/u01/app/oracle/diag/tnslsnr/hostname/listener/alert` folder. The file is stored for one year. The file is stored for one year. Rotation applies to each 10 Mb of the file. The file is deleted automatically by the **crond** service.
   b. TRC and TRM files that contain detailed information about errors of the **listener** service. Files are stored for 30 days and then they are automatically deleted by the **crond** service.
   c. `listener.log` - a log file of the **listener** service in a text format. The file is located in the `/u01/app/oracle/diag/tnslsnr/hostname/listener/alert` folder. Rotation applies to each 100 Mb of the file. The file is rotated by the **logrotate** service and is deleted when the number of files exceeds 100.

Settings of the **crond** service for deleting obsolete files are located in `/etc/cron.daily/delete_old_oracle_logs.cron.`

Settings of the **logrotate** service are located in `/etc/logrotate.d/iwtm-oracle-conf-server.`

8.2 PostgreSQL

To connect to DB server from Traffic Monitor server terminal, run the command as `root`:

```
psql postgres iwtm
```

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

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

This chapter contains instructions on administrating PostgreSQL:

- Tablespaces in InfoWatch Traffic Monitor database;
- Managing Daily Tablespaces;
- Load statistics of Daily Tablespaces;
- Database Backup;
- Database Server Routinely Maintenance;
- Database logging.

> **Note:**
>
> To change the DB user password, see the *Changing the Preset Password* article.

8.2.1 Tablespaces in InfoWatch Traffic Monitor database

General information

InfoWatch Traffic Monitor data are stored in DB as tablespaces (TS). There are two types of Traffic Monitor tablespaces:

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.)

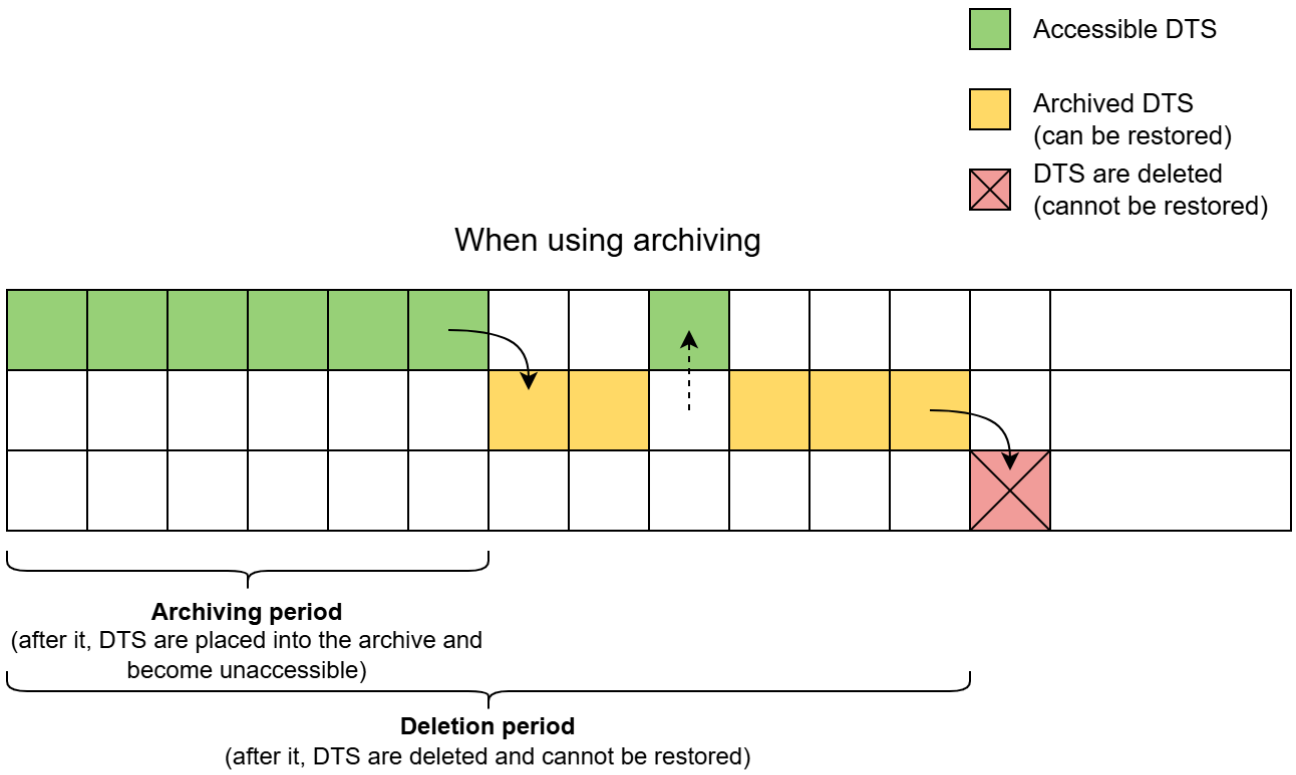
All data about the objects intercepted on a particular day (according to UTC+0) is stored in three daily tablespace (DTS) of the folowing types:

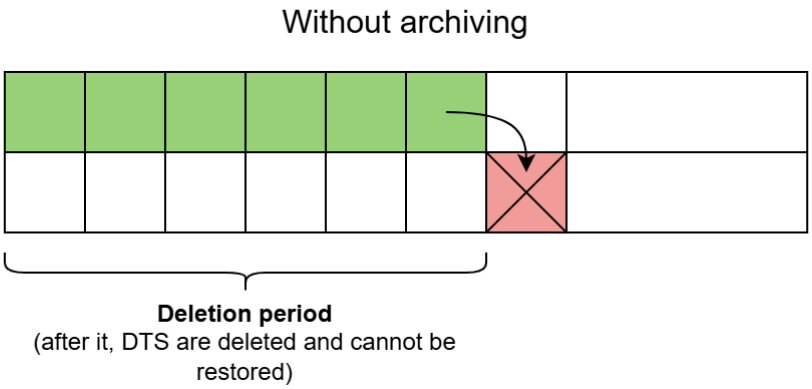
- Events without violations;
- Events with violations;
- Other (screenshots).

Daily tablespaces are created every day in such a way that the database always has DTS for the next six days, excluding the current day. All DTS automatically get the *IWTM_YYYYMMDD_X* name, where X is the DTS number (the TBS_ID value from the TBS_LIST table). The tablespace type is defined by the TBS_TYPE value: 0 – No Violations, 1- Violation, 2 - Other (screenshots).

Lifecycle of DTS can be divided into 3 stages:

1. **Ordinary storing**
   Initially, DTS are stored in the database and are in operational access. If you use Data Storage, then the event contents from this DTS such as attachments, screenshots, audio files, and so on, are stored there.
2. **Storing in an archive** (optional)
   If you need to store events for a long time, but do not need operational access to them, you can archive them before deleting.
   For this, enable automatic archiving of DTS. After the **archiving period**, they will be archived and will become unavailable. If neccesary, you can restore them (the dashed arrow on the diagram).
3. **Deleting**
   To avoid disk overflow, you can delete DTS which you do not need to store.
   For this, enable automatic deleting of DTS. After the **deletion period**, they will be deleted without the possibility of restoring.





By default, automatic archiving and deletion are disabled. You can enable them during the installation or after it. Also, you should set the DTS **archiving period** and/or the DTS **deletion period**. For details, see articles on archiving and deletion.
Configure **archiving period** and **deletion period** so that you always have enough free space on the disks, which store DTS, and they do not overflow.

If you need to archive/restore/delete a single DTS, you can do it manually in the Traffic Monitor web interface. See *InfoWatch Traffic Monitor. User Guide. Managing tablespaces*.
If the web interface is unavailable, use the **iw_space_manager** service utility for this (see *Managing Daily Tablespaces with the Console Utility*). Last operate with DTS manually in the database.

Storing

The main tablespace is stored in the `/u02/pgdata` catalogue by default.
The daily tablespaces are stored in the `/u02/pgdata1` catalogue by default.
For details on placing DTS, see *Configuring Location of Files in File System*.

On storage modes, see *Configuring Storage Modes for Tablespace Files*.

Archiving

Archiving process consists of:

- disconnecting DTS from the database;
- moving DTS to the specified catalogue (by default: `/u02/arch`).

You should place this catalogue on the separate disk to free up space on the hard drive with operational data and avoid its overflow.
When using Data Storage, binary data of the archived DTS will be moved to the Data Storage slow disk.

During archiving, data is not compressed. So, on the allocated disk, it will take about the same place. You can estimate the size of the disk for archived DTS based on how much place DTS take in operational access in their storage directories (by default: `/u02/pgdata1` in the DB and `/opt /dsdata/_seaweedfs` in Data Storage).

Archiving is described in details in the *Archiving Daily Tablespaces* section.

To access the archived DTS data, you need to restore it. See *Restoring Daily Tablespaces*.

Deleting

When automatic deletion is enabled, the System deletes DTS older than the deletion period. You specify its value separately for each DTS type: events without violations, events with violations, other (screenshots).

For details on deletion methods, see *Deleting Daily Tablespaces*.

8.2.2 Managing Daily Tablespaces

In this section:

- Configuring Location of Files in File System;
- Configuring Storage Modes for Tablespace Files;
- Archiving Daily Tablespaces;
- Restoring Daily Tablespaces;
- Deleting Daily Tablespaces;
- Managing Daily Tablespaces with the Console Utility.

Configuring Location of Files in File System

By default, the installation program (see *InfoWatch Traffic Monitor. Installation Guide* document) sets the usage of one directory for storing tablespaces: `/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.

Configuring Storage Modes for Tablespace Files

There are three modes of storing data in DB:

- **Normal** – switching to the following partition (when it is specified) happens after the previous one is overflow.
- **Fast/Slow disks** – dividing pools into fast and slow ones. Recent data are to be kept in fast pool. In a number of days specified, the System relocate them to the slow ones. Slow pool operates in Normal mode.
- **Rotate** – switching to the following partition happens every day once the previous one is overflow.

You select storage mode when installing Traffic Monitor. By default, the installer offers you **Normal** mode. You can change the storage mode later.

By default, DTS are stored in the `/u02/pgdata1` directory.

> **Note:**
>
> Modes described in this article relate to data stored in DB only. Changing mode does not affect data stored in Data Storage.

Fast/slow disks Mode

The System moves data from the fast disk to the slow one every night. If you are switching from **Normal** mode to **Fast/slow** mode, you store a large amount of DTS on your old partition, and you specify the old partition as a fast disk, then data transfer may take a long time.
If you will use the old disk as a fast one, before switching mode make sure that the following conditions are met:

- The new partition size is not less than the old one size. So, there is enough space for transferring all DTS from the old partition;
- There is free space in the old partition not less than the largest tablespace that will be transferred to the slow disk.

The System creates DTSs every day in such a way that the database always has DTS for the next six days, excluding the current day. So, if when switching from **Normal** mode to **Fast/slow** mode, you specify a new partition as a fast disk, then, for first seven days, the System will save events to the already created DTS on the slow disk. In this case, the System will create new DTSs on the fast disk.

For configuring **Fast/slow** mode, we will use the new partition `/u03/pgdata/` as a slow disk and the old partition `/u02/pgdata1/` as a fast one.

To configure "Fast/slow" storage mode (fast and slow disks):

1. Edit the `/etc/fstab` file to automatically mount the new partition to `/u03`:
   `/dev/sdd1 /u03/ ext4 defaults 1 2`
2. Create the `pgdata` folder:
   ```
   mkdir /u03/pgdata
   ```
3. Change the user:
   `chown -R postgres:postgres /u03`
4. Log into the database:
   `su - iwtm`
   `psql -p 5433 -h <DB_server_IP_address> postgres iwtm`
   `psql -p 5433 -h 127.0.0.1 postgres iwtm` – to connect to the local database
5. Specify the storage period on fast disks (7 by default):
   `select pkg_part_set_fast_days(7);`
6. Specify the path to the fast disk:
   `select pkg_part_set_fast_path('/u02/pgdata1/',1);`
7. Specify the path to the slow disk:
   `select pkg_part_set_df_path('/u03/pgdata/',1);`
8. If necessary, you can use multiple slow disks. The data will be recorded to the next slow disk when the previous one is full. To add slow disks, specify a new path:

   
   ```
   select pkg_part_set_df_path('/u03/pgdata2/',2);
   ```
9. Specify the total amount of slow disks (up to 10):
   ```
   select pkg_part_set_df_path_cnt('2');
   ```
10. Change the mode to fast-slow disks:
    `select pkg_part_set_filesys_type('fast/slow')`
    The data will be transferred from the fast disks to slow ones during a night job.
11. To start the file transfer manually, run:
    `select iwtm.pkg_part_move_fast_tablespaces_to_slow();`

> **Note:**
>
> The System allows using multiple slow disks.

> **Note:**
>
> In **Fast/slow** mode, the screenshot tablespaces are stored in slow partitions only.

To switch back to "Normal" storage mode:

1. Check the contents of the `/u02/pgdata1/` fast disk directory:
   `ls /u02/pgdata1/`
2. Check the contents of the `/u03/pgdata/` slow disk directory:
   `ls /u03/pgdata/`
3. Log into the database:
   `su - iwtm`
   `psql -p 5433 -h <DB_server_IP_address> postgres iwtm`
   `psql -p 5433 -h 127.0.0.1 postgres iwtm` – to connect to the local database
4. Change the storage period on fast disks:
   `select pkg_part_set_fast_days(-1);`
   The "-1" value is specified to transfer tablespaces for today.
5. Run the task to transfer the tablespaces from fast disks to slow disks:
   `select iwtm.pkg_part_move_fast_tablespaces_to_slow();`
6. Check the contents of the fast disks directory. The tablespaces that are created for future dates should remain. Such tablespaces should be manually deleted by using the **iw_space_manager** service:
   `iw_space_manager tbs:delete <tbs_id>`
   or via the database (if you do not use Data Storage):
   `select pkg_part_delete_tablespaces(<tbs_id>);`
7. Run the task (cron) of the **iw_space_manager** service to create DTSs imidiately:
   `iw_space_manager cron`
   or start a job in the database (if you do not use Data Storage):
   `/opt/iw/tm5/bin/dbtools/dbconf-jobs-postgres.sh start iwtm_add_parts`
8. Check that all tablespaces have been transferred from the fast disks:
   `ls /u02/pgdata1/`
9. Check that the tablespaces for future dates have been created on the slow disks:
   `ls -alt /u03/pgdata/`
10. Enable **Normal** mode:
    `select pkg_part_set_filesys_type('normal');`

Rotate Mode

To configure "Rotate" storage mode (daily rotation):

1. Mount the partition and make sure that it can be mounted automatically on reboot.
2. Create the `pgdata` folder:
   ```
   mkdir /u03/pgdata
   ```
3. Change the user:
   `chown -R postgres:postgres /u03`
4. Log into the database:
   `su - iwtm`
   `psql -p 5433 -h <DB_server_IP_address> postgres iwtm`
   `psql -p 5433 -h 127.0.0.1 postgres iwtm` – to connect local database

5. Add a path to the second partition:
   `select pkg_part_set_df_path('/u03/pgdata/',2);`
6. Specify a new number of paths:
   `select pkg_part_set_df_path_cnt(2);`
7. Switch to **rotate** mode:
   `select pkg_part_set_filesys_type('rotate');`

```
          postgres=# select * from setting where setting like 'df_%';
setting | value | editable
------------+---------------+----------
df_path1 | /u02/pgdata1/ | 1
df_path2 | /u03/pgdata/ | 1
df_path_cnt | 2 | 1
df_filesys_type | rotate | 1
```

> **Note:**
>
> Parameters of modes are stored in the `setting` table of the database. Their specifics are described in the *Tablespaces data storage settings. Data storage partition* Knowledge Base article.

Archiving Daily Tablespaces

Archiving process consists of disconnecting DTS from the database and moving them to the specified catalogue (by default: `/u02/arch`). You should place this catalogue on the separate disk to free up space on the hard drive with operational data and avoid its overflow. You can restore this data if necessary.

In the System, there are following ways of archiving DTS:

- Automatically after the specified period is expired (see *Automatic Archiving of Daily Tablespaces*);
- Manual archiving of single DTS:
  - In the Traffic Monitor web interface. See *InfoWatch Traffic Monitor. User Guide. Managing tablespaces*;
  - Using the console utility of the **iw_space_manager** service (see *Managing Daily Tablespaces with the Console Utility*);
  - In the database (see *Manual Archiving of Daily Tablespaces in the Database*).

If you need to archive a single DTS, we recommend to do it in the Traffic Monitor web interface. If the web interface is unavailable, use the **iw_space_manager** service utility. Last use manual archiving of DTS in the database.

Archiving when using Data Storage

If you use Data Storage, then, when archiving DTS, binary data will be moved to the Data Storage slow disk.
If the slow disk is not connected, then, in Traffic Monitor web interface, archived daily tablespace will have the "*Archived*" status. But in this case, binary data of DTS will be stored on the fast disk of the Data Storage server,

inside the directory for placing binary data. You specify this directory when installing the storage (by default: `/opt/dsdata/_seaweedfs`).

You specify the path to the slow disk when installing Data Storage. For details, see *InfoWatch Traffic Monitor. Installation Guide. Installing Platform*.
To add the path to the Data Storage slow disk after installing the storage:

1. Create a directory and mount the slow disk to it:

```
mkdir -p /mnt/slowdisk
mount /dev/<your_slowdisk> /mnt/slowdisk
```

2. Set a user and access permissions for the directory, where you have mounted the slow disk:

```
chown 1000 /mnt/slowdisk
chmod 700 /mnt/slowdisk
```

3. Open the Data Storage deployment for editing. For this use the command:

```
kubectl -n infowatch edit deployment datastorage-<node_label>
```

   where `<node_label>` (hereafter) is the label of the node where the storage is installed. For the central node or, if the storage is installed not in the cluster of Platform products, use the label `central`. For the office node, the label is specified during installation (`office` by default).
4. Add the following lines to the `containers` -> `volumeMounts` section:

```
      - mountPath: /var/lib/dataslow
        name: datastorage-dataslow-host-volume-<node_label>
```

5. Add the following lines to the `volumes` section:

```
      - hostPath:
          path: /mnt/slowdisk
          type: ""
        name: datastorage-dataslow-host-volume-<node_label>
```

6. Save the changes and exit the editor.

Automatic Archiving of Daily Tablespaces

By default, automatic DTS archiving is disabled. To make the System archive DTS according to schedule, enable this function and set the time after which DTS must be archived. Details are described further.
Every day, at 00:00 server time, the **iw_space_manager** service procedure will archive DTS that satisfy the following condition:

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

So, all DTS older than the specified value will be archived.

Warning!

If months or years are used as the time interval, we recommend using the maximum value of the interval in calculations. For a month – 31 days. For a year – 366 days. For example, to archive DTS older than 4 years, specify the interval 366 * 4 = 1464 days.

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

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

The `postgres` 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;
  ```

- 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;
  ```

- 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 archiving is enabled (to disable it, specify 0 instead);
  D is a number of days after which the daily tablespace is archived by the System. This number should be smaller than the set number of days before deleting the daily tablespace (see *Deleting Daily Tablespaces*).

