

INFOWATCH

InfoWatch Traffic Monitor 4.1

Administrator Guide

INFOWATCH TRAFFIC MONITOR 4.1

Administrator Guide

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

Revision date: 24.12.2015

TABLE OF CONTENTS

INTRODUCTION 6
Who Should Read this Guide 6
Guide Structure 6
Additional Documentation 7
General Conventions 7
Technical Support 7
CHAPTER 1. INFOWATCH TRAFFIC MONITOR OVERVIEW 9
1.1. InfoWatch Traffic Monitor Features 9
1.2. InfoWatch Traffic Monitor Components 10
CHAPTER 2. MONITORING 11
2.1. Monitoring Subsystem for Distributed Architecture 11
2.1.1. Configuring Addresses of Time Synchronization Server for Monitoring Subsystem 12
2.1.2. Configuring Server Connections 12
2.1.3. Configuring Threshold Value for Load Indicator 14
2.1.4. Configuring Services Autorun 14
2.1.5. Configuring Notifications 14
2.1.5.1. Configuring Notifications on Indicators Threshold Exceeding 15
2.1.5.2. Configuring Sending Notification Mails via Postfix 15
2.1.6. Viewing Monitoring Indicators 16
2.2. Monitoring Subsystem for “All-in-one” Architecture 17
2.2.1. Web-console Interface 17
2.2.1.1. General Section 17
2.2.1.2. Network Section 19
2.2.1.3. System Monitoring Section 20
2.2.2. Configuring Addresses of Time Synchronization Server 20
2.2.3. License Management 21
2.2.3.1. Sending a License Renewal Request 21
2.2.3.2. License Installation 22
2.2.4. Managing Monitoring Indicators 22
2.2.4.1. Configuring Notifications of Monitoring Subsystem 22
2.2.5. Downloading Management Console Distributive 22
2.2.6. Accumulating Diagnostic Data 23
CHAPTER 3. CONFIGURING CRAWLER INTERCEPTOR 24
3.1. Configuring Network Access Rules 24
3.2. Crawler Configuration Files 26
3.2.1. Configuration File of Crawler Server 26
3.2.1.1. Changing Account Used for Crawler Server’s Service Start 26
3.2.2. Configuration File of Crawler Scanner 27
3.3. Crawler Log Files 27
CHAPTER 4. ADMINISTRATING A DATABASE 29
4.1. Routine Database Maintenance 29
4.2. Tablespaces in InfoWatch Traffic Monitor Database 30
4.2.1. Statuses of Daily Tablespaces 31
4.3. Managing Daily Tablespaces 31
4.3.1. Configuring Location of Files within File System 32

4.3.2. Indexing Data in Daily Tablespaces ... 32
4.3.3. Archiving Daily Tablespaces ... 34
4.3.4. Restoring Daily Tablespaces ... 35
4.3.5. Deleting Daily Tablespaces ... 36
4.4. Database Backup ... 37
4.4.1. Creating Database Backup ... 37
4.4.1.1. Defining the Size of Backup ... 37
4.4.1.2. Checking the Backup Storage ... 38
4.4.1.3. Creating Backup Directories ... 38
4.4.1.4. Creating Recovery Aid Files ... 38
4.4.1.5. Collecting a List of Files to Backup ... 39
4.4.1.6. Stopping IWTM System ... 40
4.4.1.7. Stopping Oracle Database ... 41
4.4.1.8. Copying database Files to the Backup Storage ... 41
4.4.2. Restoring the Database from the Backup ... 41
4.4.2.1. Restoring at the Same Database ... 41
4.4.2.2. Restoring at the New Database ... 42
CHAPTER 5. ADMINISTRATING THE SERVER END OF INFOWATCH TRAFFIC MONITOR ... 43
5.1. Traffic Monitor Server Processes ... 43
5.1.1. List of Traffic Monitor Server Processes ... 43
5.1.2. Using Traffic Monitor Server Processes ... 45
5.1.3. Verification of the Results of Configuration Update (iw_updater Process) ... 46
5.2. Configuring the Traffic Monitor Server Settings (tm.conf File) ... 47
5.2.1. The [GENERAL] Section ... 48
5.2.2. The [AUTO_RESTART] Section ... 48
5.2.3. The [SMTPD] Section ... 50
5.2.4. The [MESSED] Section ... 50
5.2.5. The [DELIVERD] Section ... 51
5.2.6. The [QUEUE] Section ... 51
5.2.7. The [SNIFFER] Section ... 52
5.2.8. The [HTTP] Section ... 52
5.2.9. The [ICQ] Section ... 53
5.2.10. The [SMTP] Section ... 54
5.2.11. The [PROXY] Section ... 54
5.2.12. The [PROXY_ICQ] Section ... 55
5.2.13. The [PROXY_HTTP] Section ... 55
5.2.14. The [PROXY_SMTP] Section ... 57
5.2.15. The [CAS] Section ... 58
5.2.16. The [ENCODE_DETECTOR] Section ... 60
5.2.17. The [DBLOADER] Section ... 60
5.2.18. The [FILTER] Section ... 61
5.2.19. The [ORACLE] Section ... 61
5.2.20. The [EXPRESSD] Section ... 61
5.2.21. The [EXTRACTOR] Section ... 62
5.2.22. The [UPDATER] Section ... 63
5.2.23. The [WARPD] Section ... 63
5.2.24. The [ADLIBITUM] Section ... 64
5.3. Configuring OCR Usage for Interceptors (tm_ocr.conf File) ... 64
5.3.1. The [*MESSED*] Section ... 64
5.3.2. The [*EXPRESSD*] Section ... 64