Manual Archiving of Daily Tablespaces in the Database

It is recommended to archive single DTS via web interface or using the **iw_space_manager** utility.

The order of archiving daily tablespaces manually in the database is described below.

> **Important!**
>
> In this method of archiving, data stored in the Data Storage are not archived.

Selecting daily tablespaces and data files

You can get a list of tablespaces that can be disconnected by running queries to the database on behalf of the database schema owner. The queries are made 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 iwtm_iwtm_add_parts, iwtm_iwtm_delete_tablespaces, iwtm_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 required tablespace 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 disconnect.

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.

In the System, there are the following ways of restoring DTS:

- In the Traffic Monitor web interface. See *InfoWatch Traffic Monitor. User Guide. Managing tablespaces*;
- Using the console utility of the **iw_space_manager** service. See *Managing Daily Tablespaces with the Console Utility*;
- In the database – this method is described below. It is recommended to use this method last.

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 read and write privileges for the directory to move the data files to.

Connecting the daily tablespace

Warning!

Do not connect daily TS during iwtm_iwtm_add_parts, iwtm_iwtm_delete_tablespaces and iwtm_iwtm_archive_tablespaces jobs. This may cause 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 completing the procedure, the status of TS will change to *Restored*.
2. Repeat the procedure call for each daily TS you want to enable.

Deleting Daily Tablespaces

In the System, there are the following ways of deleting DTS:

- Automatic, according to schedule. Described below.
- Manual deleting of single DTS:
  - In the Traffic Monitor web interface. See *InfoWatch Traffic Monitor. User Guide. Managing tablespaces*;
  - Using the console utility of the **iw_space_manager** service. See *Managing Daily Tablespaces with the Console Utility*;
  - In the database. Described below.

We recommend using scheduled deletion. Otherwise, disk overflow can occur or the big amount of data for deletion can build up. It will result in increasing the time for running this procedure in future and consequently increasing the idle time of the Traffic Monitor Server.

Warning!

Deleting tablespaces cannot be undone. If you complete the operation, you will not be able to restore the deleted data.
The System deletes both DTS data from the storage directory (by default, `/u02/oradata1`, or `/u02/arch` for the archived ones) and information on DTS from the database. If you use Data Storage, data from it will be deleted as well.

While deleting tablespaces, access to the corresponding tables is closed. For this reason, log files of the **iw_deliver**, **iw_x2db**, **iw_updater** processes may contain database access errors. Once tablespaces are deleted, these processes automatically restore access to the database.

Automatic deletion

By default, automatic DTS deletion is disabled. To make the System delete DTS according to schedule, enable this function and set the time after which DTS must be deleted. Details are described further.
Every day, at 00:00 server time, the **iw_space_manager** service procedure will delete DTS that satisfy the following condition:

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

So, all DTS older than the specified value will be deleted.

> **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 DTS older than 4 years, specify 366*4=1464 days interval.

Enabling automatic deletion

Automatic deletion according to schedule is configured separately for each DTS type.
To enable it, set the deletion `delete_enabled` flag and specify the period of storing DTS `delete_period`.
For this, run the following scripts on behalf of the database scheme owner:

- For DTS storing objects with the *Violation* status:

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

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

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

- 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 automatic deletion is enabled (to disable, specify 0 instead of 1);
D is a number of days at the end of which the DTS will be deleted by the System. This number should be larger than the set number of days before archiving daily tablespaces (see *Automatic Archiving of Daily Tablespaces*).

Deleting daily tablespaces with a script

As well, you can configure automatic deletion of daily tablespaces, use the `/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh` or `/opt/iw/tm5/bin/dbtools/dbconf-jobs-postgres.sh` script. You can use the following commands:

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]`
View the state of settings	`/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh show [-v]`
Delete all DTS	`/opt/iw/tm5/bin/dbtools/dbconf-jobs-postgres.sh start iwtm_delete_tablespace`

Example:

To enable automatic deletion of the DTS, that store objects with the *"No violation"* status and are older than 15 days, run the commands:

```
/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh set noviolation 15 [-v]
/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh enable noviolation [-v]
```

Manual deletion in the database

If you need to immediately launch the procedure of automatic DTS deletion (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 on behalf of the database scheme owner:

```
select pkg_part.delete_tablespaces();
```

As a result, the System will delete DTS for which scheduled deletion is enabled and the period of storing is specified.

The command above affects data in DB only. If you use Data Storage, launch the procedure of automatic DTS deletion using the **iw_space_manager** service:

```
iw_space_manager cron
```

To delete one DTS by its identifier (ID), run the following script:

```
select pkg_part.delete_tablespace(<ID>);
```

This command affects data in DB only. If you use Data Storage, delete DTS using the **iw_space_manager** service:

```
iw_space_manager tbs:delete <tbs_id>
```

Managing Daily Tablespaces with the Console Utility

To manage daily tablespaces via the command line, use the console utility that calls the **iw_space_manager** service. The service is available for the **iwtm** user and is enabled by default.

When using Data Storage, the **iw_space_manager** service archives/restores/deletes binary data from the storage as well.

Commands and parameters of the service:

Command	Description
`tbs:archive [options] [--] <id>`	Starts archiving a daily tablespace with its ID specified. An example on how to archive a daily tablespace with ID=123: `iw_space_manager tbs:archive 123`
`tbs:create <type> <capture>`	Creates a daily tablespace with the following data specified: • Type: 0 – no violation, 1 – violation, 2 – screenshots • Creation date in the YYYY-MM-DD format An example on how to create a new daily tablespace with violations on September 1, 2023: `iw_space_manager tbs:create 1 2023-09-01`
`tbs:delete [options] [--] <id>`	Deletes a daily tablespace with its ID specified
`tbs:get [options]`	Gets the list of existing daily tablespaces. Additional parameters: • `--limit=LIMIT` – sets the maximal number of items to display on the screen • `--offset=OFFSET` – hides the first N items (N=0 by default) • `--order=ORDER` – sorts the daily tablespace list by its name and creation time: ASC – ascending, DESC – descending An example on how to get a list of 20 daily tablespaces sorted by name and descending date: `iw_space_manager tbs:get -- limit=20 --order="TBS_NAME:ASC,PART_DATE:DESC"`

Command	Description
`tbs:restore [options] [--] <id>`	Restores an archived daily tablespace with its ID specified. An example on how to restore a daily tablespace with ID=123 from an archive: `iw_space_manager tbs:restore 123`
	With all the commands listed above, you can use the following common parameters: • `-f, --force` – runs the command without the validation check in case of a database emergency. Enables you to perform operations on tablespaces where date of event interception coincides with today's date; • `--used-configs` – runs the command with the parameters from the configuration file; • `-p, --configpath [=CONFIGPATH]` – displays the configuration file path. By default, it is `opt/iw/tm5/etc` ; • `--force-config-load` – force loads the configuration file even if the query parameters are specified.
`tbs:clearLostBuckets`	Deleting obsolete, lost or unused buckets of table spaces (available starting from Traffic Monitor 7.10.1)

To get logs and debug messages, run the service with the parameters below:

- `-v` – displays usual logs;
- `-vv` – displays logs with extended detalization;
- `-vvv` – displays logs with full detalization.

To get a list of available commands, run the command:

`iw_space_manager list`

8.2.3 Load statistics of Daily Tablespaces

To analyze a load of daily tablespaces, you can use the `/opt/iw/tm5/bin/dbtools/tablespace_stat_postgres/tablespace_stat_postgres.sh` script. With its help, you can get the statistics on TBS content for the selected period. The script executes one of the six scenarios and in each case it collects different information. The scenarios are described in more detail *below*.

To display the information on the script usage:

1. Go to the directory where the script is located by running the command:
   `cd /opt/iw/tm5/bin/dbtools/tablespace_stat_postgres/`
2. Run the script without parameters by running the command:
   `./tablespace_stat_postgres.sh`

As a result, you will see the help information:

```
tablespace_stat.sh: usage: [ report_number ] [ -e ]

report_number:
1 - Period stats
2 - Period stats with count of objects
3 - Statistics on a given tbs id by event type
4 - Period stats by event type
5 - Period stats by person
6 - Statistics on a given person id

-e, --export : for export to csv
```

To use the script:

1. Go to the directory where the script is located by running the command:
   `cd /opt/iw/tm5/bin/dbtools/tablespace_stat_postgres/`
2. Run the script by running the command:
   `./tablespace_stat_postgres.sh <scenario_number> <-e>`
   where the scenario number is a digit from 1 to 6;
   `-e` or `--export` is a key that you can specify to unload the results of script execution in .csv format.
   Example of a command running the script:
   `./tablespace_stat_postgres.sh 1`
3. Specify the parameters depending on a scenario:
   - For scenarios 1, 2, 4, 5, 6 – a period for which the statistics should be displayed:
     a. Specify the lower bound of the period in the dd.mm.yyyy format and press **Enter**;
     b. Specify the upper bound and press **Enter**;

     > **Note:**
     >
     > If you do not specify values for bounds and just press **Enter** twice then, by default, statistics for last two weeks will be displayed.
     > If you specify only the lower bound then information for the period from the specified date to the current one will be displayed.

   - For scenario 3 – ID of the tablespace;
   - For scenario 6 – person's ID.

In case of unloading the results of script performing, the file is saved in the directory where the script is located. The file has the following name:
`report_<scenario_name>_<date>.csv`
where `<scenario_name>` has a value depending on the scenario number:

Scenario number	Scenario name	Short description
1	tbs_stat_period	Statistics for the period of time
2	tbs_stat_period_count	Statistics for the period of time including count of events in TBS
3	tbs_stat_by_tbs_id	Statistics on a particular TBS
4	tbs_stat_by_event_type	Statistics on event types for the period

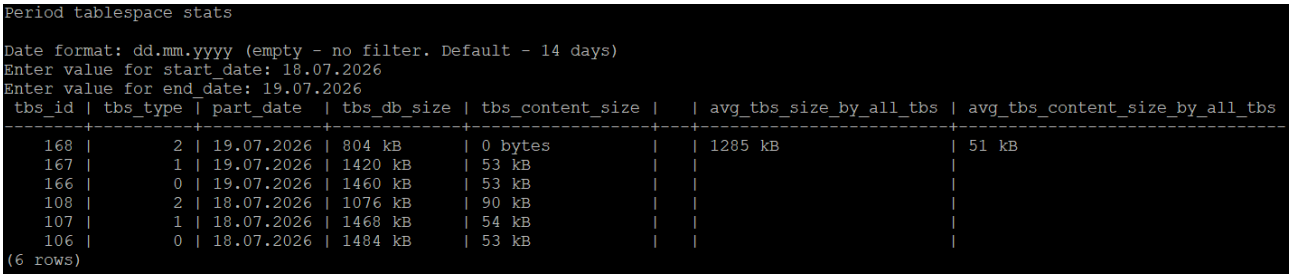
5	tbs_stat_by_persons	Statistics on top-10 persons
6	tbs_stat_by_person_id	Statistics on a particular person

`<date>` - date of script execution. It has the `<yyyy-mm-dd HH-mm-ss>` format.
Example of the unloading file name: `report_tbs_stat_period_count_2024-12-17_18-20-39.csv`

Scenarios of script execution

Scenario 1

As a result of scenario 1 execution, statistics on space that tablespaces take up for the period of time will be displayed.



```
Period tablespace stats

Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date: 18.07.2026
Enter value for end_date: 19.07.2026
 tbs_id | tbs_type | part_date  | tbs_db_size | tbs_content_size |   | avg_tbs_size_by_all_tbs | avg_tbs_content_size_by_all_tbs
--------+----------+------------+-------------+------------------+---+-------------------------+---------------------------------
    168 |        2 | 19.07.2026 | 804 kB      | 0 bytes          |   | 1285 kB                 | 51 kB
    167 |        1 | 19.07.2026 | 1420 kB     | 53 kB            |   |                         |
    166 |        0 | 19.07.2026 | 1460 kB     | 53 kB            |   |                         |
    108 |        2 | 18.07.2026 | 1076 kB     | 90 kB            |   |                         |
    107 |        1 | 18.07.2026 | 1468 kB     | 54 kB            |   |                         |
    106 |        0 | 18.07.2026 | 1484 kB     | 53 kB            |   |                         |
(6 rows)
```

The following information will be shown in columns:

tbs_id	TBS identifier
tbs_type	TBS type: 0 - No Violations 1 - Violation 2 - Other (screenshots)
part_date	Date of TBS creation
tbs_db_size	TBS size in DB not including binary data
tbs_content_size	Size of TBS binary data. If you use Data Storage, these data are stored there
avg_tbs_size_by_all_tbs	Average size of one TBS for the specified period of time, not including binary data
avg_tbs_content_size_by_all_tbs	Average size of binary data of one TBS for the specified period of time

Scenario 2

As a result of scenario 2 execution, statistics with count of objects on tablespaces for the period of time will be displayed.

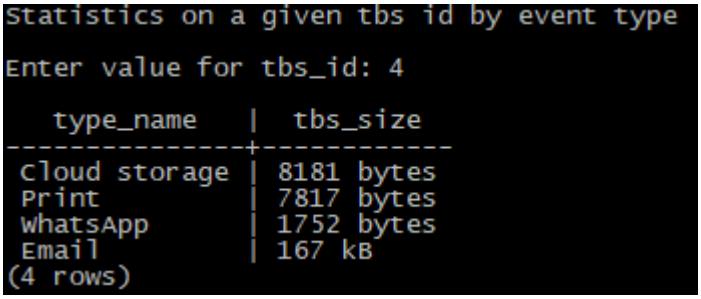
```
Period tablespace stats with count of objects

Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date: 18.07.2026
Enter value for end_date: 19.07.2026

 tbs_id | part_date  | tbs_type | tbs_status | count_objects | tbs_db_size | tbs_content_size | avg_tbs_size_by_all_tbs | avg_tbs_content_size_by_all_tbs
--------+------------+----------+------------+---------------+-------------+------------------+-------------------------+---------------------------------
    168 | 19.07.2026 |        2 | 0 - online |             0 | 804 kB      | 0 bytes          | 1285 kB                 | 51 kB
    167 | 19.07.2026 |        1 | 0 - online |            16 | 1420 kB     | 53 kB            |                         |
    166 | 19.07.2026 |        0 | 0 - online |            26 | 1460 kB     | 53 kB            |                         |
    108 | 18.07.2026 |        2 | 0 - online |             3 | 1076 kB     | 90 kB            |                         |
    107 | 18.07.2026 |        1 | 0 - online |            17 | 1468 kB     | 54 kB            |                         |
    106 | 18.07.2026 |        0 | 0 - online |            27 | 1484 kB     | 53 kB            |                         |
(6 rows)
```

The following information will be shown in columns:

tbs_id	TBS identifier
part_date	Date of TBS creation
tbs_type	TBS type: 0 - No Violations 1 - Violation 2 - Other (screenshots)
tbs_status	TBS status: 0 - online (connected, in normal state) 3 - read only (only for reading) 5 - before exchange (before disconnecting for archiving) 7 - prepared offline (prepared to be disconnected for archiving) 9 - disconnected (disconnected before moving to archive) 10 - offline (archived and disconnected) 11 - plugged (plugged in before restoration) 13 - before update (before updating for restoration) 15 - after update (after updating for restoration) 17 - before revert (before restoring from archive) 20 - restored (restored from archive)
count_objects	Count of events in a TBS
tbs_db_size	TBS size in DB not including binary data
tbs_content_size	Size of TBS binary data. If you use Data Storage, these data are stored there
avg_tbs_size_by_all_tbs	Average size of one TBS for the specified period of time, not including binary data
avg_tbs_content_size_by_all_tbs	Average size of binary data of one TBS for the specified period of time

Scenario 3

As a result of scenario 3 execution, statistics on a particular TBS will be displayed.

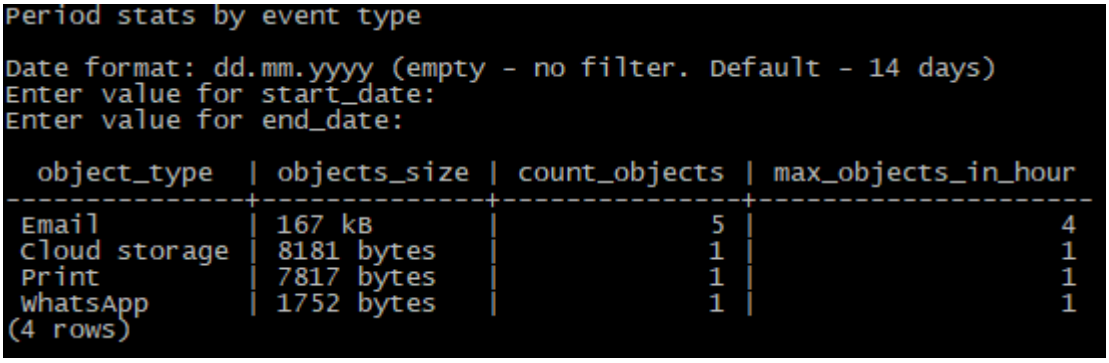


The following information will be shown in columns:

type_name	Event type
tbs_size	Overall size of the events of the particular type in TBS

Scenario 4

As a result of scenario 4 execution, statistics on event types for the specified period of time will be displayed.



The following information will be shown in columns:

object_type	Event type
objects_size	Overall size of the events of the particular type
count_objects	Count of the events of the particular type
max_objects_in_hour	Maximum count of events per hour during the day

Scenario 5

As a result of scenario 5 execution, statistics on top-10 persons for the specified period of time will be displayed. Events with participation of top-10 persons take up the largest space in DB.

```
Period stats by persons

Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date:
Enter value for end_date:

               person_id                |  display_name  | object_count | objects_size
----------------------------------------+----------------+--------------+--------------
 B37174C262444412B7AC8ECDCA544BD200000000 | Ivanov Ivan    |            3 | 109 kB
 099914C8CFD6416CB734C7721A2CF37600000000 | Petrov Petr    |            2 | 62 kB
 554BEE71D78B49CE80DA30301022AC9400000000 | Margaret Smith |            1 | 47 kB
(3 rows)
```

The following information will be shown in columns:

person_id	Person ID
display_name	Person display name
object_count	Count of events
objects_size	Overall size of the events with participation of the person

Scenario 6

As a result of scenario 6 execution, statistics on particular person for the specified period of time will be displayed.

```
Statistics on a given person id

Enter value for person_id: B37174C262444412B7AC8ECDCA544BD200000000
Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date:
Enter value for end_date:

'Ivanov Ivan'
 object_type | object_count | objects_size
-------------+--------------+--------------
 Email       |            3 | 109 kB
(1 row)
```

The following information will be shown in columns:

object_type	Event type
object_count	Count of events
objects_size	Overall size of the events with participation of the person

8.2.4 Database Backup

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

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

If, in addition to database, you use Data Storage, i.e. a storage of binary data, then back up the storage together with DB. This procedure is decribed together with DB backup creation.

This section further covers:

- Creating Database Backup;
- Резервное копирование базы данных.

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;
- Stopping PostgreSQL;
- Copying Database Files to Backup Storage;
- Creating Data Storage Backup.