5.3.3. The [*EXTRACTOR*] Section ... 65
5.4. Configuring the Work with HTTP-Requests Transmitted by ICAP Protocol (icap.conf File) ... 65
5.5. Configuring the Processing of Attachments and Archives (detector.conf File) ... 66
5.6. Sample document database synchronization across multiple servers ... 68
5.7. Configuring the Maximum Size of Added Sample Document (casdbcfg.conf file) ... 69
5.8. Configuring filtering rules for Sniffer ... 70
5.9. Management of Loading Objects to Remote Database ... 71
5.9.1. Settings of Receiving Objects at Server End ... 71
5.9.2. Settings of Sending Objects at Client End ... 72
5.9.3. Configuring the Bandwidth of the Data Transmission Channel (Client) ... 72
5.9.4. Viewing the Statistical Information on Loading of Objects to a Remote Database ... 73
5.10. Archiving a Mail Queue Directory ... 74
5.11. Logging of System Work ... 74
5.12. Moving of Objects between Queues (iw_qtool Utility) ... 75
5.13. Loading an Object Queue ... 76
5.14. Recovering the System after Failures ... 77
APPENDIX A. INSTRUCTIONS FOR USING THE AUTOARCHIVE UTILITY ... 78
A.1. Setting the Archiving Options ... 78
A.2. Starting the Autoarchiving ... 79
A.3. Determining the Environment Variables ... 79
A.3.1. Searching the paths to the modules ... 79
A.3.2. Setting the ORACLE_HOME environment variable ... 80
A.3.3. Fast launch of autoarchiving ... 80
A.4. Repeated automatic archiving of restored tablespace ... 81
A.5. Error messages ... 81
APPENDIX B. MONITORING INDICATORS ... 83
APPENDIX C. TROUBLESHOOTING ... 87
GLOSSARY ... 89

INTRODUCTION

Who Should Read this Guide

This guide contains information on how to administrate InfoWatch Traffic Monitor: system configuration after installation, recovery and routine maintenance.

The information contained in the guide is intended for administrators of InfoWatch Traffic Monitor Server.

This guide is intended for the users with the following skills:

- Oracle DBMS administrating
- Red Hat Enterprise Linux maintenance and managing configuration files
- Microsoft Windows using.

Guide Structure

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

- *Chapter 1. InfoWatch Traffic Monitor Overview (page 9)*

  General information on InfoWatch Traffic Monitor (purpose, main functions).

- *Chapter 2. Monitoring (page 11)*

  Description of installation and use of Monitoring subsystem that enables remote operations monitoring for servers where InfoWatch Traffic Monitor components & related services are installed.

- *Chapter 3. Configuring Crawler Interceptor (page 24)*

  Describes how to configure the Crawler subsystem to perform revisions of the files located in corporative network.

- *Chapter 4. Administrating a Database (page 29)*

  The description of the tasks on managing the InfoWatch Traffic Monitor database (routine maintenance, management of data segments).

- *Chapter 5 Administrating the Server End of InfoWatch Traffic Monitor (page 43)*

  Information on managing the server end after the installation of the System (additional configuration and monitoring of the server end).

- *Appendix A. Instructions for using the autoarchive utility (page 78)*

  Describes how to configure the automatic backup of the daily tablespaces with a special utility that is included in the distribution package of the System.

- *Appendix B. Monitoring Indicators (page 83)*

  List of indicators used by Monitoring subsystem to check System components status.

  List and description of monitoring indicators checking System state. Description of actions which the administrator should perform when indicator succeeds its threshold value.

- *Appendix C. Troubleshooting (page 87)*

  Description of the problems that may arise during the operation of the System, as well as troubleshooting tips.

Additional Documentation

For more information see the following documents:

- *"InfoWatch Traffic Monitor. Installation and Configuration Guide"*

  This document describes installing, configuring, updating and deleting the InfoWatch Traffic Monitor.

- *"InfoWatch Traffic Monitor. User Guide"*

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

- *"InfoWatch Device Monitor. User Guide"*

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

- *"InfoWatch OCR for IWTM 4.1. Installation Guide"*

  The document describes installation and implementation procedure of the IW OCR module designed for images extracting from intercepted files.

General Conventions

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

Style	Description	Example
Bold	Bold indicates GUI elements (buttons, menu commands, etc), system components (if they are mentioned for the first time in the document).	The **iw_qtool** utility is used to move objects form one queue to another.
Italics	Italics indicate tables, examples and descriptions, specifically the names and values of object attributes.	The content filtering database contains the *Contract* term.

`The Courier New font`	The font indicates file names, program code examples.
	When describing configuration files, the style denotes setting values, the examples of settings.
		You can verify that Traffic Monitor is running with the commands:
		`service iw-trafmon status`
		`service iw-caserv status`

`THE COURIER NEW FONT (UPPER CASE)`	This font is used in the descriptions of the configuration files and indicates the file sections (in square brackets), variables and settings. If this font is used in the description of a database, it indicates SQL keywords, PL/SQL instructions, data types and privileges	The autorun settings are specified in `/usr/local/infowatch/tm3/etc/tm.conf` file (`[AUTO_RESTART]` section)

Technical Support

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

- If you purchased the product from InfoWatch's partner, then contact the Technical Support Service of this partner company.

- If you purchased the product directly from InfoWatch, you can contact our Technical Support Service at support@infowatch.com.

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

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

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

CHAPTER 1. INFOWATCH TRAFFIC MONITOR OVERVIEW

This chapter covers the following topics:

- *InfoWatch Traffic Monitor Features (i. 1.1 on page 9).*
- *InfoWatch Traffic Monitor Components (i. 1.2 on page 10).*

1.1. InfoWatch Traffic Monitor Features

InfoWatch Traffic Monitor allows you to control data traffic in the corporate network in order to detect and prevent unauthorized use of confidential data.

InfoWatch Traffic Monitor Main Features:

- Intercepting SMTP traffic. The System also can intercept traffic (or a copy of traffic) relayed by a mail relay server or a copy of traffic which goes through the equipment supporting the CISCO SPAN features
- Intercepting HTTP traffic. The System allows intercepting traffic transmitted through an ICAP proxy server or a copy of traffic which goes through the equipment supporting the CISCO SPAN features
- Intercepting a copy of ICQ traffic (the OSCAR protocol) transmitted through the equipment supporting the CISCO SPAN features. When ICQ connects through HTTP, the System intercepts ICQ traffic in a way that is similar to HTTP traffic
- Reviewing files located in the corporative network (open network folders, workstation local discs and SharePoint 2007 file storage) with Crawler subsystem.
- Analyze the Skype traffic, shadow copies of files and print jobs, traffic transferred by FTP protocol, control sharing data through Jabber (XMPP protocol) and through Mail.Ru Agent (MPP protocol). Interception of listed data is performed by InfoWatch Device Monitor system.
- Analyze the file shadow copies intercepted by DeviceLock version 6.3 or higher (provided by SmartLine, Inc.) to detect the violations of the corporate security policy
- Analyze the contents of the intercepted traffic to detect the violations of the corporate security policy
- Filtering the intercepted traffic by allowing or blocking delivery of certain data

> **Note:**
>
> This feature is not available when the copy of traffic is processed.

1.2. InfoWatch Traffic Monitor Components

InfoWatch Traffic Monitor component	Purpose
Server end	**Traffic Monitor Server**: intercepts, analyzes and filters traffic, analyzes data received from the InfoWatch Device Monitor and DeviceLock systems. **Sniffer**: intercepts a copy of traffic which goes through the SPAN port of a switch and transfers it for analysis. **ICAP integration module**: intercepts, analyzes and filters HTTP traffic transmitted through the ICAP server. ICAP server is a part of the ICAP module. **Crawler**: reviewing files located in the corporative network (open network folders, workstation local discs and SharePoint 2007 file storage). **Remote database management module**: transmits data for storage to a remote database over narrow-band channels
Database	Stores the information provided by the system running (intercepted data, results of the analysis)
Management Console	Configures the rules for traffic analyzing and filtering, analysis of the incoming data

CHAPTER 2. MONITORING

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

Monitoring subsystem exercises the following functions:

- Monitoring operations of all servers (both physical and virtual) included in InfoWatch Traffic Monitor solution
- Monitoring of all software components (OS, DBMS, DB, processes etc.) included in InfoWatch Traffic Monitor solution
- Control of indicator values for each server and component. Here by control we mean regular retrieval of indicator value and comparing this indicator value to a threshold value. For more details on indicators, see i. 2.1.6 at page 16 and Appendix B at page 83.
- Enabling or disabling monitoring of specific indicators or servers.
- Sending email notifications when indicator values exceed the normal range.

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

If InfoWatch Traffic Monitor system is deployed in such a way that the database server (**IWDBX** kickstart option) is installed apart of Traffic Monitor server (servers) (**IWTMX** kickstart option), then the Monitoring subsystem is operating at the database server. To perform a diagnostic of all servers included to the solution, system administrator should make some additional settings. For more details see i. 2.1 at page 11.

If InfoWatch Traffic Monitor system is deployed in such a way that all the server components (both database server and TM servers) are located at one computer (**IWALLX** or **IWTMSX** kickstart option), then administrator can use simplified management with the web-interface accessible from any browser of any workstation of the local network. For more details see i. 2.2 at page17.

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

2.1. Monitoring Subsystem for Distributed Architecture

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

- *Configuring Addresses of Time Synchronization Server (i 2.1.1 at page 12)*
- *Configuring Server Connections (i 2.1.2 at page 12)*
- *Configuring Threshold Value for Load Indicator (i 2.1.3 at page 14)*
- *Configuring Services Autorun (i 2.1.4 at page 14)*
- *Configuring Notifications (i. 2.1.5 at page 14)*
- *Viewing Monitoring Indicators(i. 2.1.6 at page 16)*

2.1.1. Configuring Addresses of Time Synchronization Server for Monitoring Subsystem

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

To configure time synchronization at the server:

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

2.1.2. Configuring Server Connections

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

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

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

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

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

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

- TMCap servers – interception servers
- TMCas servers – servers with analysis subsystem
- DB-servers – servers with Oracle DB which is used by InfoWatch Traffic Monitor
- IW-Linux-servers – all servers containing server InfoWatch Traffic Monitor components
- DM-servers – servers with InfoWatch Device Monitor (optional parameter; disabled by default).

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

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

Example 1. Default settings

The following servers are used:

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

```
define host{
        use                     linux-server
```

```
        host_name               TMcap1
        alias                   "TM capture stack server1"
        address                 127.0.0.1
        }

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

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

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

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

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

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

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

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

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

```
define host{
       use                     linux-server
       host_name               IWTM
       alias                     "Traffic Monitor server"
       address                 127.0.0.1
       }
```