Defining the Size of Backup

To define size of the future archive, it is necessary to find out summary size of following catalogues:

- a catalogue with PostgreSQL DB;
- a catalogue with the main tablespace;
- catalogues with daily tablespaces catalogues;
- the `/opt/dsdata/_seaweedfs` catalogue for storing data of Data Storage if you use it.

For this:

1. On the DB server, enter the system as the **root** user.
2. Get summary catalogue size:
   ```
   du -sx -BM /u01/postgres/ /u02/pgdata /u02/pgdata1 /u02/arch
   ```
3. On the Data Storage server, define size of the `/opt/dsdata/_seaweedfs` catalogue similarly.

If you use another storage mode, the data can be stored in different directories (for details, see *Configuring Storage Modes for Tablespace Files*).

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, the database and Data Storage are located on different computers.
   - Computers 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. Define 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 on a computer other than the database or Data Storage is located.

1. Log the system as **root** user.
2. Create the directory for backup files storage:
   `mkdir /opt/IWTM_Backup_Files`
3. Create subdirectories:
   ```
   mkdir /opt/IWTM_Backup_Files/postgres
   mkdir /opt/IWTM_Backup_Files/pgdata
   mkdir /opt/IWTM_Backup_Files/pgdata1
   mkdir /opt/IWTM_Backup_Files/arch
   ```

Stopping IWTM System

Stopping IWTM system is not required but we recommend doing it especially if there is little free space on IWTM server.

To stop IWTM system:

1. On each computer that hosts IWTM services, log in as **root**.
2. Stop all running Traffic Monitor Server services:
   `iwtm stop`
   You can start services later (when backup is finished) using the following command:
   `iwtm start`

Stopping PostgreSQL

> **Important!**
>
> Before backuping the database files, you should obligatorily stop the PostgreSQL database.

To stop PostgreSQL database:

1. On the computer that hosts the database, log on as the **root** user.
2. In the command line, enter:
   ```
   systemctl stop pgagent-15
   systemctl stop postgresql-15
   ```
   You can start services later (once backup is finished), using the following command:
   ```
   systemctl start pgagent-15
   systemctl start postgresql-15
   ```

Copying Database Files to Backup Storage

To copy database files:

1. Stop all PostgreSQL services (*Stopping PostgreSQL*). To make sure that all services are stopped, run the following command:

`ps aux | grep postgre`
If PostgreSQL services are not stopped, backup files can be damaged and unsuitable for recovery.
2. On the computer that hosts the database, copy data from DB directories to previously created directories. You need to copy all the contents of the directories including links.
If the system has been installed with the installer and default settings are not modified, then:
   - copy contents of the **/u01/postgres/** directory to the **/opt/IWTM_Backup_Files/postgres** directory
   - copy contents of the **/u02/pgdata/** directory to the **/opt/IWTM_Backup_Files/pgdata** directory
   - copy contents of the **/u02/pgdata1/** directory to the **/opt/IWTM_Backup_Files/pgdata1** directory
   - copy contents of the **/u02/arch/** directory to the **/opt/IWTM_Backup_Files/arch** directory

Important!

Use only the following devices as file storages:

- an external drive with Ext4 or XFS file system
- a remote block device connected via iSCSI or NFS protocol
- a locally connected block device with Ext4 or XFS file system

Creating Data Storage Backup

In Data Storage, Traffic Monitor data are stored in buckets. To back up the storage of binary data, you need to back up these buckets. This procedure consists of the following steps:

1. Enabling functionality of backup
2. Getting a token to work with the Data Storage service
3. Getting a list of buckets for backup
4. Creating the backup task
5. Checking successful completion of backup

During the backuping process you need to send requests using the **curl** utility. When doing this, you can specify the following values as a server address `<ADDRESS>`:

- **localhost:40731**, if you send requests from the server where Data Storage is installed.
- **<server_IP_address>:40732**, if you send requests from another server.

Enabling functionality of backup

To enable creating a backup of Data Storage, you need to specify a directory for that.

We recommend to do it when you install the storage. For this, run the installer using the `--dsbackupspath` parameter with the directory for backups.
Example: `./setup.py install --dsbackupspath=/opt/dsbackups`

To specify the directory after installation, add it to the Data Storage deployment. For this:

1. On the Data Storage server, create a directory for storing a backup:

```
mkdir /opt/dsbackups
```

2. Mount an external storage for backups into this directory. Requirements for the backup storage are described in the *Checking Backup Storage* article.
3. Set a user and access permissions for the created directory:

```
chown 1000 /opt/dsbackups
chmod 700 /opt/dsbackups
```

4. Open the Data Storage deployment for editing. For this use the command:

```
kubectl -n infowatch edit deployment datastorage-<node_label>
```

   where `<node_label>` (hereafter) is the label of the node where the storage is installed. For the central node or, if the storage is installed not in the cluster of Platform products, use the label `central`. For the office node, the label is specified during installation (`office` by default). The following actions depends on a text editor that you use. In our example, we use **vi**. To enter insert mode, press **i**.
5. Add the following lines to the `containers` -> `volumeMounts` section:

```
- name: datastorage-databackups-host-volume-<node_label>
  mountPath: /var/lib/databackups
  mountPropagation: HostToContainer
```

   In this and the next step, indent with spaces and do not use a tab.
6. Add the following lines to the `volumes` section:

```
- name: datastorage-databackups-host-volume-<node_label>
  hostPath:
    path: /opt/dsbackups
```

7. Save the changes and exit the editor.
   For example, if you use the **vi** editor, press **Esc** and type `:wq`.

Getting a token to work with the Data Storage service

To work with the Data Storage service, you need to get a Bearer token for HTTP authorization. In requests to Data Storage, specify it in the Authorization header.
The token value can become outdated. So in response to a request, the service returns the 440 HTTP code. In this case, get the token again.

To get the token, send the following request to Data Storage:

```
curl -X GET -I --silent "http://<ADDRESS>/v2/logon?extAPIToken=<DS_user_token>" 2>&1 | grep
'^Authorization'
```

where `<ADDRESS>` is the server address. For details, see above.
`<DS_user_token>` is the Data Storage authorization token. The default value: `1exwo92iwpczl1hy6jxy`.
To learn more, see *Configuring Connection with Data Storage*.

As a result, you will see the Authorization header in the following format:
`Authorization: Bearer <token_value>`

Getting a list of buckets for backup

To get a list of identifiers of Data Storage buckets which store Traffic Monitor data, connect to the Traffic Monitor database and run the query:

```
select distinct(storage_bucket_id) from iwtm.tbs_list;
```

If you need to know a list of all existing Data Storage buckets (their bucketID identifiers), send the following request to the storage service:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets?filter=*" 2>&1
```

where `<AUTH_HEADER>` is the Authorization header received on the previous step;
`<ADDRESS>` is the server address. For details, see above.

Results in the JSON format may look as follows:


```
{
  "data": [
    {
      "backendType": "seaweedfs",
      "id": "barbucket",
      "isDumped": false,
      "isInaccurate": false,
      "isSlowDrive": false,
      "size": 27632
    },
    {
      "backendType": "seaweedfs",
      "id": "bazbucket",
      "isDumped": false,
      "isInaccurate": false,
      "isSlowDrive": false,
      "size": 27633
    },
    {
      "backendType": "file",
      "id": "oldbucket",
      "isDumped": false,
      "isInaccurate": false,
      "isSlowDrive": false,
      "size": 27634
    }
  ]
}
```


Also you can filter the bucket list with a regular expression using the **jq** utility. For example, the following request will find all buckets whose bucket ID value begins with the "bar" substring:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets?filter=*" 2>&1 | jq --raw-output
'.data.[] | select(.backendType=="seaweedfs") | select(.id|test("^bar")).id'
```

Creating the backup task

To create a task of bucket backup, send the following request:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?bucketID=<BUCKET_ID>"
```

where `<AUTH_HEADER>` is the Authorization header;
`<ADDRESS>` is the server address. For details, see above;
`<BUCKET_ID>` is the bucket identifier.

In response, the ID of the created task will be displayed:

```
{
  "taskID": "fe8163f2-a0fb-4990-8bb7-87aee5c425bc"
}
```

Also you can create a bucket backup task and get the ID of this task using the **jq** utility:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?bucketID=<BUCKET_ID>" |
jq --raw-output '.taskID'
```

Next, you can check successful completion of bucket backup using the task ID.

Checking successful completion of backup

To make sure that backuping completed successfully, check the status of the task. For this, send the request:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?taskID=<TASK_ID>"
```

where `<AUTH_HEADER>` is the Authorization header;
`<ADDRESS>` is the server address. For details, see above;
`<TASK_ID>` is the task identifier.

If succesfull, you will see names of data and index files created in the backup directory:

```
{
  "bucketID": "foobucket",
  "dataFilename": "foobucket_0.tar.gz",
  "indexFilename": "foobucket_extindex.tar.gz",
  "taskStatus": "Success"
}
```

In case of failure, the error description will be displayed:

```
{
  "bucketID": "foobucket",
  "error": "permission denied: cannot extract data tarball",
  "taskStatus": "Success"
}
```

Make sure that the task is completed and has one of the following statuses: Success, Canceled, Failed.

Also you can get the task status using the **jq** utility:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?taskID=<TASK_ID>" | jq
--raw-output '.taskStatus'
```

Restoring Database from Backup

To restore the database and/or Data Storage:

1. Choose the appropriate method of database recovery if necessary:
    - If the database was damaged due to the system failure or user error, restore the old database. For example, if an important file has been occasionally deleted, you can restore the database to the state when this file still existed. For details, see *Restoring to the Same Database*.
    - If the old database cannot be used any more, create a new database and recover data to it. See *Restoring to a New Database*.
2. Follow one of the scenarios below. You can find required instructions in the followinf articles: *Stopping IWTM System*, *Stopping PostgreSQL* and *Restoring Data Storage*.

If you use Data Storage and it is not damaged then no action with the storage is required when restoring DB. Data Storage does not interact with the database directly.

To restore only DB:

1. Stop the Traffic Monitor services.
2. Restore the DB the chosen way.
3. Start the Traffic Monitor services.

To restore only Data Storage:

1. Stop the Traffic Monitor services.
2. Stop the database.
3. Restore Data Storage.
4. Start the database.
5. Start the Traffic Monitor services.
6. Make sure that Traffic Monitor is connected with Data Storage. If necessary, configure connection. For detailes, *Configuring Connection with Data Storage*.

To restore both DB and Data Storage:

1. Stop the Traffic Monitor services.
2. Restore Data Storage.
3. Restore the database.
4. Start the Traffic Monitor services.
5. Make sure that Traffic Monitor is connected with Data Storage. If necessary, configure connection.

> **Important!**
>
> If you need to update Traffic Monitor to a new version, you should first restore the database. Updating Traffic Monitor either before or during the database recovery is not supported.

Restoring to the Same Database

Below you can find instructions on how to restore data to a database that has the same directory structure as the one that was backed up.

To restore the database without 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 PostgreSQL services:
   ```
   systemctl stop postgresql-15
   systemctl stop pgagent-15
   ```
3. Take the following steps:
   a. Delete all the content of the **/u01/postgres/**, **/u02/pgdata/**, **/u02/pgdata1/**, **/u02/arch/** directories;
   b. Copy the content of the **/opt/IWTM_Backup_Files/postgres** directory to the **/u01/postgres/** directory;
   c. Copy the content of the **/opt/IWTM_Backup_Files/pgdata/** directory to the **/u02/pgdata/** directory;
   d. Copy the content of the **/opt/IWTM_Backup_Files/pgdata1/** directory to the **/u02/pgdata1/** directory;
   e. Copy the content of the **/opt/IWTM_Backup_Files/arch/** directory to the **/u02/arch/** directory.
4. Check the permissions. If necessary, change them:
   ```
   chown -R postgres /u01/postgres/
   chown -R postgres /u02/pgdata/
   chown -R postgres /u02/pgdata1/
   chown -R postgres /u02/arch/
   ```
5. Start the database:
   ```
   systemctl start postgresql-15
   systemctl start pgagent-15
   ```

Restoring to a New Database

To restore the database by creating a new one:

1. Install a new database and configure it according to the following article: *InfoWatch Traffic Monitor. Installation Guide. Configuring Remote Database*.

   > **Note:**
   >
   > If you have installed the DB on the same server, reinstall additional packages `pgagent` and `postgresql-contrib` during configuration by using the `--reinstall` parameter in the command.

2. Copy the content of the directories, check permissions and start the database services similarly to *Restoring to the Same Database*.
   You should copy DB files to the same directories, in which they were stored in the old database.

Restoring Data Storage

Restoring the storage of binary data lies in restoring buckets from their backups. This procedure consists of the following steps:

1. Getting a token to work with the Data Storage service
2. Creating the task of restoring bucket
3. Checking successful completion of the task

When sending **curl** requests, you can specify the following values as a server address `<ADDRESS>`:

- **localhost:40731**, if you send requests from the server where Data Storage is installed.
- **<server_IP_address>:40732**, if you send requests from another server.

Getting a token to work with the Data Storage service

To work with the Data Storage service, you need to get a Bearer token for HTTP authorization. In requests to Data Storage, specify it in the Authorization header.
The token value can become outdated. So in response to a request, the service returns the 440 HTTP code. In this case, get the token again.

To get the token, send the following request to Data Storage:

```
curl -X GET -I --silent "http://<ADDRESS>/v2/logon?extAPIToken=<DS_user_token>" 2>&1 | grep
'^Authorization'
```

where `<ADDRESS>` is the server address. For details, see above.
`<DS_user_token>` is the Data Storage authorization token. The default value: `1exwo92iwpczl1hy6jxy`.
To learn more, see *Configuring Connection with Data Storage*.

As a result, you will see the Authorization header in the following format:
`Authorization: Bearer <token_value>`

Creating the task of restoring bucket

To create a task of restoring bucket, send the following request:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?bucketID=<BUCKET_ID>"
```

where `<AUTH_HEADER>` is the Authorization header;
`<ADDRESS>` is the server address;
`<BUCKET_ID>` is the bucket identifier.

In response, the ID of the created task will be displayed:

```
{
  "taskID": "fe8163f2-a0fb-4990-8bb7-87aee5c425bc"
}
```

Also you can create the task of restoring bucket and get the ID of this task using the **jq** utility:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?bucketID=<BUCKET_ID>"
 | jq --raw-output '.taskID'
```

Next, you can check successful restoration of bucket using the task ID.

> **Important!**
>
> You can restore the bucket only if there is no one with the same ID in Data Storage.

Checking successful completion of the task

To make sure that restoration completed successfully, check the status of the task. For this, send the request:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?taskID=<TASK_ID>"
```

where `<AUTH_HEADER>` is the Authorization header;
`<ADDRESS>` is the server address.;
`<TASK_ID>` is the task identifier.

If succesfull, you will see the following response:

```
{
  "bucketID": "foobucket",
  "taskStatus": "Success"
}
```

Make sure that the task is completed and has one of the following statuses: Success, Canceled, Failed.

Also you can get the task status using the **jq** utility:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?taskID=<TASK_ID>" | jq
--raw-output '.taskStatus'
```

8.2.5 Database Server 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.

If you need to carry out routine maintenance on the database server, take the following steps:

1. Close all instances of the Management Console. Make sure that all connections of other programs to Traffic Monitor database scheme are closed; if there are any active connections, disable them.
2. Stop all TM processes on Traffic Monitor server:
   `iwtm stop`
   `systemctl stop iwtm-php-fpm`
   `systemctl stop nginx`
3. On the database server, retrieve the list of scheduled jobs. For this, in psql, run the following query as the database scheme owner:
   `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 jobs to be disabled.
5. To make sure that there are no running jobs, run the following query:
   ```
   select pga_job.jobname
   from pgagent.pga_job
   where pga_job.jobagentid is not null;
   ```
   A current task cannot be stopped in PostgreSQL, this should be done by stopping the agent from Linux using thy following command:
   `systemctl stop pgagent-15` (stopping all tasks with one command)
6. Make all the necessary operations with the database.
7. After all operations are complete, check the connection to the database server from Traffic Monitor server:
   ```
   psql postgres iwtm
   ```
   where `server_name` is database name or IP address
   If the test is successful, the following psql invitation will appear:
   `postgre=#` or `postgres=>`
8. Run the Traffic Monitor server processes:
   ```
   iwtm start
   systemctl start iwtm-php-fpm
   systemctl start nginx
   ```
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 the 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 the previously stopped jobs.

8.2.6 Database logging

Traffic Monitor saves logs of PostgreSQL database to `/u01/postgres/pg_log/postgresql.log` file. The System also generates logs on tasks running with pgAgent and saves them to `/u01/postgres/pg_log/pgagent-15.log` file.

PostgreSQL DBMS operation in Traffic Monitor is logged with a script. This script allows you to set the logging level and export log data to a CSV file. The script uses settings of the current configuration file: `/opt/iw/tm5/csw/database.conf`.

The script supports the following commands:

- To set the logging level, run the command:
  `/opt/iw/tm5/csw/postgres/scripts/sys_log/sys_log.sh level <level_value>`
  where `<level_value>` can be `debug`, `info`, `warning` or `error`.
  If you run the command without specifying the level value, the current logging level will be displayed.
- To export the log archive, run the command:
  `/opt/iw/tm5/csw/postgres/scripts/sys_log/sys_log.sh export`
  If necessary, you can set the number of lines to be exported:
  `/opt/iw/tm5/csw/postgres/scripts/sys_log/sys_log.sh export <number_of_lines>`
  The exported file gets a name of `iwtm_sys_log_<yyyy-mm-dd_hh-mm-ss>.csv.gz` format and is saved to the current directory.

On how logs are stored on the disk, see *Rotation of database logs*.

Rotation of database logs

Rotation of database logs is the process of archiving, storing, and deleting obsolete data in logs. This process is required to save space and free up disk space. In Traffic Monitor, rotation applies to the DB log in a text format: `/u01/postrges/pg_log/*.log`. This log file is rotated by the **logrotate** service. Rotation applies to each 100 MB of the file. When the number of files exceeds 100, the log file is deleted.

Settings of the **logrotate** service are stored in `/etc/logrotate.d/iwtm-pg-conf`.

9 Administrating the Server End of InfoWatch Traffic Monitor

This chapter describes Traffic Monitor server end components, their settings and how to use them:

- Traffic Monitor Server Processes;
- Configuring OCR;
- Configuring Settings for Processing Enclosed Archives;
- Configuring Settings of Search Using Wildcards;
- Configuring Integration with Data Analysis Service;
- Configuring Connection with Data Storage;
- Configuring Sending Events to Platform;
- Logging System Work;
- File Queues;
- Recovering the System after Failures;
- Managing Languages Including Morphological Support;
- Configuring Forwarding Data to SIEM;
- Deleting Temporary Files.

9.1 Traffic Monitor Server Processes

This section covers:

- List of Traffic Monitor Server End Processes;
- Setting Traffic Monitor Server End Configuration Files;
- Using Traffic Monitor Server End Processes.

9.1.1 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 the analysis, the response is sent to the ICAP client to allow/deny the delivery of the HTTP request. The HTTP request is passed to the **`iw_x2x`** process through the file queue, and then to the **`iw_x2db`** process.	`/opt/iw/tm5/etc/icap.conf`
	`iw_icap_buf`	Saves parts of a large file in its storage. Then, sends the created object as a complete file with a single request to **`iw_icap`** for analysis.	`/opt/iw/tm5/etc/icap_buf.conf`
	`iw_proxy`	Receives a copy of the traffic, divides it to HTTP, ICQ, and SMTP traffic, and sends it to the	`/opt/iw/tm5/etc/proxy.conf`

Purpose	Process name	Process description	Configuration file
		`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 and decision making subsystem **`iw_analysis`**. • `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 and decision making subsystem **`iw_analysis`**. • `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 **`iw_messed`** analysis subsystem. After the analysis is complete, the object is passed to the **`iw_x2x`** process and then to the **`iw_x2db`** process.	
	`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 email) is transferred to the analysis and decision making subsystem. After the analysis, **`iw_messed`** transfers the allowed SMTP messages to the mail	`/opt/iw/tm5/etc/messed.conf`

Purpose	Process name	Process description	Configuration file
		system component that delivers mail (only in the normal and transparent transport modes). If integration with the 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. The checked SMTP email is passed to the **iw_x2x** process via the file queue, and then to the **iw_x2db** process.	
	iw_xapi	Includes 2 services: **iw_xapi_xapi** and **iw_xapi_puppy**. Receives objects from Device Monitor and external systems (through adapters) via the Thrift interface and places them in a file queue. Then it sends objects to the **iw_analysis** process. When receiving EML objects, sends them to the **iw_messed** process.	/opt/iw/tm5/etc/xapi.conf
	iw_analysis	Takes objects from the file queue, previously placed there by **iw_xapi_xapi** / **iw_xapi_puppy**, **iw_proxy_icq**, **iw_proxy_http**. By means of the file queue it transmits objects to **iw_warpd**, **iw_cas**, **iw_pas**, **iw_luaengined** for processing. Then it sends the objects to the file queue for sending to the **iw_x2x** process, and then to the **iw_x2db** process.	/opt/iw/tm5/etc/analysis.conf /opt/iw/tm5/etc/analysis_client.conf – client configuration file for connecting to iw_cas and iw_pas
	iw_rest2push	Allows receiving objects from external systems via the HTTP/HTTPS protocol. Connects to the iw_xapi_puppy service, sends events via the Thrift protocol.	/opt/iw/tm5/etc/rest2push.conf
Data processing	iw_warpd	Manages processes of extracting data from containers enclosed in intercepted objects.	/opt/iw/tm5/etc/warpd.conf
	iw_image2text_fre	Recognizes text in images using OCR Content AI ContentReader Engine.	/opt/iw/tm5/etc/image2text_fre.conf
	iw_image2text_ts	Recognizes text in images using OCR Tesseract.	/opt/iw/tm5/etc/image2text_ts.conf
	iw_cas	Takes the role of the content analysis server. Interception subsystems send text requests in plain text format to the **iw_cas** process for content analysis. When the analysis is complete,	/opt/iw/tm5/etc/cas.conf

Purpose	Process name	Process description	Configuration file
		the request result is sent to the analysis and decision-making subsystem.	
	`iw_image_autoling`	Takes the role of the graphic objects automatic classifier.	`/opt/iw/tm5/etc/iw_image_autoling.conf`
	`iw_text_autoling`	Takes the role of the text objects automatic classifier.	`/opt/iw/tm5/etc/iw_text_autoling.conf`
	`iw_pas`	Receives analysis results from **`iw_cas`**. Defines the presence of a protected object 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` `/opt/iw/tm5/etc/lua.conf` – client configuration file for connecting to `iw_luaengined`
	`iw_x2x`	The process gets data with XML+DAT files via the file queue. The files provided are modified and sent to the **`iw_x2db`** process.	`/opt/iw/tm5/etc/x2x.conf`
	`iw_tech_tools`	Verifies conditions for DB unloadings and regular expressions, 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 in a branch office. Sends intercepted objects to the headquarters' DB.	`/opt/iw/tm5/etc/qmover_client.conf`
	`iw_qmover_server`	Works on the Traffic Monitor server installed in the central office. Gets objects received from the Agent installed in the branch office. Sends objects to the **`iw_x2db`** process through **`iw_x2x`** for saving to the DB.	`/opt/iw/tm5/etc/qmover_server.conf`
	`iw_x2db`	Loads objects verified by the analysis and decision making systems from the output file queue of the **`iw _x2x`** process to the DB.	`/opt/iw/tm5/etc/x2db.conf`

Purpose	Process name	Process description	Configuration file
Infrastructure	`iw_adlibitum`	Manages processes of receiving actual data from the Active Directory, Domino Directory, Samba DC, Alt Domain, Astra Linux Directory, Astra Linux Directory Pro, and FreeIPA servers.	`/opt/iw/tm5/etc/adlibitum.conf`
	`iw_agent`	Required for managing the System configuration.	`/opt/iw/tm5/etc/agent.conf`
	`iw_attributor`	Enables interaction with Data Analysis Service: transfers data for analysis and loads the received data to the DB.	`/opt/iw/tm5/etc/attributor.conf`
	`iw_blackboard`	Provides a Thrift interface to read a file queue of commands and delegates their execution to other services. The commands include adding statuses and contacts to persons, updating meta information about contacts, adding statuses to workstations, sending notifications about events, adding applications to lists.	`/opt/iw/tm5/etc/blackboard.conf`
	`iw_bookworm`	Acts as a reference book in the System.	`/opt/iw/tm5/etc/bookworm.conf` `/opt/iw/tm5/etc/bookworm.conf` `/opt/iw/tm5/etc/bookworm_client.conf` – client configuration file for connecting to `iw_bookworm`.
	`iw_cas_config_compiler`	Converts the configuration file of the content analysis server to a 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_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 the **`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`

Purpose	Process name	Process description	Configuration file
	`iw_metainfo_fetcher`	Selects data from the DB containing meta information about all contacts, including contacts participating in events (for indexing). Sends them to the **`iw_is`** process.	–
	`iw_audit_fetcher`	Selects extended audit events from the DB for indexing. Sends them to the **`iw_is`** process.	–
	`iw_is`	Manages the data indexing process and the operation of search servers for full-text search. Prepares the files with data description, which get to the indexer through the file queues, and starts the indexer.	`/opt/iw/tm5/etc/is.conf`
	`iw_indexer`	Indexes the text in events from the DB. Gets access to the DB for indexing it and adds indexes to the file storage. When a **`sphinx`** search query is running, receives object IDs from the file storage of indexes.	`/opt/iw/tm5/etc/indexer.conf`
	`iw_kicker`	Enables operation of WebGUI and starts the following services: `agent`, `blackboard`, `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` `/opt/iw/tm5/etc/license.conf` – client configuration file for connecting to `iw_licensed`
	`iw_rammer`	Sends emails with processing errors when working inline.	`/opt/iw/tm5/etc/rammer.conf`
	`iw_sample_compiler`	Creates fingerprints from uploaded sample files.	`/opt/iw/tm5/etc/sample_compiler.conf`
	`consul`	Detects, registers, and monitors availability of services which interact with the user interface.	`/opt/iw/tm5/etc/consul/consul.json`

Purpose	Process name	Process description	Configuration file
	`iw_system_check`	Collects data from the Nagios service and provides it for display in the Management Console.	`/opt/iw/tm5/etc/system_check.conf`
	`iw_updater`	Loads the configuration from the DB to the Traffic Monitor server.	`/opt/iw/tm5/etc/updater.conf`
	`iw_space_manager`	Manages tablespaces in the **Tablespaces** section of the Management Console.	`/opt/iw/tm5/etc/space_manager.conf`

9.1.2 Setting Traffic Monitor Server End Configuration Files

You can find the list of System configuration files and their settings that can be changed to configure the System for operation in your organization in the *InfoWatch Traffic Monitor. Configuration Files Guide* document. We recommend not editing files that are not described in this document.

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

The System configuration files are in JSON format. Configuration file names match the names of corresponding System components to be configured. For example, for configuring **iw_x2x** component, **x2x.conf** configuration file is used**.**

There are common configurable settings and parameters specific for each configuration file

See the document *InfoWatch Traffic Monitor. Configuration Files Guide:*

- common configurable settings:
  - *General section Bookworm;*
  - *General section Discovery;*
  - *General section Logging;*
  - *General section Statistics;*
  - *General section Statistic;*
  - *General section ThriftServers.*
- parameters specific for each configuration file.

9.1.3 Using Traffic Monitor Server End Processes

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

All Traffic Monitor Server processes are launched under `iwtm` user, which is 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 unit files of processes in `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 bash script `/opt/iw/tm5/bin/iwtm` which is an autorun script for run levels 2, 3, 4, 5.

Note:

- The `iw_qmover_server`, `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.
- The `iw_rammer` process is not installed by default. After manual installation, the process is available in the process list.
- In case you have to stop services on servers of a distributed Traffic Monitor cluster, first stop processes on a server installed with the *Interceptors* template, and at the end stop processes on a *Database* server. To start processes, begin with a server installed with the *Database* template and finish with *Interceptors*.
- If Traffic Monitor Server uses Data Storage, actions for stopping/starting processes are the same as without the storage.

Start keys for `iwtm` script:

Start key	Purpose
`start`	Starting processes
`stop`	Safe stop of processes
`status`	Displaying process state (running/not started/available/ unavailable)
`restart`	Restarting processes (sequential execution of start+stop commands)
`reload`	Reloading process configuration
`kill`	Transmitting a signal to immediately end the process (SIGKILL)
`test`	Displaying all available iwtm daemons
`enable`	Setting the "available" status to a daemon - the daemon autostart is allowed
`disable`	Setting the "unavailable" status to a daemon - the daemon autostart is forbidden
`services_state`	Displaying all available iwtm daemons with bit masks

Sample commands

Command	Action
`iwtm status`	Check the state of Traffic Monitor Server processes

One of the following commands:
`service iw_cas start` (if you need to view logs)
`iwtm start cas`
`iwtm start iw_cas`
`iwtm start iw_cas.service`
`systemctl start iw_cas` (viewing logs is unavailable)
`systemctl start iw_cas.service`
	Start the content analysis server (CAS)

> **Warning!**
>
> PID files are stored in `/opt/iw/tm5/run` directory. In case of an 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 Autorun*.

For each process managed by **iwtm** bash script, autorun parameters can be specified in a command line. Enabling/disabling autorun for processes (with `iw_sniffer` service as an example) is described in *Enabling and Disabling Process Autorun*. For details about systemd commands see article *Commands to work with systemd*.

9.1.4 SSL Thrift Encryption

To use encryption:

1. Prepare a key and certificates.
2. Stop Traffic Monitor services. Use the command:

   ```
   iwtm stop
   ```

3. Edit the ThriftServers and ThriftClients sections in configuration files of servers that will use SSL Thrift connection.
4. In `ssl` section of the `/opt/iw/tm5/etc/web.conf` file, specify `true` for the services that will use the SSL Thrift connection.
   For example:

   ```
   "ssl": {
       "iw_xapi_puppy": true,
   ```

```
    "iw_adlibitum": false,
    "iw_blackboard": false,
    "iw_bookworm": false,
    "iw_agent": false,
    "iw_licensed": true,
    "iw_sample_compiler": false,
    "iw_image_autoling": true,
    "iw_text_autoling": true,
    "iw_system_check": false,
    "iw_tech_tools": false
},
```

5. Start the services:

```
iwtm start
```

Important!

If encryption was enabled before updating Traffic Monitor to version 7.15, make sure configuration files contain your changes.

Preparing a key and certificates

For encryption, you need:

- Trusted root certificate (CA). After Traffic Monitor installation, it is available in `/opt/iw/tm5/etc/cert/trusted_certificates`;
- Certificate signed by the root certificate (CA). After Traffic Monitor installation, it is stored in `/opt/iw/tm5/etc/cert/server.pem`;
- Private key. After Traffic Monitor installation, it is stored in `/opt/iw/tm5/etc/cert/private_key.pem`.

You can:

- Use the preinstalled certificates and key (the locations are specified above);
- Generate and use your own certificate and key.

To prepare your own certificates and key:

1. Backup preinstalled certificates located in `/opt/iw/tm5/etc/cert`.

   Note:

   The instruction uses the names of preinstalled certificates for the new ones.

2. Create a private key. Use the the command:

```
openssl genrsa -out ca.key 4096
```

3. Create a self-signed root certificate (CA). Use the command:

```
openssl req -x509 -new -key ca.key -out trusted_certificates -days 3650 -subj "/C=RU/
ST=Moscow/L=Moscow/O=MyOrg/CN=My Internal CA"
```

where:

- `C` is the country;
- `ST` is the region;
- `L` is the city;
- `O` is the organization name;
- `CN` is the product/service name.

4. Create a private key for the server. Use the command:

```
openssl genrsa -out private_key.pem 2048
```

5. Create a certificate-signing request (CSR). Use the command:

```
openssl req -new -key private_key.pem -out server.csr -subj "/C=RU/ST=Moscow/O=MyOrg/
OU=Department/CN=XAPI"
```

where:

- `C` is the country;
- `ST` is the region;
- `L` is the city;
- `O` is the organization name;
- `OU` is the organizational unit/department name;
- `CN` is the product/service name.

6. Sign the request with your root certificate (CA). Use the command:

```
openssl x509 -req -in server.csr -CA trusted_certificates -CAkey ca.key -CAcreateserial
-out server.pem -days 365
```

> **Important!**
>
> In case you are planning to use different certificates for different nodes and services, generate and sign each server certificate with the root certificate (CA).
>
> Use the same root certificate (CA) for all nodes and services.

7. On each Traffic Monitor node:
   a. Copy root certificate (CA) from `/opt/iw/tm5/etc/cert/trusted_certificates`. No other folder is supported.
   b. Copy the server certificate from `/opt/iw/tm5/etc/cert/server.pem`.
   c. Copy the private key from `/opt/iw/tm5/etc/cert/private_key.pem`.
8. Change the owner of all files in the `/opt/iw/tm5/etc/cert` folder. Use the command:

```
chown -R iwtm:iwtm /opt/iw/tm5/etc/cert
```

Editing configuration files

You can set up Thrift connection in configuration files:

- `/opt/iw/tm5/etc/image_autoling.conf`
- `/opt/iw/tm5/etc/cas.conf`
- `/opt/iw/tm5/etc/agent.conf`
- `/opt/iw/tm5/etc/system_check.conf`
- `/opt/iw/tm5/etc/pas.conf`
- `/opt/iw/tm5/etc/luaengined.conf`
- `/opt/iw/tm5/etc/blackboard.conf`
- `/opt/iw/tm5/etc/sample_compiler.conf`
- `/opt/iw/tm5/etc/licensed.conf`
- `/opt/iw/tm5/etc/adlibitum.conf`
- `/opt/iw/tm5/etc/bookworm.conf`
- `/opt/iw/tm5/etc/text_autoling.conf`
- `/opt/iw/tm5/etc/xapi.conf`
- `/opt/iw/tm5/etc/tech_tools.conf`
- `/opt/iw/tm5/etc/messed.conf`

Edit the following sections:

- `ThriftServers`, for services to which clients connect;
- `ThriftClients`, for services that connect to servers.

By default, encryption is disabled in configuration files.

To enable encryption, make changes in both sections:

- In the `TransportType` parameter, specify `ssl`.
- In the `CertificatePath`, `PrivateKeyPath` and `TrustedCertificatesPath` parameters, specify paths to:
  - The client certificate signed by the root certificate;
  - The private key;
  - The root key.
- To enable authentication, specify `true` in `AuthenticateClient` parameter.
- To install an encryption version of the protocol for SSL sockets to at least TLS 1.2 and exclude all algorithms from the 3DES and RC4 groups from available encryption algorithms, specify `false` in the `UseLegacySSL` parameter.

Besides, in the `Port` parameter of the `ThriftServers` section, specify the port of incoming connections depending on the service:

- `adlibitum` – 9096
- `agent` – 9099
- `blackboard` – 9093
- `bookworm` – 9090
- `cas` – 9987
- `image_autoling` – 9103
- `text_autoling` – 9104
- `licserv` – 9095

- `luaengined` – 9988
- `pas` – 9989
- `sample_compiler` – 9091
- `system_check` – 9097
- `tech_tools` – 9102
- `puppy` – 9101
- `xapi` – 9100

See more on section parameters in *InfoWatch Traffic Monitor. Configuration files guide*.

Important!

For successful connection, key and client and server certificates (`ThriftClients` , `ThriftServers`) should be signed with the same root certificate.

9.2 Configuring OCR

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

- Intercepted images;
- Images loaded as sample documents.

The following processes are used for the technology operation:

- **`iw_warpd`** extracts data from containers included into intercepted objects;
- **`iw_sample_compiler`** creates digital prints from downloaded sample documents.

Using the configuration files of these processes, you can configure OCR technology usage. For details, see *Configuring OCR Extractors*.

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

Interception level	Settings apply to the content of events	Priority of the setting
Service	Received via protocols of event types which belong to this service (if OCR settings are not specified for these event types or protocols)	Low
Event type for a particular service	Received via protocol of this event type (if OCR settings are not specified for these protocols)	Medium
Protocol for a particular event type	Received via 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` catalogue:

- `ocr.xml` – preset settings;
- `ocr_custom.xml` – custom settings for a specific type of implementation.

Important!

When you update the System to current version, 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 remain within the `ocr_custom.xml` file.

9.2.1 Enabling OCR technology when implementing the System

You can enable using OCR technology when you implement the System. For this, modify the `ocr_custom.xml` file (for details see *Configuration File ocr_custom.xml*) the following way:

1. Select required objects: services, protocols, and event types[1].
2. Set identifiers for service directory objects and event types (files with a description are located in the `/opt/iw/tm5/etc/config/bookworm/` catalogue).
3. Enable OCR (`ocr_enabled="true"`).

Note:

[1] New event types registered via plugins are added to `/opt/iw/tm5/etc/config/bookworm/services.xml`. They can be processed or moved to the `ocr_custom.xml` file.

9.2.2 Configuring OCR on several nodes

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 catalogue `/opt/iw/tm5/etc/config-perm/bookworm`, create a new XML file that will describe the node.
2. Specify the created XML file in `CustomNodeXMLPath` section of configuration file `/opt/iw/tm5/etc/bookworm.conf`.
3. In `<ocr_option node>` parameter, specify instance name from `/opt/iw/tm5/node_name` file.
4. Define overridable rules for the instance as described above.

Note:

In this case, settings have the following priority (in descending order):

- Catalogue with settings for the server instance;
- Catalogue with custom settings;
- Catalogue with preset settings.

9.2.3 Configuration File ocr_custom.xml

Below you may find disabled OCR rules, where:

- `object_type` – object type;

- `service` – services;
- `protocol` – protocols;
- `key` – keys;
- `mnemo` – catalogues objects IDs of object types, services and protocols.