```
define hostgroup{
       hostgroup_name  TMcap-servers
       alias                   IW Traffic Monitor Capture Stack Servers
       members             IWTM
       }
define hostgroup{
       hostgroup_name  TMcas-servers
       alias                    IW Traffic Monitor Content Analysis Servers
       members             IWTM
       }
define hostgroup{
       hostgroup_name   DB-servers
       alias                    Oracle Database for IW Traffic Monitor Servers
       members             IWTM
       }
define hostgroup{
       hostgroup_name   IW-Linux-servers
       alias                    All IW Servers
       members             IWTM
       }
```

Running setup script

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

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

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

2.1.3. Configuring Threshold Value for Load Indicator

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

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

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

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

2.1.4. Configuring Services Autorun

Run nagios and apache services for the web-interface:

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

Configure nagios and apache services autorun:

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

2.1.5. Configuring Notifications

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

In this section:

- Configuring Notifications on Indicators Threshold Exceeding (i. 2.1.5.1 on page 15).

- Configuring Sending Notification Mails via Postfix (i. 2.1.5.2 on page 15).

2.1.5.1. Configuring Notifications on Indicators Threshold Exceeding

To set up sending of email notifications:

1. In `nagios` user's `$HOME` (`/var/log/nagios`) create `.forward` file.
2. In newly created `.forward` file list email addresses to send notifications to. Each address is specified in a separate string.

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

3. Define the name to be displayed in «*From:*» field for notification mails. For this purpose specify the name of the system in the `gecos` field in `/etc/passwd` file for `nagios` user.

   > **Warning!**
   >
   > For InfoWatch-supported projects including sender email address should be specified in the following format:
   >
   > `[PRJ]<nagios@example.com>`
   >
   > where `PRJ` is the project code and `example.com` – your mail domain.

4. Based on LAN configuration set up sending mails from server with monitoring subsystem installed to the addressed listed in `.forward` file.

Notifications will contain the following information:

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

2.1.5.2. Configuring Sending Notification Mails via Postfix

If the installation of the System enables sending SMTP-messages via Postfix (see "*InfoWatch Traffic Monitor. Installation and Configuration Guide*", "*System Deployment Schemas*" chapter), then for correct sending of notification mails you should:

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

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

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

   A separate string should be specified for each recipient.

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

2. Run the command:

   `postmap /etc/postfix/transport`

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

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

4. Restart Postfix:

```
service postfix restart
```

2.1.6. Viewing Monitoring Indicators

Monitoring is available via web-interface at the following address: http://server_name/nagios/, where `server_name` is the name or IP address of the server hosting monitoring subsystem.

Default account for access:

- login **nagiosadmin**
- password **nagiosadmin**

You can change access login or password in `/etc/nagios/htpasswd.users` file by running the following command:

```
htpasswd /etc/nagios/htpasswd.users <USERNAME>
```

System & hosts status overview

Status of the entire system as well as the status of each server where the System is deployed may have one of the following values:

- operative
- partially inoperative
- totally inoperative

Indicators status overview

To review indicators status please go to the **Services** section.

The following information is displayed for each indicator:

- **Service** – indicator name.
- **Status** – current indicator value:
  - – CRITICAL, value of a checked setting exceeds critical threshold;
  - – WARNING, value of a checked setting is within the warning area (if any);
  - – OK, setting value is within the normal range.
- **Last Check** – date and time of the last check.
- **Duration** – duration of current indicator status.
- **Attempt** – number of a successful attempt (out of total count of possible attempts) of indicator value retrieval.
- **Status Information** – detailed information on check results.

If an indicator value retrieval was failed, then the current indicator value is considered as exceeding the threshold value.

Indicator settings setup is carried out in configuration files located in `/etc/nagios/iwmon/` folder:

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

Page 83 of Appendix B lists all indicators with reference to their check frequency values as well as to administrator actions when indicators achieve their threshold.

For more details on configuring indicator operations, see Nagios documentation: http://nagios.sourceforge.net/docs/nagioscore/3/en/objectdefinitions.html.

2.2. Monitoring Subsystem for “All-in-one” Architecture

If InfoWatch Traffic Monitor system is deployed in such a way that all the server components (both database server and TM servers) are located at one computer (**IWALLX** or **IWTMSX** kickstart option), then administrator can use simplified management with the web-interface accessible from any browser of any workstation of the local network.

To enter web-console:

1. In the address bar of any browser enter Traffic Monitor server IP-address.
2. Enter credentials of Traffic Monitor Management Console administrator account:
    a. In the **Login** field enter **administrator**
    b. In the **Password** field enter **xxXX1234**

> **Warning!**
>
> Above the default settings of administrator account are specified. It is strongly recommended to change the password of this account after Management Console installing. See more information in *«InfoWatch Traffic Monitor. User guide»*.

3. Click **Authentificate**.

The facilities of web-console are described in the following sections:

- *Web-console Interface (see i 2.2.1 at page 17)*
- *Configuring Addresses of Time Synchronization Server (see i 2.2.2 at page 20)*
- *License Management (see i 2.2.3 at page 21)*
- ***Ошибка! Источник ссылки не найден.*** *(see i* ***Ошибка! Источник ссылки не найден.*** *at page* ***Ошибка! Закладка не определена.****)*
- *Managing Monitoring Indicators (see i 2.2.4 at page 22)*
- *Downloading Management Console Distributive (see i at page 2.2.5 at page 22)*
- *Accumulating Diagnostic Data (see i 2.2.6 at page 23)*

2.2.1. Web-console Interface

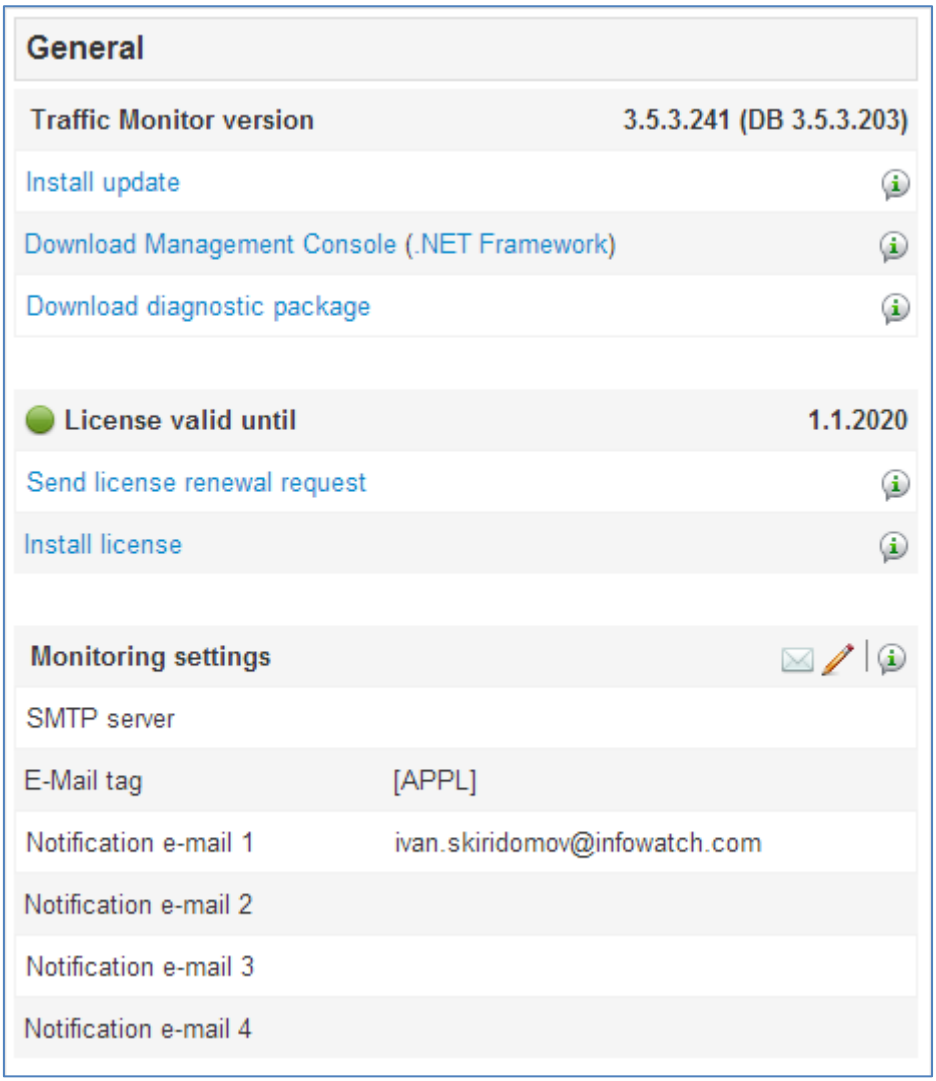
The web-console is designed for administrator to manage Traffic Monitor server. This section contains description of web-console interface elements and links to another document sections describing details on diagnostic and management features.

IWTM web-console is conventionally divided to three main areas:

- **General** – updates installation, downloading Management Console, managing the license and monitoring notifications: see i. 2.2.1.1 at page 17.
- **Network** – managing network parameters: see i. 2.2.1.2 at page 19.
- **System monitoring** – monitoring indicators: see i. 2.2.1.3 at page 20.

2.2.1.1. General Section