When enabling the rules, it is recommended specifying only the required ones:

```
<ocr_options node="*" ocr_enabled="false">
  <service key="CE6D8E0E27DA11E2962FC1DB6088709B00000000" mnemo="email" ocr_enabled="false">
    <object_type key="D2B5132E27DA11E28444C2DB6088709B00000000" mnemo="email" ocr_enabled="false">
      <protocol key="501A9868F3460E2E5AAF0C6AB21F8D6F63C09109" mnemo="pop3" ocr_enabled="false"/>
      <protocol key="2ECB2A264E31677895BC5D8845D33BC26F637CDF" mnemo="imap" ocr_enabled="false"/>
      <protocol key="A324CCB227DA11E2A8D99FDB6088709B00000000" mnemo="smtp" ocr_enabled="false"/>
      <protocol key="5F7E60DB3E86EFF90FDA87E72209EA1B0E017F16" mnemo="mapi" ocr_enabled="false"/>
      <protocol key="93B79EB44EE1A45522C08319EC47B499294776D7" mnemo="nrpc" ocr_enabled="false"/>
    </object_type>
    <object_type key="D8333C9027DA11E29E34CADB6088709B00000000" mnemo="email_web" ocr_enabled="false">
      <protocol key="A779DB3627DA11E2ADDCA0DB6088709B00000000" mnemo="http" ocr_enabled="false"/>
      <protocol key="7ED97C84BDBDD99C1C21AC0A6D6191F6A891C440" mnemo="https" ocr_enabled="false"/>
    </object_type>
  </service>
  <service key="DD6ECB5227DA11E2B507CBDB6088709B00000000" mnemo="im" ocr_enabled="false">
    <object_type key="E266719627DA11E2A83ECCDB6088709B00000000" mnemo="im_icq" ocr_enabled="false">
      <protocol key="ABA5D02027DA11E2B78FA1DB6088709B00000000" mnemo="oscar" ocr_enabled="false"/>
    </object_type>
    <object_type key="EEC2D87627DA11E29EA6D2DB6088709B00000000" mnemo="im_mail_ru" ocr_enabled="false">
      <protocol key="B8C7FC6A27DA11E2A080B7DB6088709B00000000" mnemo="mmp" ocr_enabled="false"/>
    </object_type>
    <object_type key="F249A80827DA11E29BA2D3DB6088709B00000000" mnemo="im_skype" ocr_enabled="false">
      <protocol key="DD3D593857521DE2E9618C26FD3E1B914F8A16F9" mnemo="skype" ocr_enabled="false"/>
    </object_type>
    <object_type key="E7C3A26C27DA11E296D3CDDB6088709B00000000" mnemo="im_xmpp" ocr_enabled="false">
      <protocol key="AF69EA3427DA11E2BE09A2DB6088709B00000000" mnemo="xmpp" ocr_enabled="false"/>
    </object_type>
  </service>
  <service key="62E7C68AD1354D118282FAFF07DA59ED00000000" mnemo="multimedia" ocr_enabled="false">
    <object_type key="55E10E81F5C94B3FB742CB61CA9476F800000000" mnemo="multimedia_photo"
ocr_enabled="false"/>
  </service>
  <service key="0794BBB227DB11E2BD81E9DB6088709B00000000" mnemo="web" ocr_enabled="false">
    <object_type key="0CAFCC9027DB11E2AD27EDDB6088709B00000000" mnemo="web_common" ocr_enabled="false">
      <protocol key="A779DB3627DA11E2ADDCA0DB6088709B00000000" mnemo="http" ocr_enabled="false"/>
      <protocol key="7ED97C84BDBDD99C1C21AC0A6D6191F6A891C440" mnemo="https" ocr_enabled="false"/>
    </object_type>
  </service>
  <service key="111CBA0427DB11E2AB82EEDB6088709B00000000" mnemo="file" ocr_enabled="false">
    <object_type key="1515A7B027DB11E2BBB2EFDB6088709B00000000" mnemo="file_exchange" ocr_enabled="false">
      <protocol key="BEFB1A7C27DA11E2AB10B8DB6088709B00000000" mnemo="ftp" ocr_enabled="false"/>
    </object_type>
    <object_type key="190D004827DB11E287B1F0DB6088709B00000000" mnemo="file_copy_out" ocr_enabled="false"/>
  </service>
  <service key="1DA8A90427DB11E289E8F5DB6088709B00000000" mnemo="print" ocr_enabled="false">
    <object_type key="225BD8F427DB11E2926DF9DB6088709B00000000" mnemo="print_common" ocr_enabled="false"/>
  </service>
  <service key="7843FC5BEA024E9B274E26DB43B7E680D8BC9356" mnemo="placement" ocr_enabled="false">
    <object_type key="602A224D9335579214E3188D1D2745DB9F85D500" mnemo="crawler" ocr_enabled="false"/>
  </service>
</ocr_options>
```

```
<ocr_options node="*" ocr_enabled="false">
</ocr_options>
```

Note:

To enable OCR on all the levels at one time (service level, event type and protocol level), at the end of the `ocr_custom.xml` file replace the line:

```
<ocr_options node="*" ocr_enabled="false">
```

with the following:

```
<ocr_options node="*" ocr_enabled="true">
```

9.3 Configuring Settings for Processing Enclosed Archives

The attachment processing is configured in the following configuration files:

- `/opt/iw/tm5/etc/`**`extractors.conf`** (see *InfoWatch Traffic Monitor. Configuration Files Guide. extractors.conf*);
- `/opt/iw/tm5/etc/config-perm/bookworm/`**`extractors.xml`** file (see *The extractors.xml Configuration File*);
- `/opt/iw/tm5/etc/config-perm/bookworm/`**`extractors_customization.xml`** file (see *The extractors_customization.xml Configuration File*).

Important!

If MS Exchange uses a journal rule, then, for the correct processing of such emails, enable the corresponding option in Traffic Monitor. For this, in the `messed.conf` configuration file, specify:

```
"ExchangeJournalReports": true,
```

To make the option active, reload the configuration, or restart the service.

9.3.1 The extractors.xml Configuration File

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

Parameter	Description and configuration examples
`FilenameCharsets`	GHz The default values are `UTF-8`, `cp1251`, `cp866`

`MinFileSizeInBytes`	Minimum file size (in bytes) subjected to unpacking. This limit lets you increase the System performance by avoiding to unpack small files. The default value is `10` **Note:** • the setting also applies to *Clipboard* events, i.e. the System does not process clipboard text if its volume is less than the value specified; • the setting does not apply to *Keylogger* events; • for the XML extractor, the default value is `76`
`MaxTextPlainSizeInKb`	Maximum size of a file whose signature is not defined. When the threshold is exceeded, the file is automatically considered to be binary and is not sent to `iw_cas` The default value is `25600`
`SpeedInKBs`	<TimeoutInSec> The default value is `100`
`TimeoutInSec`	Waiting time till file processing ends (in seconds). The default value is `0`
`UseLog`	Extractor logging. The default value is `false`

If the general values of parameters specified in the `<extractor_defaults>` section are not appropriate for some file types, then enable these parameters in the section for required file types with different values.

Example:

You can calculate the extractor operating time by the formula:

The extractor operating time = File size in KB / 1024 / (`SpeedInKBs` * CPU clock speed in MHz / 1000)

Other sections define signatures used for detection of file types from archives and enclosures. Each section contains the following set of parameters:

Parameter	Description and configuration examples
`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`
`Name`	Format name. Used for exact detection of format name when unpacking files.

Parameter	Description and configuration examples
	To define/specify the format, can 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` , the file is considered as having `name1` format. The list of names can include a default name (`defaultname`) which will be assigned when the code is not assigned: • **Example 1** (one format name): `text/xml` • **Example 2** (list of format names): `"application/arj, UNKNOWN(9), text/encrypted(4)"` By default, the file format is defined as `application/arj` . If the archive format cannot be determined, it is assigned the name `UNKNOWN` . For encrypted archives, the format name `text/encrypted` is used.
`Signature`	Format signature which is a "sample" sequence of values (bytes) with initial offset 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 triads of the following format: `[OFFSET]:BYTE_VALUE/[MASK]` There can be a string signature like " `BZh` " for BZIP2. This signature means specified bytes sequence from offset 0. The search of string signatures is not case-sensitive. 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 the first `N` bytes of a file. For example, to search for a pattern in the first 500 bytes of a file, specify the offset ' `500?` '. The `MASK` setting is optional and equals to `0xFF` by default. **Example** (signature of a header of a WAV format): `Sign = "'RIFF', 0x8: 'WAVEfmt'"` Starting from offset 0, there is a sequence ' `R` ',' `I` ',' `F` ',' `F` ', then from offset 8 there should be ' `W` ',' `A` ',' `V` ',' `E` ',' `f` ',' `m` ',' `t` '
`Comment`	The explanation commentary. **Example** (indicating the version of archiving utility): `Comment = "bzip2 v. 1.0.x"`
`Command`	Command string for file extracting. **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 a file to unpack.

Parameter	Description and configuration examples
`ExcludeFromContext`	If the parameter is enabled (`true`), then the object is unpacked but information on archiving utility is not added to the object's XML-context. This lets to exclude fictional containers like MS-TNEF from the object's context. By default, the parameter is enabled.
`CaseInsensitive`	Indicates whether file processing is case-sensitive. The default value is `false`
`CreateTags`	Indicates whether to extract metadata from a file. The default value is `true`
`Archive`	Regulates the kind of retrieved information: • `true` – files; • `false` – data.
`PIRegexp`	Contains a description of PIRE signature for file format detection. Can be specified several times within 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 attempts to open a FIFO queue.
`OpenFifoRetryCount`	Number of attempts to open the FIFO queue.
`ResultCharset`	Specifies the code of extracted text.
`NeedProcess`	If the files with MIME type specified should be sent for analysis.

Note:

Some intercepted files of XML format may contain sensitive data specified within XML tags of file markup. By default, the System does not extract text from tags. To configure text extraction from XML tags:

1. Open the **/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml** file for editing.
2. Find the element with the following contents:

```
<Command>bin/text-extractor -t xml -i ${OUTDIR}</Command>
```

3. Replace `-t xml` parameter with `-t xmltxt`
4. Save the changes and close the file.
5. Reload the configuration of the `iw_bookworm` process by running the command:

```
iwtm reload bookworm
```

6. Restart the processes:

```
iwtm restart analysis
iwtm restart messed
iwtm restart icap
```

As a result, the extracted text will include XML tags and other service information that is not preserved in the standard method of extracting text from XML.

9.3.2 The extractors_customization.xml Configuration File

In `/opt/iw/tm5/etc/config-perm/bookworm/extractors_customization.xml` file, you can add or adjust extractor settings specified in `/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml`.

Parameter	Description	Example setting
`<Signature>`	Format signature, which is a "sample" sequence of values (bytes) with initial offsets and masks. This sequence is required for unambiguous definition of file format by its content. The signature can include up to 16 triads of the following format: `[OFFSET]:BYTE_VALUE/[MASK]` There can be a string signature like "`BZh`" for BZIP2. This signature means specified bytes sequence from offset 0. The search of string signatures is not case-sensitive. Optional parameters: • `OFFSET` To specify the offset, use the "`?`" symbol. This will enable searching for a pattern in first `N` bytes of a file. For example, to search the pattern in the first	Example for a WAV-header signature: `Sign = "'RIFF', 0x8: 'WAVEfmt'"` Starting from offset 0, there is a sequence '`R`','`I`','`F`','`F`', then from offset 8 there should be '`W`','`A`','`V`','`E`','`f`','`m`','`t`'

	500 bytes, specify the offset "`500?`" • `MASK`	
`<FilenameCharsets>`	If file name encoding differs from the standard one (ANSI, UTF), the file will be processed as corresponding to the encodings specified in this parameter. Several values are listed comma-separated; the System sequentially tries to process the file in listed encodings while it finds a matched one.	`UTF-8`, `cp1251`, `cp866`
`<SpeedInKBs>`	Proposed extractor's operation speed per 1 GHz of the processor (in Kb/s). Can take integer values from 1 and greater.	`100`
`<UseLog>`	Extractor logging.	• `true` – use • `false` – do not use
`<TimeoutInSec>`	Waiting time till file processing ends (in seconds).	`1000`
`<MinFileSizeInBytes>`	Minimum file size (in bytes) subjected to unpacking. This limit lets you increase the System performance by avoiding to unpack small files. **Note:** • files smaller than 10 bytes are not supported. This restriction also applies to the *Clipboard* event type. • for the XML extractor, the default value is `76`	`1024`
`<MaxTextPlainSizeInKb>`	Maximum size of a file whose signature is not defined. When the threshold is exceeded, the file is automatically considered to be binary and is not sent to `iw_cas`	`25600`
`<PreCommand>`	Command to be executed before or after data extraction.	`bin/dwg-extractor -i ${SRC} -t ${OUTDIR}/out.txt -u ${OUTDIR}/out.vectxt`
`<PostCommand>`		

Note:

Some System-intercepted JPEG files can be linked with archives potentially containing sensitive data. By default, the System does not extract text from such files. To configure text extraction for such JPEG files:

1. Open the file **extractors_customization.xml** for editing:
2. Inside the `<extractors>` element, paste the element with the following contents:

```
<extractor profile_name="jpg" key="dY5k14hWa0nivGOvSP4BUe0vTJdME5IY4xjNsqKl">
        <PostCommand>bin/7zz x -y -p{} ${SRC} -o${OUTDIR}</PostCommand>
</extractor>
```

3. Save your changes and close the file.
4. Restart the Traffic Monitor processes:

```
iwtm restart
```

9.4 Configuring Settings of Search Using Wildcards

When creating a query in the "**Events**" section of Traffic Monitor Management Console, you can specify senders and recipients. To specify values of their contacts or contacts metadata, you can use wildcards at the end of the string. For search using wildcards, the System considers contacts and their metadata as keywords and indexes all possible prefixes of keywords. Prefix is an initial part of a word. If System searches for a certain prefix in an index, then it finds all keywords containing the prefix.

The System perfoms indexing starting with the minimum prefix length that is determined by the parameter `min_prefix_len` in the `is.conf` file. By default, the `min_prefix_len` value is 3.

Example:

There are users having *ex_user*, *exact_user* и *example_user* logins. The `min_prefix_len` value is 3.

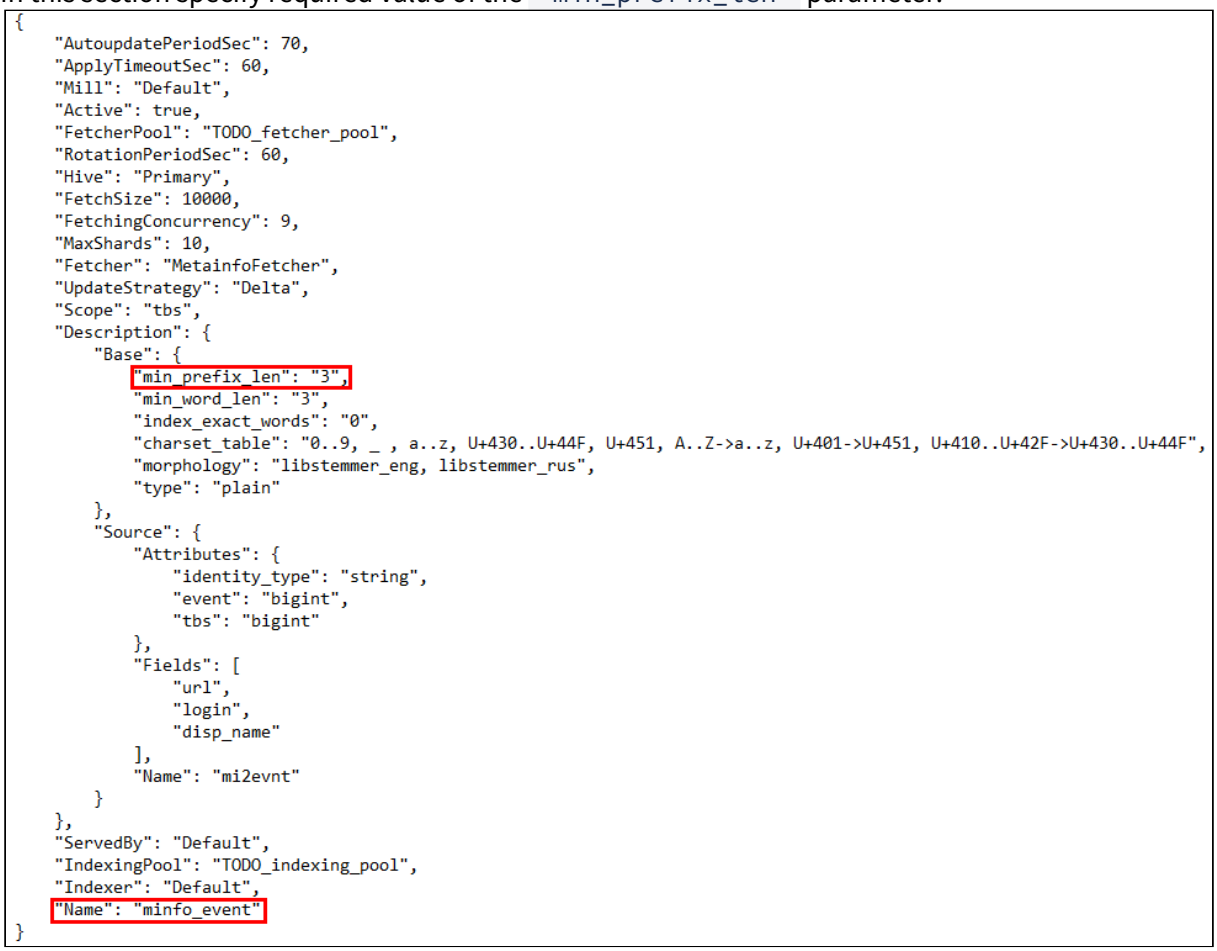
If you create a query with the `"exa*"` mask, then as a result the events with *exact_user* and *example_user* are to be found. At the same time a query with the `"ex*"` mask will not return any result.

If you change the `min_prefix_len` value to 2, then the result of the search for `"ex*"` mask will contain events with all three users – *ex_user*, *exact_user* and *example_user*.

To change the prefix minimum length:

1. On Traffic Monitor server, go to the `/opt/iw/tm5/etc/` directory.
2. Open the `is.conf` file.
3. In the `"Indices"` root field, find the section with the `"Name": "minfo_event"` parameter.

4. In this section specify required value of the `"min_prefix_len"` parameter.



```
{
    "AutoupdatePeriodSec": 70,
    "ApplyTimeoutSec": 60,
    "Mill": "Default",
    "Active": true,
    "FetcherPool": "TODO_fetcher_pool",
    "RotationPeriodSec": 60,
    "Hive": "Primary",
    "FetchSize": 10000,
    "FetchingConcurrency": 9,
    "MaxShards": 10,
    "Fetcher": "MetainfoFetcher",
    "UpdateStrategy": "Delta",
    "Scope": "tbs",
    "Description": {
        "Base": {
            "min_prefix_len": "3",
            "min_word_len": "3",
            "index_exact_words": "0",
            "charset_table": "0..9, _ , a..z, U+430..U+44F, U+451, A..Z->a..z, U+401->U+451, U+410..U+42F->U+430..U+44F",
            "morphology": "libstemmer_eng, libstemmer_rus",
            "type": "plain"
        },
        "Source": {
            "Attributes": {
                "identity_type": "string",
                "event": "bigint",
                "tbs": "bigint"
            },
            "Fields": [
                "url",
                "login",
                "disp_name"
            ],
            "Name": "mi2evnt"
        }
    },
    "ServedBy": "Default",
    "IndexingPool": "TODO_indexing_pool",
    "Indexer": "Default",
    "Name": "minfo_event"
}
```

5. Save the file.
6. Perform the re-indexing. For this:
    a. Stop the **iw_is** process.
    b. Delete the `/var/lib/sphinx/indices/minfo_event` directory.
    c. Start the **iw_is** process.
    The re-indexing may take some time depending on the number of events in Traffic Monitor. During this time, if you perform the `iwtm status iw_is` command, you will get the query execution error.

9.5 Configuring Integration with Data Analysis Service

In Traffic Monitor, you can use the *Search for analogues* feature for events that contain attachments (for details, see *InfoWatch Traffic Monitor. User Guide. Search for Analogues*).

To enable the *Search for Analogues* feature, configure integration between Traffic Monitor and Data Analysis Service:

1. Install Data Analysis Service. For details, see *InfoWatch Data Analysis Service. Installation, Configuration and Administration Guide. Installing Data Analysis Service*.
2. Set up a connection with Data Analysis Service using the **platform_conf_ctl** utility. For this:
    a. On the Traffic Monitor server, open the `/opt/iw/tm5/bin/` directory where the utility is located.

b. Run the command:
```
./platform_conf_ctl --das-set-uri <host_DAS>:30050
                    --das-set-token <token_value>
                    --das-set-enabled
                  1
```
where `<host_DAS>` is the hostname or IP address of the Data Analysis Service server, `<token_value>` is the value of the token for connection with Data Analysis Service. By default, use the `2exwo92iwpczl1hy6jxy` token value.
You can find the actual value of the token:
- On the central node of the cluster, in which the Data Analysis Service server is located, via the command line:
  i. Go to the `<distr>/platform` directory. `<distr>` is the directory, where the distribution kit of Data Analysis Service or any platform product was extracted;
  ii. Run the command:
  `./setup.py tokens list`
  As a result, you will see a list of tokens for connecting to the Platform. The actual Data Analysis Service authorization token will be displayed opposite the *DMServer* identity.
- In the Platform product management console, in the **Token for Device Monitor Server** field of the **Global settings** section.
  Available if the Platform product with web interface is installed in the cluster and the web interface contains such a setting.

3. In the `"tmhost": "set_tmhost_here"` line of the `/opt/iw/tm5/etc/attributor.conf` configuration file, specify the IP address of the Traffic Monitor server instead of `set_tmhost_here` . Save the changes.

> **Note:**
>
> Here you can also change:
>
> - the logging level for the **iw_ attributor** process. For this, in the " `Logger` " section, set the required value for the " `level` " parameter. For details, see *Logging System Work*.
> - minimum size of contents sent to Data Analysis Service for processing. For details, see *below*.
> - maximum number of contents sent in a single request to Data Analysis Service for processing. For details, see *below*.

4. Enable file queue in the database. For this, connect to the DB server (for details, see *Database Administration*) and run the following command:
```
UPDATE object_queue
SET enabled = 1
WHERE object_queue_id = 5;
```
5. Unmask the **iw_ attributor** process. For this, on the Traffic Monitor server, run the command:
```
systemctl unmask iw_attributor
```

6. Run the **iw_ attributor** process:
   `iwtm start iw_attributor`
7. Make sure the **iw_ attributor** process is running and have the *active* status.
   `Service iw_attributor.service is active (running); enabled state: loaded (enabled)`
   For this, run the command:
   `iwtm status iw_attributor`
8. Enable autorun for the **iw_ attributor** process:
   `iwtm enable iw_attributor`

> **Note:**
>
> Data Analysis Service starts processing events since you have configured this setting. For events that happend before, the *Search for analogues* feature does not work and those events will not be taken into account if you run *Search for analogues* for other events.

To disable the *Search for Analogues* feature:

1. Stop the **iw_ attributor** process. For this, on the Traffic Monitor server, run the command:
   `iwtm stop iw_attributor`
2. Disable autorun for the **iw_ attributor** process:
   `iwtm disable iw_attributor`
3. Disable file queue in the database. For this, connect to the DB server and run the following command:
   ```
   UPDATE object_queue
   SET enabled = 0
   WHERE object_queue_id = 5;
   ```

Setting a minimum size of contents sent to Data Analysis Service for processing

To filter a flow of contents sent to Data Analysis Service for processing, you can set their minimum size for sending. It allows you to filter out uninformative contents of a small size, e.g. texts extracted from images and containing less than 50 symbols. To set a minimum size:

1. On the Traffic Monitor server, open the `/opt/iw/tm5/etc/attributor.conf` configuration file for editing.
2. In the `"TextSizeMinimumInBytes"` field, specify the minimum size in bytes.
3. Save the changes.

By default, the `"TextSizeMinimumInBytes"` field has the value of 500 bytes.

> **Note:**
>
> The parameter limits sending data only by text content size. If the attachment contains an image or a container of another kind, only the size of extracted text will be considered.
>
> If the attachment is an archive, then each element of its content will be filtered separately.

Setting a number of contents sent to Data Analysis Service in a request

If too much contents are sent to Data Analysis Service in a single query, the time during which Traffic Monitor waits for a response from Service can be exceeded. In this case, the request may not be processed. To prevent this, the maximum allowable number of contents in a request is limited by the `contentAmountPerRequest` parameter.

Traffic Monitor combines groups of contents extracted from different files into one request if the total number of these contents does not exceed the parameter value.
If the number of contents from a single file exceeds the `contentAmountPerRequest` parameter value, then nevertheless they will be sent in a single request.

To change the maximum allowable number of contents sent in a single request:

1. On the Traffic Monitor server, open the `/opt/iw/tm5/etc/attributor.conf` configuration file for editing.
2. In the `"contentAmountPerRequest"` field, specify the number of contents.
3. Save the changes.

By default, the `"contentAmountPerRequest"` field has the value of 1000.

9.6 Configuring Connection with Data Storage

To optimize data storing and increase DBMS productivity, you can install external storage of binary data – Data Storage. For details, see *InfoWatch Traffic Monitor. Installation Guide. System Deployment Schemes and Installation Types* and *Installing Data Storage*.

To configure the connection between Traffic Monitor and Data Storage:

1. Set the `debug` logging level for the `iw_x2db` process. This will allow you to make sure the connection is successful when it is configured. For details, see *Logging System Work*.
2. On the Traffic Monitor server, run the command:
`platform_conf_ctl --ds-set-enabled <bool> --ds-set-uri <platform-uri> --ds-set-token <token>`
where you specify the following parameters:

Parameter	Description	Examples
`--ds-set-enabled <bool>`	Using Data Storage. To store binary data of events in Data Storage, specify the "1" value. If you specify the "0" value, the System will not use Data Storage for storing binary data of new events	`--ds-set-enabled 1`
`--ds-set-uri <platform-uri>`	Hostname or IP address of the Data Storage server. The `http` protocol and the `40731` port are used by default.	`--ds-set-uri my.platform.com` `--ds-set-uri https://my.platform.com:40731`
`--ds-set-token <token>`	Data Storage authorization token The default value of the token: `1exwo92iwpczl1hy6jxy`	`--ds-set-token default` `--ds-set-token 1exwo92iwpczl1hy6jxy`

Parameter	Description	Examples
	Warning! To improve security, it is not recommended to use the default value of the token. You can find the actual value of the token: • On the Data Storage server, via the command line. For this: a. Go to the directory where the Platform distribution kit was extracted. b. Run the command: `./setup.py tokens list` As a result, you will see a list of tokens for connecting to the Platform. The actual Data Storage authorization token will be displayed opposite the *DataStorageUser* identity. You can refresh the Data Storage authorization token by running the command: `./setup.py tokens refresh DataStorageUser` • In the Platform product management console, in the **Token for Data Storage User** field of the **Global settings** section. Available if the Platform product with web interface is installed on the server with Data Storage and the web interface contains such a setting. In this case, you can refresh the token by pressing the button  .	

If the connection is succesfull, a message of the following type will appear in the `/var/log/infowatch/x2db.log` log file:

```
[DEBUG  ] : <DataStorage> platform request headers: GET /v2/logon?extAPIToken=1exwo92iwpczl1hy6jxy HTTP/1.1
Host: my.platform.com
User-Agent: tmOperator
Accept: application/json
X-IW-ACTIVEPRODUCT: TM

[DEBUG  ] : <DataStorage> platform response: HTTP/1.1 200 OK
```

After configuring is complete, you can set the logging level for the `iw_x2db` process that was set before configuring.

To view current settings of the connection with Data Storage:

On the Traffic Monitor server, run the command:
`platform_conf_ctl`

To break the connection with Data Storage:

On the Traffic Monitor server, run the command:
`platform_conf_ctl --ds-remove`
Data in the storage will no longer be available.

If you want to stop storing binary data of events in Data Storage but have access to already stored data, run the command:
`platform_conf_ctl --ds-set-enabled 0`
New events will be stored entirely in Traffic Monitor DB, starting with the next daily tablespace, i.e. starting tomorrow in UTC+0.

9.7 Configuring Sending Events to Platform

Starting with version 7.14, Traffic Monitor can send events to the Platform in two ways:

- According to synchronization settings in the Investigation Centre
- Real-time pushing

Sending events in real time helps reduce Traffic Monitor load.

> **Important!**
>
> Make sure that Traffic Monitor and Investigation Centre use the same way to load events.
>
> For the Platform to receive events in real time, its version must be 2.5 or later.

9.7.1 Switching the way of sending events

To switch the way of sending events in Traffic Monitor settings, use the `platform_conf_ctl` utility on the Traffic Monitor server:

```
platform_conf_ctl --fl-set-enabled <bool> --fl-set-uri <uri> --fl-set-token <token> --fl-set-integration-id
<id>
```

In the command above, specify the following parameters of connection with the platform **FactsLoader** service:

Parameter	Description
`--fl-set-enabled`	Enable/disable real-time pushing: • `true` (by default) – enable real-time event pushing • `false` – disable real-time event pushing and send events according to Investigation Centre synchronization settings
`--fl-set-uri`	URI of Platform host in the following format: **`http://`** `<host>:<port>`, where `<host>` is the Platform server hostname or IP-address and `<port>` is the Platform server port.By Default port is `10104`.

Parameter	Description
	Important! In this parameter, you should specify an address of the same Platform node as selected in the "Branch" field of integration with Traffic Monitor in Investigation Centre. For details, see the *Integration with InfoWatch Traffic Monitor* article in the *Administration Guide* for the Platform product you are using.
`--fl-set-token`	Token for connection with the Platform. You can get it in Investigation Centre, **Settings** → **System Settings** → **Global settings**, in the **Token for Data Storage User** field. For details, see the *Global Settings* article in *Administration Guide* of the Platform product you are using. You can set the default value of the token if you did not refresh it. For this, specify `--fl-set-token default`. For security purposes, it is not recommended to use the default token value.
`--fl-set-integration-id`	Unique identifier of the Platform integration with Traffic Monitor. You can copy the integration ID in the **Settings** → **System Settings** → **Integrations** section. On the integration tile, click and select **Copy ID**. For details, see *Integration with InfoWatch Traffic Monitor* article in the *Administration Guide* for the Platform product you are using.

If Traffic Monitor use Data Storage to store its own data, then, in the `--fl-set-uri` parameter, specify address of the Data Storage server or address of any other Platform server located in the same cluster with Data Storage. The same Data Storage as before will continue to store binary data. Text data will be stored in Traffic Monitor database as before. At the same time, the **FactsLoader** service will download text contents on its server and store them there for displaying events in Investigation Centre.
On how to configure connection with a storage, see *Configuring Connection with Data Storage*.

If Traffic Monitor does not use Data Storage to store its own data, then, after configuring connection with the **FactsLoader** service, all data will be stored in the Traffic Monitor DB as before. But, in this case, copies of the data will be stored on the Platform server specified in the `--fl-set-uri` parameter.

> **Note:**
>
> In case of distributed installation, the utility must be run on the server installed with the *Interceptors* template.

Example of enabling real-time pushing:

```
platform_conf_ctl --fl-set-enabled true --fl-set-uri http://10.60.23.249:10104  --fl-set-token default --fl-set-integration-id e06bd150-513b-4eb6-975a-533cf96e50ab
```

Command to disable real-time pushing and switch to scheduled sending:

```
platform_conf_ctl --fl-set-enabled false
```

9.7.2 Configuring real-time pushing

To configure real-time pushing:

1. In the Investigation Centre, copy the integration ID.
2. On the Traffic Monitor server, switch the way of sending events using the utility.
3. Restart the `iw_x2db` service:

   ```
   systemctl restart iw_x2db
   ```

4. Go to the Investigation Centre. For the System to display events between the last synchronization and until switching to real-time pushing, start the synchronization manually.
5. In the Investigation Centre, switch the way of sending events and save the changes.

9.7.3 Configuring scheduled events sending

If the Investigation Centre has not previously synced with Traffic Monitor, you only need to set up the integration in the Investigation Centre.

If real-time event pushing was previously configured:

1. On the Traffic Monitor server, switch the way of sending events using the utility:

   ```
   platform_conf_ctl --fl-set-enabled false
   ```

2. Restart the service `iw_x2db`:

   ```
   systemctl restart iw_x2db
   ```

3. Go to the Investigation Centre and disable the real-time event loading in the integration with Traffic Monitor.
4. If necessary, change the automatic synchronization schedule and save the changes.

For more information about integration settings in the Investigation Centre, see *Integration with InfoWatch Traffic Monitor* article in *Administration Guide* for the Platform product you are using.

9.8 Logging System Work

For the convenience of monitoring processes, the logging subsystem has 6 levels:

Level	Description
`fatal`	Writes errors that are critical for the process operation
`error`	Writes messages about errors that are not critical for the process operation

Level	Description
`warning`	Writes information about potentially dangerous cases
`Information`	General information about the process that can be useful (process start/stop, applying configurations, etc.)
`debug`	Writes information which is mostly used to diagnose the service operation (IT, system administrators and so on)
`trace`	Mostly used by programmers to track the code

Configuring logging levels

> **Warning!**
>
> Please, note that choosing a more detailed logging level may significantly reduce the System performance.

Configuration files are located in the `/opt/iw/tm5/etc` directory. By default, the `warning` level is used for all processes.

To change the logging level for Traffic Monitor Server processes:

1. In the configuration file of the required process, find the `Logging` section and set the needed value for `GlobalLevel` parameter.
2. Save changes.
3. After you have changed the system log, restart the process:
   `iwtm restart <service_name>`

By default, all process logs are stored in the `/var/log/infowatch` directory.

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

1. Open the configuration file.
2. For `text-extractor` parameter, add the value `-l <level>,` where `<level>` is the logging level. For example:
   `< Command> bin/text-extractor -l error -t ooxml -i ${OUTDIR}" < Command>`
3. After you have made changes, restart processes:
   `iwtm restart bookworm`
   `iwtm restart warpd`

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

9.9 File Queues

To enable loading the existing object queues:

1. Stop the following services: `iw_icap`, `iw_deliver`, `iw_luaengined`, `iw_is`, `iw_smtpd`, `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 error queue to the required queue.
3. Wait until all objects in the file queue are processed.
4. Run the following services: `iw_icap`, `iw_deliver`, `iw_luaengined`, `iw_is`, `iw_smtpd`, `iw_xapi_xapi`, `iw_xapi_puppy`, `iw_analysis`, `iw_messed`, `iw_proxy_http`, `iw_proxy_icq`, `iw_proxy_smtp`, `iw_capstack`.

To start all the services, run the command:

```
iwtm start
```

To check if the processes are started, use the following command:

```
iwtm status
```

Commands for starting/stopping separate services:

Starting	Stopping
`iwtm start icap`	`iwtm stop icap`
`iwtm start deliver`	`iwtm stop deliver`
`iwtm start luaengined`	`iwtm stop luaengined`
`iwtm start is`	`iwtm stop is`
`iwtm start smtpd`	`iwtm stop smtpd`
`iwtm start xapi_xapi`	`iwtm stop xapi_xapi`
`iwtm start xapi_puppy`	`iwtm stop xapi_puppy`
`iwtm start analysis`	`iwtm stop analysis`
`iwtm start messed`	`iwtm stop messed`
`iwtm start proxy_http`	`iwtm stop proxy_http`
`iwtm start proxy_icq`	`iwtm stop proxy_icq`

Starting	Stopping
`iwtm start proxy_smtp`	`iwtm stop proxy_smtp`
`iwtm start capstack`	`iwtm stop capstack`

Objects in the System are moved by means of file queues:

Path to the directory of the queue	Format of files in the queue
queue/analysis	`.xml & .dat`
`queue/smtp`	`.xml & .dat`
`queue/db`	`.xml & .dat`
`queue/blackboard`	`.dat`
`queue/blackboard_errors`	`.dat`
`queue/is`	`.xml & .dat`
`queue/x2x`	. `xml & .dat`
`queue/errors`	`.xml & .dat`
`queue/x2x-errors`	`.xml & .dat`
`queue/x2db-errors`	`.xml & .dat`
`queue/final-errors`	`.xml & .dat`

Each queue contains additional technical queues which allow you to monitor for processing objects: `.db, .in, .out`.

Note:

For the `queue/smtp` process, the processing can be divided into the following steps:

1. `queue/smtp/.in` – as the **iw_smtpd** service receives objects from Postfix, a file is generated in this queue. If for some reason, the object processing in this queue is delayed, please, check **iw_smtpd** or **iw_proxy_smtp** service.
2. `queue/smtp/.db` – when the processing is complete, the file is moved from the `.in` qu eue to the `.db` queue. EML mail objects from **iw_xapi** are placed in this queue.
3. `queue/smtp/.out` – the object is placed in this queue by the **iw_messed** service.

Note that:

Queues of the **iw_is** service are additionally divided into:

- `queue/is/cmd/` – a file queue of **iw_is** commands;
- `queue/is/fetching/` – a queue of commands for loading;
- `queue/is/indexing/` – a queue of commands for indexing;
- `queue/is/errors/` – an error queue.

Queue name	Services that place an event in the queue	Services that remove an event from the queue
`queue/analysis`	`iw_xapi_xapi`, `iw_xapi_puppy`	`iw_analysis`
`queue/smtp`	`iw_xapi_xapi`, `iw_xapi_puppy`, `iw_smtpd`, `iw_proxy_smtp`, `iw_capstack`	`iw_messed`
`queue/db`	`iw_messed`, `iw_analysis`, `iw_icap`, `iw_proxy_icq`, `iw_proxy_http`	`iw_x2x`
`queue/blackboard`	`iw_x2db`, `iw_deliver`	`iw_blackboard`
`queue/blackboard_errors`	an error when processing `iw_blackboard`	-
`queue/x2x`	`iw_x2x`	`iw_x2db`
`queue/is`	`iw_metainfo_fetcher`	`iw_is`
`queue/errors`	all services in case of processing errors	`iw_rammer`
`queue/x2x-errors`	errors when processing `iw_x2x`	
`queue/x2db-errors`	errors when processing `iw_x2db`	
`queue/final-errors`	`iw_rammer`	-

You can enable collecting statistics on file queues in the service configuration file which is located in the `/opt/iw/tm5/etc` directory. For this, in the *Statistic* section, set the **Enabled** parameter value to `true`.