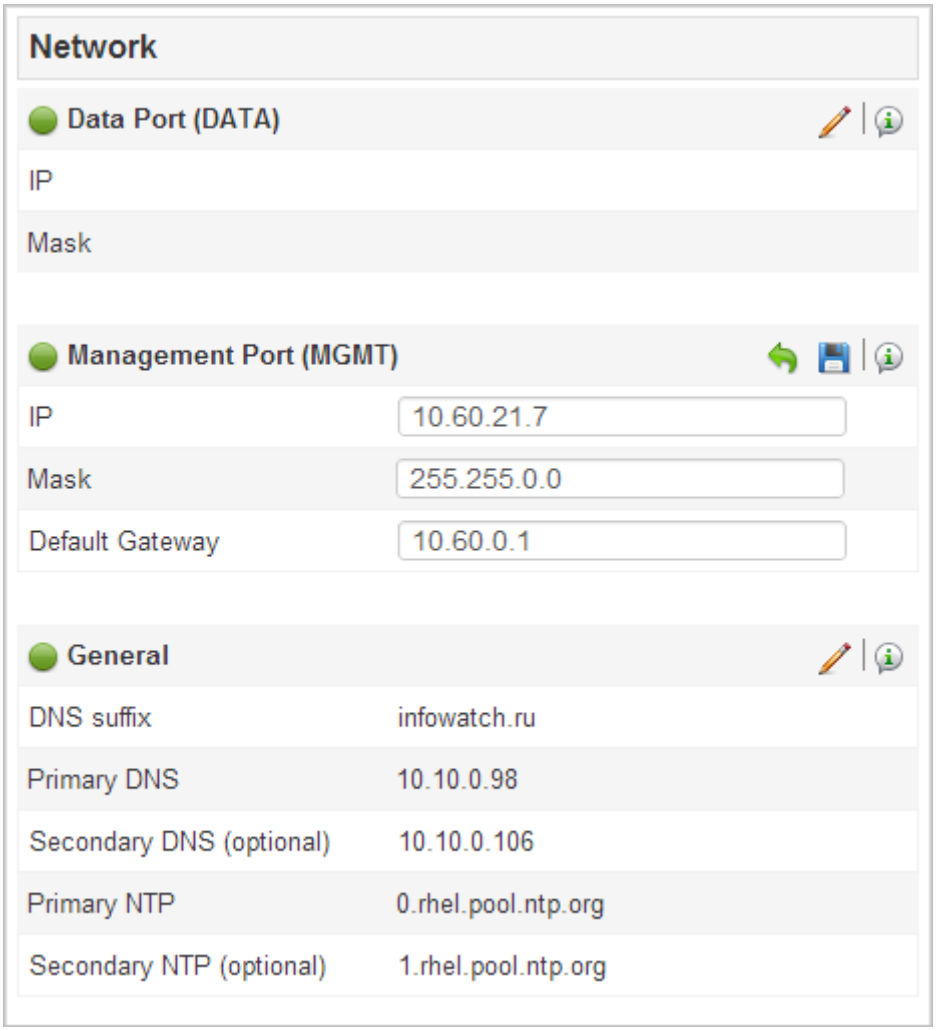
The **General** section contains information on system version, period of license validity. It allows you to install system updates, to download the Management Console to manage the license and to configure the monitoring notifications.



Setting	Description, links
Traffic Monitor version	Traffic Monitor server version. The database schema version is specified in brackets.
Install Update	Server updates installation. For details see i. **Ошибка! Источник ссылки не найден.** at page **Ошибка! Закладка не определена.**.
Download Management Console (.Net Framework)	Management Console distributive downloading. For details see i. 2.2.5 at page 22
Download diagnostic package	Gathering the data for server diagnostic. For details see i. 2.2.6 at page 23
License valid until	Validity end date for installed license.
Send license renewal request	Sending a request to the InfoWatch Technical Support Service for a license renewing. For details see i. 2.2.3.1 at page 21.
Install license	System license installation. For details see i 2.2.3 at page 21.
Monitoring settings	Group of configurations notification from Monitoring subsystem. For details see i. 2.2.4.1 at page 22

2.2.1.2. Network Section

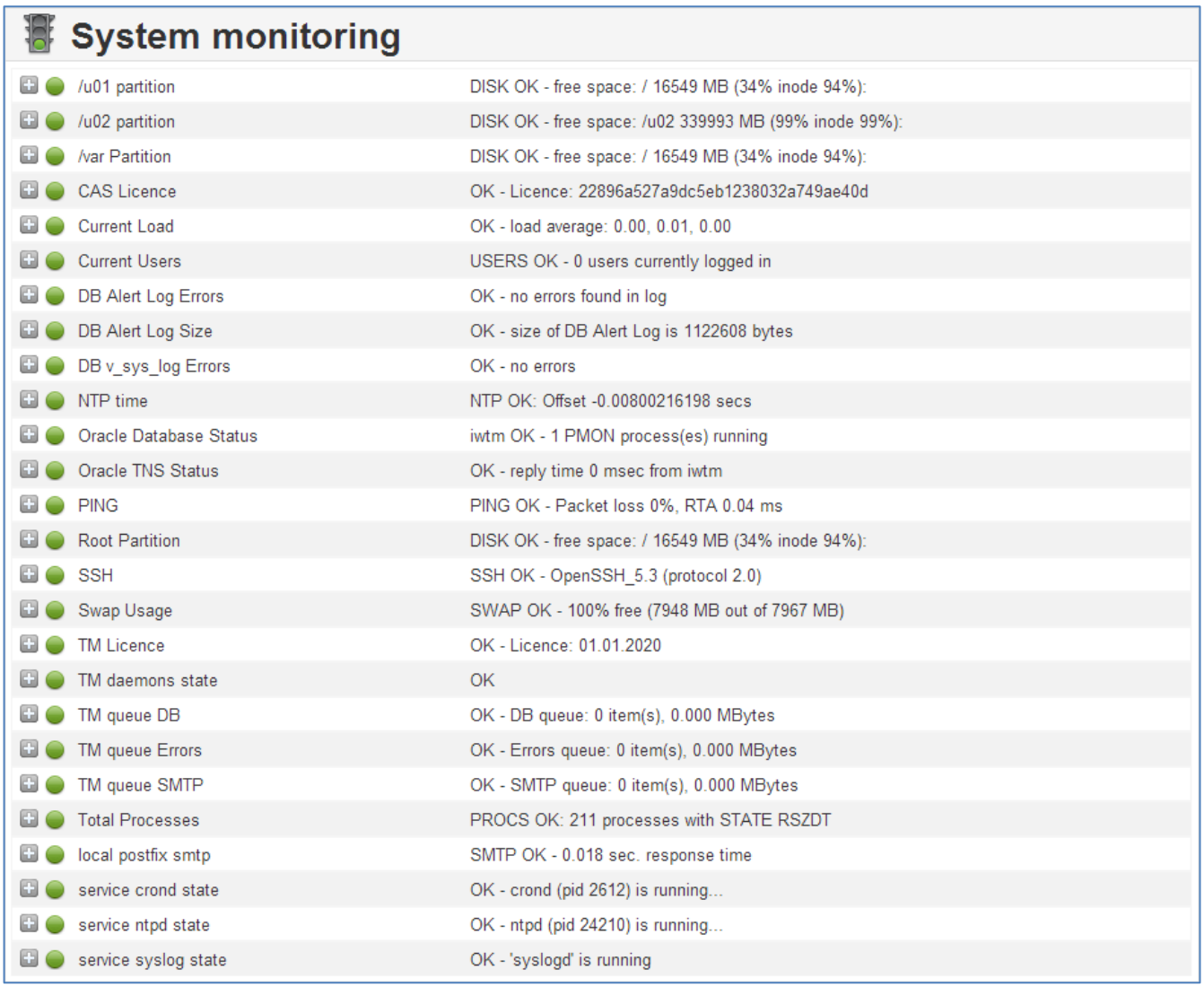
The **Network** section is designed for managing network connections of IWTM server.



Setting	Description
Data Port (DATA)	Network parameters of a port used for delivering traffic to analysis from ICAP servers, SPAN-copy; from InfoWatch Device Monitor and so on. See details in implementation schema in "*InfoWatch Traffic Monitor. Installation and Configuration Guide*" document.
Management Port (MGMT)	Network parameters of a port used for management Console connecting to IWTM server. This port can be used for delivering traffic to analysis. See details in implementation schema in "*InfoWatch Traffic Monitor. Installation and Configuration Guide*" document.
DNS/NTP	General network parameters of IWTM server: DNS, NTP

2.2.1.3. System Monitoring Section

The **System monitoring** section displays indicators of Monitoring subsystem allowing diagnostics of different system components states.



The current state is displayed for each indicator:

- – parameter value is within the normal range
- – parameter value is within the warning area (if any)
- – parameter value exceeds critical threshold.

The common information on current indicator state is displayed in the string; to receive detailed data click in the beginning of indicator string.

Description of indicators, their threshold values, polling periods and actions which the administrator should perform when indicator succeeds its threshold value, are listed in Appendix B at page 83.

2.2.2. Configuring Addresses of Time Synchronization Server

General server parameters of InfoWatch Traffic Monitor servers are set during in (see «*InfoWatch Traffic Monitor. Installation and Configuration Guide*». However to provide correct time synchronization, IP address of NTP-server should be specified at the 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. In the web-console, **General** section, **Network** area, click  **Edit**.
2. Specify NTP-server IP address in **Primary NTP** field
3. In necessary, you can specify **Secondary NTP**.
4. Click  **Save**.
5. After the IP-addresses change is done, run the `service network restart` command.

2.2.3. License Management

InfoWatch Traffic Monitor operation requires actual license. The trial license is valid for 30 days after the Traffic Monitor Server is installed. To continue using the System, you must install a commercial license for the interceptors which you plan to use.

Current license state is displayed in web-console. In the **License valid until**… string a license validity end date is displayed. Further there is **TM Licence** indicator in the **System monitoring** section. If indicator state alarms about expiry date approaching (**Warning** – less than two weeks; **Critical** – less than two days) than the notification is sent to administrator address specified as described in i. 2.2.4.1 at page 22

Consider these items when you install and use a license key:

- If the validity period of a trial license has expired, interceptors will be disabled. If this is the case, you must renew the license or uninstall the System.
- If you change configuration of the traffic transfer according to the new deployment scheme, please replace a license key considering new interceptors.
- The license key (`iw_license.dat` file) is permanently bound to the hardware and software configuration of the computer, where a request for the license was generated. Thus, after moving `iw_license.dat` file to another computer, InfoWatch Traffic Monitor feature will not be available
- If you completely re-install InfoWatch Traffic Monitor, you need to install license newly. Therefore it is recommended to save `iw_license.dat` file to the external media.

The license key (**iw_license.dat** file) is permanently bound to the hardware and software configuration of the computer, where a request for the license was generated. Thus, after moving license file to another computer InfoWatch Traffic Monitor feature will not be available.

To install a new license key or replace the current one:

1. Request a new license key as described in i. 2.2.3.1 at page 21.
2. Install received license key as described in i. 0 at page 21.

Current license state is displayed in web-console. In the **License valid until**… string a license validity end date is displayed. Further there is **TM License** indicator in the **System monitoring** section. If indicator state alarms about expiry date approaching (**Warning** – less than two weeks; **Critical** – less than two days) than the notification is sent to administrator address specified as described in i. 2.2.4.1 at page 22.

2.2.3.1. Sending a License Renewal Request

To request a new license:

1. At the web console, in **General** section click **Send license renewal request**.

   Then an e--mail to Technical Support Service is generated. E-mail body contains unique code generated personally for your TM server instance. Do not change this code!

2. Send a letter.

Within the time limit prescribed by Service Level Agreement you will receive a license key file - **iw_license.dat**.

2.2.3.2. License Installation

To install Traffic Monitor license:

1. Place the license key (**iw_license.dat** file) received after request (see i. 2.2.3.1 at page 21) at the computer where TM web console is running, or at the resource it has an access.
2. At the web console, in **General** section click **Install license**
3. At the opening file dialog window select **iw_license.dat** file and click **OK**.
4. Wait for the license installation (**Installing license…** status).

As a result of successful installation, license validity end date (displayed in **License valid until**) is renewed.

2.2.4. Managing Monitoring Indicators

Monitoring subsystem of the InfoWatch Traffic Monitor system provides remote monitoring of server parameters, network services and other indicators of the system.

The subsystem periodically receives indicators values and compares them with threshold values. You can view information on the current indicators state in the TM web-console, **System monitoring** section. To receive more detailed data click  in the beginning of indicator string.

Description of indicators their threshold values, polling periods and actions which administrator should perform if indicator reaches its threshold values, are listed in Appendix A at page 83.

Monitoring subsystem also provides sending email notifications to system administrator if at least one of indicators reaches its threshold value. The configuring of notifications sending see in i. 2.2.4.1 at page 22.