9.10 Recovering the System after Failures

You can recover the System when server failures occur or during a network outage by completing the steps described below:

1. Stop Traffic Monitor Server processes by running the command:
   `iwtm stop`

2. Move objects from the `queue/x2db-errors` error queue to the `queue/x2x` queue. For this, use **iw_qtool** utility (see the Knowledge Base article *Moving of Objects between Queues (iw_qtool Utility)*).
3. If Traffic Monitor Server works with installed PostgreSQL DBMS, then, to check the connection, run the following command:
   `su - iwtm`
   `psql -p 5433 -h <DB_server_IP_address> postgres iwtm`
   `psql -p 5433 -h 127.0.0.1 postgres iwtm` - to connect local database
   If the check is successful, then, in response to the execution of the command, PSQL invitation will be displayed:
   `postgres=#`
   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>`
4. Run the Traffic Monitor Server processes by executing the command:
   `iwtm start`

If after Traffic Monitor launch the System is not recovered:

1. Collect the diagnostic information, i.e. logs.
   For details on logging, see *Oracle Database Logging*, *PostgreSQL Database Logging*, *Logging System Work*.
2. Check the system log for errors. The path to the system log: `/var/log/messages` .
3. Analyze the collected information. You can find typical errors and methods of their solution in the Knowledge Base article: *Errors in PostgreSQL database*. If needed, consult the DB administrator or technical support service.

9.11 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.

Depending on settings specified during installation, two and more languages can be installed in the System (find information on installation in the document *InfoWatch Traffic Monitor. Installation Guide*). Russian and English morphology dictionaries are preinstalled (even if it was not specified during installation).

Upon installation, user also can:

- Adding New Language for Events Search. Morphology and Adding Terms;
- Updating Installed Language Including Morphological Support;
- Deleting Search Language and Terms.

9.11.1 Adding New Language for Events Search. Morphology and Adding Terms.

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

1. Stop thy **iw_indexer** and **iw_is** processes:
   `iwtm stop indexer`
   `iwtm stop is`

2. Go to the local repository that keeps packages downloaded during the installation:
   `cd /opt/iw/distr`
3. Go to directory that matches current Traffic Monitor version.
4. Select the required package and install it using the command:
   `rpm -i <package name>`
   For example, to install French dictionary package, enter the command:
   `rpm -i iwtm-sphinx-dict-fra-7.0.0-792.x86-64.rpm`
5. Run the processes:
   `iwtm start indexer`
   `iwtm start is`

> **Note:**
>
> Installing a new dictionary causes full database re-indexing, which may take some time.

To enable morphology for events search:

6. Stop the **iw_indexer** and **iw_is** processes:
   `iwtm stop indexer`
   `iwtm stop is`
7. Open the **sphinx_options.ini** file using the command:
   `mcedit /opt/iw/tm5/etc/sphinx_options.ini` and add the required language key to `sphinx_language` parameter.
   For example, to activate the morphology for Russian and Turkish languages, specify the following parameter 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.

8. When using PostgreSQL DBMS, open the **database.conf** file to add terms:
   `mcedit opt/iw/tm5/csw/postgres/database.conf` When using Oracle DBMS, open the **database.conf** file to add terms:
   `mcedit /opt/iw/tm5/csw/oracle/database.conf`
9. Add the language key 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*.

10. Run the **iw_indexer** and **iw_is** processes:
    `iwtm start indexer`
    `iwtm start is`

9.11.2 Updating Installed Language Including Morphological Support

To update existing dictionary:

1. Go to directory with dictionary packages:
   `cd /opt/iw/disrt/7.0.0/`
2. Run package installation:
   `rpm -i <package name>`
   For example:
   `rpm -i iwtm-sphinx_dict-deu-7.0.0.792.x86_64.rpm`

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

9.11.3 Deleting Search Language and Terms

To delete a dictionary from the System:

1. Stop the **iw_indexer** and **iw_is** processes:
   `iwtm stop indexer`
   `iwtm stop is`
2. Open **database.conf** file if you use PostgreSQL DBMS:
   `mcedit /opt/iw/tm5/csw/postgresql/database.conf`
   If you use Oracle DBMS, open file **database.conf** to add terms:
   `mcedit /opt/iw/tm5/csw/oracle/database.conf`
3. Delete code of language with morphology support from `define cfdb_language` parameter.
4. Delete indexing files from `/var/lib/sphinx/` directory.
5. Start processes:
   `iwtm start indexer`
   `iwtm stop is`

After you delete a dictionary, the database is completely reindexed.

> **Note:**
>
> If you want to save the language in Categories and Terms, then add the code of the language with morphology support to the `cfdb_language` parameter of the **database.conf** configuration file just before updating the System. This will also restore the language with morphology support. If you want to delete the language with morphology support after the System update, repeat the steps described above.

9.12 Configuring Forwarding Data to SIEM

Traffic Monitor can be integrated with SIEM systems (Kaspersky Unified Monitoring and Analysis and others). Integration means forwarding consolidated information from all installed TM components to SIEM.

Configuring this functionality is possible using the script **/opt/iw/tm5/bin/config/iwtm-siem.conf.py**, which is available on Traffic Monitor server.

Information from TM is available for SIEM system:

1. By means of a table view:
    - Events, registered in TM;
    - TM console user session audit;
2. By means of rsyslog:
    - Logging in and out TM Linux server;
    - Events, registered in TM Linux server system log, including information on logging in and out Oracle or PostgreSQL DB users;
    - State of services on TM Linux server or group of servers.

In this chapter:

- Configuring SIEM Side;
- Configuring TM Side;
- Type of Logs, Transmitted to SIEM.

9.12.1 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 *Table Representation of TM Events* 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_OBJECTS2` 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
`monitorcode`	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 • Mail.Ru Agent • Telegram • VK (ВКонтакте) • Facebook • WhatsApp • MS Lync • FTP • Email • Web email • Web message • Clipboard • Cloud storage • Keyboard input • Terminal session • Network resources • File reading • File writing	Email
`protocol`		*Protocol* attribute of the event	Possible values: • OSCAR • Skype • XMPP • MMP • SIP • FTP • POP3	

Attribute name	Data type	Description	Possible values	Example
			• IMAP • MAPI • SMTP • HTTP • HTTPS • NRPC • WhatsApp • 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
`capture_data`	timestamp	Event interception date (in UTC, without specifying the timezone) in `timestamp` format. In PostgreSQL DBMS, the attribute has an increased accuracy to milliseconds. 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.	Kingston USB Drive 5.0

Attribute name	Data type	Description	Possible values	Example
			Can be blank.	
`Web-source`	varchar2(256)	*Resource* attribute of the event	Address of the visited web resource or address of cloud storage. Can be blank.	Yahoo.com
`recipients contacts`	clob	*Recipients* attribute of the event	List of recipients separated by commas in `<contact type>:<contact value>` format. Can be blank.	email:ivanov@infowatch.ru, email:petr.petrov@infowatch.ru
`recipients fullname`	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
`recipients domainaccountname`	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
`sendercontacts`	clob	*Senders* attribute of the event	Sender's contact in `<contact`	email:petr.petrov@infowatch.ru

Attribute name	Data type	Description	Possible values	Example
			`type>:<contact value>` format. Can be blank.	
`sendermachinedomainname`	clob	*Workstation* attribute of the event	Domain name `dnshostname` of the sender's workstation. Can be blank.	XP-PETROV
`sendermachineip`	clob	*Workstation* attribute of the event	IP address of the sender's workstation. Can be blank.	192.0.2.0
`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 categories, 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
`fingerprints`	clob	*Form*, *Sample document*, *Stamp*, *DB*	List of forms, sample documents, stamps, and DB unloadings detected	Application form.doc

Attribute name	Data type	Description	Possible values	Example
		unloading attributes of the event	in the intercepted object. Elements in the list are separated by commas. Can be blank.	
`protecteddocuments`	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
`policies`	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
`violationtype`	varchar2(40)	*Rules group* attribute of the event	Possible values: • *Copy* (*Copying violation*) • *Placement* (*Placing violation*) • *Transfer* (*Transferring violation*) 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*	Violation

Attribute name	Data type	Description	Possible values	Example
			Can be blank	
`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$ \example.txt
`attachments`	clob	*Attachment name* attribute of the event	Names of attachments separated by commas	example.txt, Petrov.doc, 3.jpg
`url`	varchar2(4000)	*URL* attribute of the event	Full address from which data has been sent Can be blank.	192.0.2.0/3.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

Warning!

The number of elements to display within one cell of one record is limited to 1000 (For example: 1000 recipients or extracted files in the event).

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	Description	Example
`audit_log_id`	Number(20)	TM user session audit entry ID.	12345
`change_date`	Varchar2(50)	Date and time of registered user action	05.08.2015 09:35:10.641446000
`user_login`	varchar2(256)	Login of user, who performed an action	Admin

Attribute	Data type	Description	Example
`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
`operation`	varchar2(40)	Type of action, performed by user Possible values: • restart (restart) • delete_hash (hash deletion) • sync (synchronization) • add_tag (adding tag) • remove_tag (removing tag) • run (performing query) • start (starting) • stop (stopping) • view (viewing) • create (creation) • update (editing) • delete (deletion) • login_failure (unsuccessful login attempt) • login (successful login) • logout (logout) • change_password (password change) • decision_update (changing 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)	Edit

Attribute	Data type	Description	Example
		• add (adding) • import (import) • export (export)	
`entity_type`	varchar2(40)	Type of object on which the action was carried out. Possible values: • AgentJob (diagnostic data) • Adlibitum (Adlibitum) • Agent (service) • Classifier (classifier) • NetworkSettings (network parameters) • NotificationSettings (system status) • ObjectReport (events unloading) • Query (launching objects search) • QueryReportRun (report creation) • Setting (settings) • UpdateSystem (system update) • 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) • ProtectedDocuments (protected object)	Dashboard

Attribute	Data type	Description	Example
		• Report (report) • Role (role) • Selection (selection) • ServiceLog (service log) • SystemList (list of resource topics) • SystemListItem (list of resources with definite topic) • Tag (tag) • Term (term) • TextObject (text pbject) • User (user) • VisibilityArea (visibility scope) • Config (configuration) • License (license) • Object (object) • ProtectedCatalog (protected object catalog)	
`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.	

		`{`
		`“old”: {`
		`“<OBJECT TYPE>”:{`
		`{`
		`“<FIELD>”: “<VALUE>”,`
		`“<FIELD>”: “<VALUE>”`
		`}`
		`}`
			`{`
			`"old":{`
			`"visibilityareas":{`
			`}`
			`},`
			`"new":{`
			`"visibilityareas":[`
			`{`

Attribute	Data type	Description	Example

		}
		{
		“new”: {
		“<OBJECT TYPE>”:{
		{
		“<FIELD>”: “<VALUE>”,
		“<FIELD>”: “<VALUE>”
		}
		}
		}
		}
			"VISIBILITY_AREA_ID":"F00207A1E7E743EE0433D003C0A5DD400000000",
			"DISPLAY_NAME":"<idclip>",
			"NOTE":"<idclip>",
			"VISIBILITY_AREA_CONDITION":"{"data": {"link_operator": "and","children": []}}",
			"IS_SYSTEM":1
			}
			}
			}

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

		{
		“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.**	

Attribute	Data type	Description	Example
		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"`
			`}`
			`}`

9.12.2 Configuring TM Side

To configure the transfer of consolidated information from Traffic Monitor:

1. Create a database account for SIEM (see *Creating Siem User*).
2. Configure data transfer from Traffic Monitor to SIEM (see *Forwarding Logs to SIEM*).
3. If necessary, modify logging settings for Traffic Monitor database user session audit (see *Log Management for TM DB User Sessions*).

> **Note:**
>
> To change SIEM settings, use *SIEM integration* manager, which you can run in the command line with `iwtm-setuptool.py` script. To navigate in the settings manager, use keyboard arrows and **Enter** key or a mouse. To return to a previous window of the manager, press left key. To quit the manager, press **Ctrl+C**. For details on working in the settings manager, see the articles specified above.

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. Run the command to start SIEM integration manager:
   `/opt/iw/tm5/bin/config/iwtm-setuptool.py`
2. Select **DB siem user** option.

3. Select **Create DB siem user** option.
4. Set parameters:

Parameter	Description
`DB admin login`	Login name for Oracle/PostgreSQL administrator account **Note:** the following login names are used: • `sys` for Oracle • `postgres` for PostgreSQL
`DB admin password`	Password for Oracle/PostgreSQL administrator account
`DB siem user password`	Password for new siem user

5. Press **Create**.

Changing Siem User Password

To change siem user password:

1. Run the command to start SIEM integration manager:
   `/opt/iw/tm5/bin/config/iwtm-setuptool.py`
2. Select **DB siem user** option.
3. Select **Change password for DB siem user** option.
4. Set parameters:

Parameter	Description
`DB admin login`	Login name for Oracle/PostgreSQL administrator account **Note:** the following login names are used: • `sys` for Oracle • `postgres` for PostgreSQL
`DB admin account`	Password for Oracle/PostgreSQL administrator account
`New siem user password`	New password for siem user

5. Press **Change password**.

Deleting Siem User

To delete siem user:

1. Run the command to start SIEM integration manager:
   `/opt/iw/tm5/bin/config/iwtm-setuptool.py`
2. Select **DB siem user** option.
3. Select **Delete DB siem user** option.
4. Set parameters:

Parameter	Description
`DB admin login`	Login name for Oracle/PostgreSQL administrator account
`DB admin password`	Password for Oracle/PostgreSQL administrator account

5. Press **Delete**.

Forwarding Logs to SIEM

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

1. Run the command to start SIEM integration manager:
   `/opt/iw/tm5/bin/config/iwtm-setuptool.py`
2. Select **Log messages forwarding configuration** option.
3. Set parameters for logs transfer:

Parameter	Description
`Enable forwarding`	Enable/disable forwarding logs to SIEM. Possible values: `Yes/No`
`Forwarding server`	SIEM server 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 values: `TCP` `/UDP`
`Log messages severity`	Minimal level of log messages sent to SIEM server. Possible values: `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Info`, `Debug`
`Size (MB)`	Acceptable size of the queue of messages to be sent to SIEM. Default value: `500`

4. Press **Ok**.

> **Warning!**
>
> The System does not log disconnection of users with database administrative permissions and therefore does not forward this information to SIEM.

Log Management for TM DB User Sessions

You can enable or disable logging of TM database user sessions in the OS log via **rsyslog** utility.

To enable logging of TM database user sessions:

1. Run the command to start SIEM integration manager:
   `/opt/iw/tm5/bin/config/iwtm-setuptool.py`
2. Select **DB audit logging management** option.
3. Enter database administrator credentials:
   - **DB admin login**: login name for Oracle/PostgreSQL administrator account;
   - **DB admin password**: password for Oracle/PostgreSQL administrator account.
4. Click **Check logging status**.
5. If:
   - **Logging status: disabled**, click **Change logging status** to enable logging
   - **Logging status: enabled**, 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.

9.12.3 Type of Logs, Transmitted to SIEM

Rsyslog forms common 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 to **Oracle DB** and logout from it:
   ```
   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)
   ```

9.13 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`

10 Working in Traffic Monitor via Administration Centre Web Interface (Platform)

To make it easier for users to work with both Traffic Monitor and products based on Platform, the ability to work with Traffic Monitor via the web interface of Administration Centre (Platform) is available. This allows users to work in a single web interface without switching between products.

Follow the steps to work with Traffic Monitor via Platform web interface:

1. Add a new integration with Traffic Monitor. If you have already done this before, skip this step.
    a. Go to **Settings** → **System settings** → **Integrations** in the web interface of Investigation Centre.
    b. Click:
        - **+ Add integration** in the centre of the window, if there has been no integration configured before.
        - **+ Add** in the upper-right corner, if there has been another integration configured earlier.
    c. Select **InfoWatch Traffic Monitor** and specify the following parameters. More details about the integration and parameters see in *Administration Guide* of the Platform product that you are using, in the *Integration with InfoWatch Traffic Monitor* article.
    d. Click **Test connection** to check if you've specified all required parameters correctly. Wait until you see the message **Successfully connected**.
    Or you can see one of the following statuses:
        - **Invalid token specified** – you have provided an invalid token;
        - **Failed to establish connection** – you have specified an incorrect address or the server is unavailable;
        - **Timeout for service respond is exceeded** – high load on Traffic Monitor, network problems, or other problems (however, Traffic Monitor can be available and synchronization will be done);
        - **Access to data is not allowed** – in Traffic Monitor, there is no license for data export to Investigation Centre or the license has expired.
    e. Click **Save and start** synchronization to start the synchronization immediately.
2. To enable the Traffic Monitor interface in Platform:
    a. Connect to the central Platform node.
    b. Run the command:

```
kubectl exec -it -n infowatch $(kubectl get pods -n infowatch | grep postgresql-
central |  awk '//{print $1;}') -- psql -U postgres -d configstorage -c "UPDATE
key_values SET obj = jsonb_set(obj, '{Obj}', 'true'::jsonb) WHERE id = 'FT_TMFrame'"
```

    c. To apply the changes in the Platform web interface, reload the browser page.
3. For secure access to the product, we recommend installing an ssl/tls certificate signed by a trusted certificate authority or by a certificate issued by a certification authority on the computer which you will use for logging to the products.

> **Note:**

If the certificate is not installed, you can access Traffic Monitor by opening it in a separate browser tab ad confirming the insecure connection to the site. After that, reload the tab with the Platform web interface; Traffic Monitor authentification window will become available in Administration Centre.

4. To open Traffic Monitor interface in Platform:
    a. To navigate Administration Centre, click the button  located in the bottom-left corner.
    b. In the upper-left corner, expand Traffic Monitor section and select the server you want to connect to.
    c. In the authorization window that opens, enter the login and password for your Traffic Monitor account.

You can also configure single sign-on between Investigation Centre products and Traffic Monitor, for more details, see *Configuring Single Sign-On in InfoWatch products*.

Note:

In the Traffic Monitor interface in Administration Centre, the Dashboard, Events and Reports sections and the event ID search bar are unavailable. You can work with events and reports in Investigation Centre.

When working in the Platform web interface, logging out of Traffic Monitor is not available. After authentification, the user session will expire only after a timeout.

11 Configuring Single Sign-On in InfoWatch products

Single Sign-On feature enables you to switch between InfoWatch Traffic Monitor and Investigation Centre without re-entering login and password. Single Sign-On works only when the transition between products is explicit and only for users created on the basis of the same Active Directory account.

To implement Single Sign-On:

1. On the main Investigation Centre server (`central` Platform node), type the following command in the command line:

   ```
   kubectl get secret guardkeys-central -n infowatch --output='go-template={{index .data
   "ec256-public.pem"}}' | base64 -d
   ```

   This will display a generated public key in PEM format. Key example:

   ```
   -----BEGIN PUBLIC KEY-----
   MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEIlNdAukpfJjZspZHWV2uu6U9D9/H
   IDCRYBmIRApbE4J2aiS3DGQICAJ3QShiFZtRYVATtJSPsyWGX4CP46Dbxg==
   -----END PUBLIC KEY-----
   ```

2. Copy and save the key.
3. On Traffic Monitor server, connect to the database:
   - For PostrgreSQL DBMS:

     ```
     psql postgres iwtm
     ```

   - For Oracle DBMS:

     ```
     sqlplus iwtm@iwtm
     ```

4. Specify a list of trusted systems which can authorize in Traffic Monitor by their user accounts. Give a name to each trusted system and paste the corresponding public key. For example, run the command:

   ```
   insert into trusted_system(system_name, public_key)
   values('my system','-----BEGIN PUBLIC KEY-----
   MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEIlNdAukpfJjZspZHWV2uu6U9D9/H
   IDCRYBmIRApbE4J2aiS3DGQICAJ3QShiFZtRYVATtJSPsyWGX4CP46Dbxg==
   -----END PUBLIC KEY-----');
   commit;
   ```

5. Exit the database:

   ```
   exit
   ```

6. In Traffic Monitor Management Console, configure and run synchronization with Active Directory to import a user who is going to work with both Systems. Wait for synchronization to fully complete.
7. In **Users and roles** section, add a new user from LDAP, assign a role to view events and visibility scopes.

8. Log out of this user account.
9. On a separate browser tab, open Investigation Centre web interface.
10. Configure and run synchronization with Active Directory to import the user mentioned earlier.
11. On **Users** tab, add a new user and assign a role to them.
12. Log out and then log in to the new user's account.
13. Go to **Events** section and click to select one or several events from the list and press **View events**.

A new tab with **Events** section of Traffic Monitor Management Console will open and the System will automatically authorize you. Besides, audit log will hold an event of the user logging in from an external system.

12 Interaction with external systems

Traffic Monitor and external systems exchange data via API. For more information, see *InfoWatch Traffic Monitor. API Introduction*.

Traffic Monitor also supports interactions with other external systems via InfoWatch adapters. For more information, see the section *IW Traffic Monitor Integrations*.

13 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	

14 Appendix B. Monitoring Indicators

The table below is listing all indicators, used by monitoring subsystem to check the state of System components, installed and operating on servers in All-in-one mode. The check includes obtaining indicator values at regular intervals and comparing them with threshold values. Critical values of all indicators may mean that the server is physically inaccessible. In this case, please check if the server works properly.

Warning!

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

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, where it is checked	Poll interval	Values	Details and recommendations
General System load	Load of IW-Linux-servers, TMcap servers, DB servers over the last 15, 5, and 1 minute	30 minutes	🔴 – 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	Check the load of interception and analysis servers, and DB servers: 1. Run `top` 2. Sort the results, using the commands: a. Shift+m to sort by RAM load; b. Shift+p to sort by CPU load.
System components statuses	System services statuses	30 minutes	🔴 – at least one service is not started 🟢 – all services are started	In All-in-one installation mode, the list and number of System services are known and permanent. To display services status

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
				details, type `iwtm status`
Syslog service status	Whether the `syslog` service is started or not	30 minutes	🔴 – service not started 🟢 – service started	Check if `rsyslog` service is running: `systemctl status rsyslog`
Number of active users	Number of users (Security Ofiicers), registered with the System (Linux servers)	30 minutes	🔴 – > 50 users 🟡 – from 20 to 50 🟢 – < 20 users	It is necessary to decrease number of security officers to 50 persons
DB Alert Log Errors	Whether Alert Log contains errors (DB servers)	5 minutes	🔴 – errors found 🟢 – no errors	It is necessary to decrease the number of errors having `SEVERITY=HIGH` label. **Search in Alert Log should be based on the following words:** • ORA- • Failed to archive • ORACLE Instance .* - Archival Error • ARC[0-9]: I/O error • ARC[0-9]: RFS network connection lost at host • ARC[0-9]: Error 3113 creating • Media Recovery failed with error • Corrupt block • Fractured block • Bad header • Data in bad block • Reread of rdba • log corruption • RESETLOGS **Search in pg_log should be based on the following words:** • FATAL • PANIC

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
				• ERROR
Server availability	Response time for sent packages and number of lost packages (Linux servers)	5 minutes	🔴 – > 500 ms 🟡 – from 100 to 500 ms 🟢 – < 100 ms	Ping results with the following parameters `100.0,20%! 500.0,60%` show that: Response to sent packages exceeds 100 milliseconds and more than 20% of packages are lost; Response to sent packages exceeds 500 milliseconds and 60% of packages are lost.
Availability of incorporated mail transfer agent	Postfix server availability	30 minutes	🔴 – not available 🟢 – available	1. Check Postfix server status: s `ystemctl status postfix` 2. Start checking correctness of configuration file `/etc/postfix/main.cf`, using the command `postfix check`
Server availability via SSH	Response time	10 minutes	🔴 – >= 10 seconds 🟢 – < 10 seconds	Check `sshd` daemon status, using the command `systemctl status sshd`
Device Monitor server availability	Response for request	30 minutes	🔴 – no connection 🟢 – connection established	If the System has an active Device Monitor license, it should be displayed. Check the license in **Administration** -> **License s** in Traffic Monitor Management Console.
Using swap file	Free space in swap (virtual memory) (Linux servers)	5 minutes	🔴 – < 10% free 🟡 – from 10 % to 50% free 🟢 – > 50% free	For details, see *InfoWatch Traffic Monitor. Installation Guide. Recommendations on Disk Space Partitioning*

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
Free space on root partition	Free space in the root file system (Linux servers)	30 minutes	🔴 – < 10 000 MB 🟡 – from 10 000 MB to 20 000 MB 🟢 – > 20 000 MB	
Free space on `/var` partition	Free space in the `/var.` file system `(` Linux servers)	30 minutes	🔴 – < 10 000 MB 🟡 – from 10 000 MB to 20 000 MB 🟢 – > 20 000 MB	
Status of time synchronization service	`ntpd.` service status (NTPD)	30 minutes	🔴 – NTP server is unavailable 🟢 – NTP server is available	Check `ntpd` daemon status, using the command `systemctl status ntpd`
System time offset	Time lag on System servers and NTP server (Linux servers)	360 minutes	🔴 – > 40 seconds 🟡 – from 20 to 40 seconds 🟢 – < 20 seconds	The error occurs, if the System cannot connect NTP servers, or System configuration has no NTP servers. In this case, the error message "*Can't create socket connection*" will appear. Make sure that `ntp.conf` and `iwmon-services-ntp.cfg` configuration files have the same correct NTP server specified.
Core dump	Checking the functionality of services, the absense of failures, the number of files with in the `/opt/iw/tm5` directory that look like: • core_<....>	30 minutes	🔴 – 5 or more core dumps 🟡 – 1 to 4 core dumps 🟢 – no core dumps	Contact InfoWatch technical support at *support@infowatch.com*

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
	• <...>.core (Linux-servers)			

Queue of events processing errors	Number of objects in **queue/final-errors** queue (`iw_rammer`)	1 minute	🔴 – > 1 objects
			🟢 – 0
				Option 1: Clear queues using the commands:
				`su - iwtm`
				`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/final-errors`
				`exit`
				Option 2:
				1. Open the `/etc/cron.d/iwtm_cleanup` file in the edit mode.
				2. Reduce the period of cleaning files in file queue folders. You can do it in a regular `cron` job (the default value is 30 days).
				3. Save changes and close the file.
				For more details see Inline Mode

Database status	Database status (depending on the DBMS in use)	10 minutes	🔴 – <> ok 🟢 – ok	Check availability of the database: 1. Log in to the database: `s qlplus iwtm@iwtm` 2. Enter password `xxXX1234` 3. Watch `SQL>`
Database access service status	Oracle TNS listener's status	10 minutes	🔴 – TNS listener is not started	Indicator is enabled and displayed in the list only in case when Oracle SMDB is used in the System

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
			🟢 – TNS listener is started	
The number of Oracle data files	If the number of files has reached 90% of the specified maximum value	60 minutes	🔴 – if the current number of data files reaches the maximum value 🟡 – if the number of files is 90% of the maximum value 🟢 – if the number of files is fewer than 90% of the maximum value	If the number of files reaches the maximum value, you should increase the value of the `db_files` Oracle paramerer
Free space on the database main partition	Free space on the partition that stores main information (By default: `/u01`)	30 minutes	🔴 – < 10 000 MB 🟡 – from 10000 to 20 000 MB 🟢 – > 20 000 MB	Dedicate more disk space for `/u01` (for details, see *InfoWatch Traffic Monitor. Installation Guide. Recommendations on Disk Space Partitioning*)
Free space in database events catalogue	Free space on the partitions that store events (By default: `/u02`)	30 minutes	🔴 – < 7% 🟡 – from 7 to 15% (if daily table spaces are stored in several sections, then when the value is < 7% in one section, at least) 🟢 – > 15%	If daily table spaces are stored in several sections, then the free space is calculated as a total sum of all sections, which during the installation were dedicated for storing daily table spaces. For details, see *InfoWatch Traffic Monitor. Installation Guide. Recommendations on Disk Space Partitioning*
Free space on daily events partition on fast disk	Free space on fast disk on partition that stores daily table spaces	30 minutes	🔴 – < 7% 🟡 – from 7 to 15% 🟢 – > 15%	The indicator is added, if during the installation *Fast and slow disks* storing mode was chosen.

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
				For details, see *InfoWatch Traffic Monitor. Installation Guide. Recommendations on Disk Space Partitioning*
Database patch availability	Whether Oracle patches, required for correct operation of the System, are installed	Once a day	🔴 – not installed 🟢 – installed	Indicator is on and displayed in the list only if Oracle DBMS is used in the System. Download and install the required patch.
Size of database alert log	Size of PostgreSQL DBMS alert log: System LogSize of Oracle DBMS alert log: Alert Log	5 minutes	🔴 – > 3 GB 🟡 – from 1 GB to 3 GB 🟢 – < 1 GB	Contact InfoWatch technical support at *support@infowatch.com*
DB syslog errors	Database log contains errors	30 minutes	🔴 – > 1 errors found 🟡 – 1 error found 🟢 – no errors found	It is necessary to decrease the number of errors with `SEVERITY=Error`
Mail traffic processing queue	Number of objects in queue **queue/smtp** (`iw_messed`)	30 minutes	🔴 – > 10000 objects 🟡 – from 1000 to 10000 objects 🟢 – < 1000 objects	1. Check status of service: `s ystemctl status iw_messed` 2. View service logs in `opt/iw/tm5/log/messed_app.log` 3. Check RAM and swap load: a. For a short response, run command `free -m` b. For a detailed response, run command `cat /proc/meminfo`

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
Queue for specific analysis for xAPI/pushAPI objects	Number of objects in queue **queue/analysis** (`iw_analysis`)	30 minutes	🔴 – > 10000 objects 🟡 – from 1000 to 10000 objects 🟢 – < 1000 objects	1. Check status of service: `s systemctl status iw_analysis` 2. View service logs in `opt/iw/tm5/log/analysis.log` 3. Check RAM and swap load: a. For a short response, run command `free -m` b. For a detailed response, run command `cat /proc/meminfo`
Queue of objects loading from interceptors to **iw_x2x** service	Number of objects from interceptors for **iw_x2x** queueing in **queue/db** (`iw_x2x`)	30 minutes	🔴 – > 10000 objects 🟡 – from 1000 to 10000 objects 🟢 – < 1000 objects	1. Check status of service: `s systemctl status iw_x2x` 2. View service logs in `opt/iw/tm5/log/x2x.log` 3. Check RAM and swap load: a. For a short response, run command `free -m` b. For a detailed response, run command `cat /proc/meminfo`
Loading to storage queue	Number of objects queueing in **queue/x2x**, which are to be loaded to storage by service **iw_x2db** (TMcap servers)	30 minutes	🔴 – > 10000 objects 🟡 – from 1000 to 10000 objects 🟢 – < 1000 objects	1. Check status of service: `s systemctl status iw_x2db` 2. View service logs in `opt/iw/tm5/log/x2db.log`

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
				3. Check RAM and swap load: a. For a short response, run command `free -m` b. For a detailed response, run command `cat /proc/meminfo`
Queue of applied policies actions processing	Number of objects queueing in **queue/ blackboard** (Linux servers)	30 minutes	🔴 – > 1000 objects 🟡 – from 200 to 1000 objects 🟢 – < 200 objects	1. Check status of service: `systemctl status iw_analysis` 2. View service logs in `opt/iw/tm5/log/analysis.log` 3. Check RAM and swap load: a. For a short response, run command `free -m` b. For a detailed response, run command `cat /proc/meminfo`
Queue of objects to be indexed in Sphinx for full-text search	Number of objects queueing to be indexed in Sphinx, for full-text search	30 minutes	🔴 – > 10000 objects 🟡 – from 1000 to 10000 objects 🟢 – < 1000 objects	1. Check status of service: `searchd --status -c /etc/infowatch/sphinx.conf` 2. View service logs in `opt/iw/tm5/log/sphinx/` 3. Check RAM and swap load: a. For a short response, run command `free -m` b. For a detailed response, run command

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
				`cat /proc/meminfo` 4. Calculate the number of running `searchd` instances: a. If `iw_is` is running on a node, then: 1 (`iw_is itself)` + 4 (`grep max_children /opt/iw/tm5/etc/is.conf)` = 5 b. If `iw_indexer` is running on a node, then: 1 (`iw_ndexer itself)` + 8 (`grep max_children /opt/iw/tm5/etc/sphinx.conf)` = 9 c. Total: a+b=14 `searchd` instances. The more processes, the less are the odds of slow user request processing.
Queue of objects to be indexed in Sphinx for meta-information search	Number of objects queueing to be indexed in Sphinx, for meta-information search	30 minutes	🔴 – > 10000 objects 🟡 – from 1000 to 10000 objects 🟢 – < 1000 objects	1. Check status of service: `searchd --status -c /etc/infowatch/sphinx.conf` 2. View service logs in `opt/iw/tm5/log/sphinx/` 3. Check RAM and swap load: a. For a short response, run command `free -m` b. For a detailed response, run command

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
				`cat /proc/meminfo`
Events indexation by **iw_indexer** service number of errors	Indexation errors number (`iw_indexer`)	30 minutes	🔴 – > 100 errors 🟡 – from 10 to 100 errors 🟢 – 10 errors	1. Check status of service: `s ystemctl status iw_indexer` 2. View service logs in `opt/iw/tm5/log/indexer.log` 3. Check RAM and swap load: a. For a short response, run command `free -m` b. For a detailed response, run command `cat /proc/meminfo`
Number of meta-information indexation by **iw_is** service errors	Number of errors occurred during indexation of meta-information by **iw_is** service	30 minutes	🔴 – > 100 errors 🟡 – from 10 to 100 errors 🟢 – 10 errors	1. Check status of service: `s ystemctl status iw_is` 2. View service logs in `opt/iw/tm5/log/is.log` 3. Check RAM and swap load: a. For a short response, run command `free -m` b. For a detailed response, run command `cat /proc/meminfo`
iw_is commands queue	Number of commands in **iw_is** service queue	30 minutes	🔴 – > 100 commands 🟡 – from 50 to 100 commands 🟢 – < 50 commands	
Data selection queues	Number of objects in **iw_is** service queue	30 minutes	🔴 – > 100 objects 🟡 – from 50 to 100 objects 🟢 – < 50 objects	
iw_is indexation queue	Number of commands in **iw_is** service queue	30 minutes	🔴 – > 100 objects 🟡 – from 50 to 100 objects	

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
			🟢 – < 50 objects	
iw_is errors queue	Whether **iw_is** service has errors	5 minutes	🔴 – > 500 errors found 🟡 – from 50 to 500 errors found 🟢 – < 50 errors found	
Queue of commands for text tablespace	Number of commands in text tablespace queue	30 minutes	🔴 – > 50 commands 🟡 – from 20 to 50 commands 🟢 – < 20 commands	1. Enable logging of **iw_indexer** service work on `debug` (see *Logging System Work*). 2. Check if log file `iw_indexer` in `opt/iw/tm5/log/indexer.log` has errors. 3. Contact InfoWatch technical support.
Queue of commands for meta-information tablespace	Number of commands in meta-information tablespace queue	30 minutes	🔴 – > 50 commands 🟡 – from 20 to 50 commands 🟢 – < 20 commands	

Events processing errors queue	Number of objects in errors queue **queue/errors** (Extractors Framework, TMcap servers: `iw_luaengined`, `iw_warpd`, `iw_cas`)	30 minutes	🔴 – > 500 objects
			🟡 – from 50 to 500 objects
			🟢 – < 50 objects
				Option 1: Clear queues by using the commands:
				`su - iwtm`
				`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/errors`
				`exit`
				Option 2:
				1. Open the `/etc/cron.d/iwtm_cleanup` file in the edit mode.
				2. Reduce the period of cleaning files in file queue folders. You can do it in a regular `cron` job (the default value is 30 days).
				3. Save changes and close the file.

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations

Errors queue of processing events by **iw_x2x**	Number of objects in queue **queue/x2x-errors** (`iw_x2x`)	30 minutes	🔴 – > 500 objects
			🟡 – from 50 to 500 objects
			🟢 – 50 objects
				Option 1: Clear queues by using the commands:
				`su - iwtm`
				`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/x2x-errors`
				`exit`
				Option 2:
				1. Open the `/etc/cron.d/iwtm_cleanup` file in the edit mode.
				2. Reduce the period of cleaning files in file queue folders. You can do it in a regular `cron` job (the default value is 30 days).
				3. Save changes and close the file.

Errors queue of processing events by **iw_x2db** service	Number of objects in queue **queue/x2db-errors** (`iw_x2db`)	30 minutes	🔴 – > 500 objects
			🟡 – from 50 to 500 objects
			🟢 – 50 objects
				Option 1: Clear queues by using the commands:
				`su - iwtm`
				`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/x2db-errors`
				`exit`
				Option 2:
				1. Open the `/etc/cron.d/iwtm_cleanup` file in the edit mode.
				2. Reduce the period of cleaning files in file queue folders. You can do it in a regular `cron` job (the default value is 30 days).

Indicator name	What is checked, where it is checked	Poll interval	Values	Details and recommendations
				3. Save changes and close the file.

Errors queue of applied policies actions processing	Number of objects in queue **queue/blackboard_errors** (Linux servers)	30 minutes	🔴 – > 500 objects
			🟡 – from 50 to 500 objects
			🟢 – 50 objects
				Option 1: Clear queues by using the commands:
				`su - iwtm`
				`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/blackboard-errors`
				`exit`
				Option 2:
				1. Open the `/etc/cron.d/iwtm_cleanup` file in the edit mode.
				2. Reduce the period of cleaning files in file queue folders. You can do it in a regular `cron` job (the default value is 30 days).
				3. Save changes and close the file.