2.2.4.1. Configuring Notifications of Monitoring Subsystem

To configure sending of email notifications from Monitoring Subsystem to specified addresses of system administrators:

1. In the web-console, **Monitoring settings** section, click  **Edit**.
2. Specify parameters of notifications sending:
   - **SMTP server** – address of mail server used for sending.
   - **E-Mail tag** – prefix added to heads of all e-mails sent by Monitoring subsystem.

     > **Note:**
     >
     > For projects with InfoWatch technical support please specify **[SUP]**. For implementation or pilot InfoWatch projects specify **[PRJ]** where **PRJ** is an implementation/pilot project code.

   - **Notification e-mail** – address which should receive notifications.

     > **Note:**
     >
     > For projects with InfoWatch technical support the additional monitoring@infowatch.com address is recommended.

3. Save chances: click  **Save**.
4. Check the settings consistency: click  **Send test email**. If parameters were correct, specified addresses receive test e-mail.

2.2.5. Downloading Management Console Distributive

InfoWatch Traffic Monitor Management Console application is the main tool for managing system settings and monitoring results of its work. Detailed information on working with Management Console see in *«InfoWatch Traffic Monitor. User Guide»* document.

To download Management Console distributive, in the web-console, **General** section, click **Download Management Console**.

To download .Net Framework platform needed for Management Console operation, in the web-console, **General** section, click **.NET Framework**.

The procedure of Management Console installation is described in «*InfoWatch Traffic Monitor. Installation and Configuration Guide*» document.

2.2.6. Accumulating Diagnostic Data

If any system problems occur and you cannot resolve using standard methods described in system documentation and in Knowledge Base section at InfoWatch customer site (http://cp.infowatch.com/en/kb), you can contact the InfoWatch Technical Support Service. For resolving some issues you should need to accumulating diagnostic data on the system.

IWTM web-console allows you to accumulate diagnostic data from TM server using **sosreport** utility. This is standard Linux tool designed for accumulating detailed information on the system: hardware parameters, list of installed packages, configured settings, etc.

To receive system diagnostic data:

1. In the web-console, **Monitoring settings** section, click **Download diagnostic package**.
2. Wait for ending the accumulating information process (the «**collecting…**» state is displayed), do not make any configurations.
3. When **download link** appears, click it to download a package containing diagnostic data.

Resulting file has a name `sosreport-iwdb-xxx-yyy.tar.xz`, where `xxx` is server name and `yyy` is date of file creation. You can send the resulting file to InfoWatch Technical Support Service.

CHAPTER 3. CONFIGURING CRAWLER INTERCEPTOR

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

Crawler subsystem operates as one of Traffic Monitor interceptors.

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

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

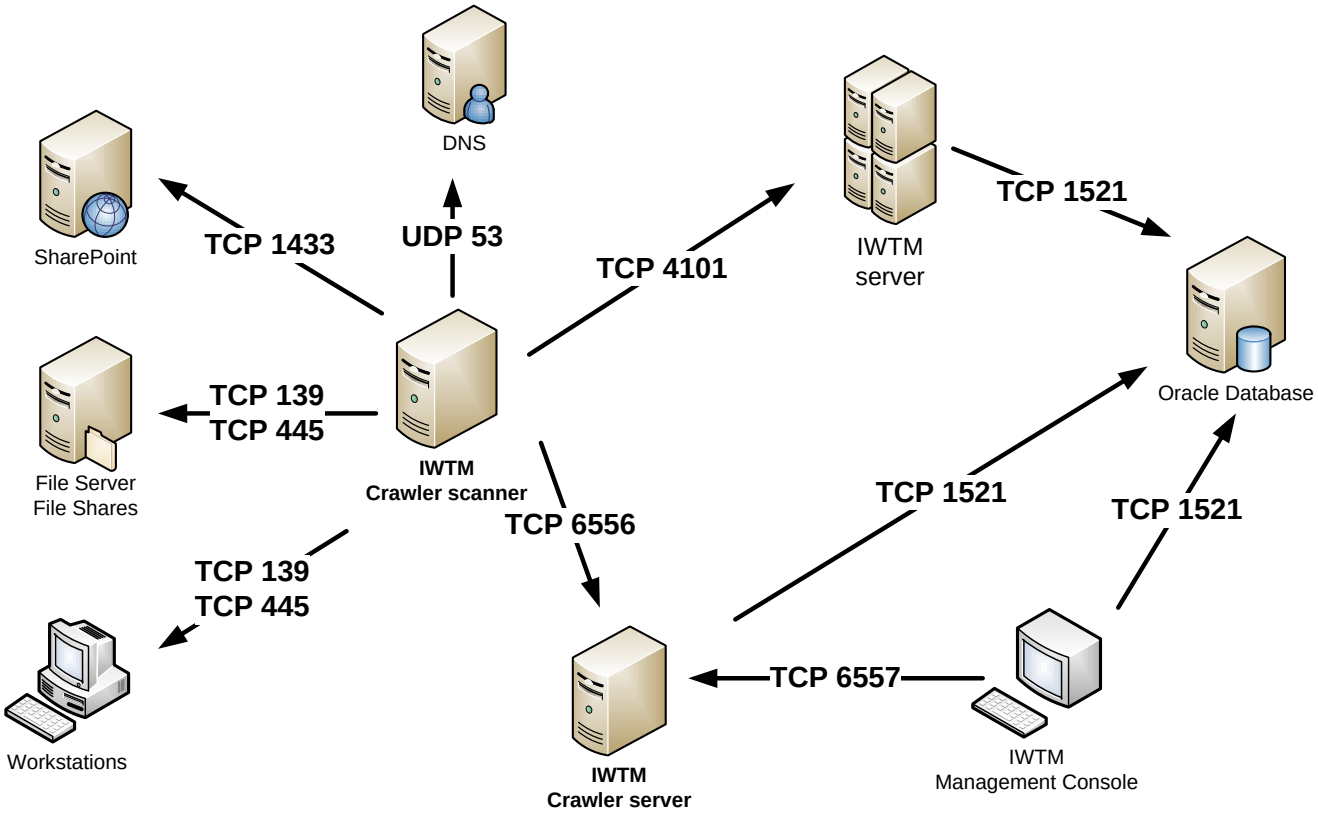
See detailed information on the Crawler configuration in following sections:

- *Configuring Network Access Rules (i 3.1 at page 24)*
- *Crawler Configuration Files (i 3.2 at page 26)*
- *Crawler Log Files (i 3.3 at page 27)*

3.1. Configuring Network Access Rules

If network segments where InfoWatch Traffic Monitor with Crawler is deployed, are divided by firewalls, then for correct Crawler operation TCP ports **6556** (Crawler scanner connects to Crawler server) and **6557** (IWTM Management Console connects to Crawler server) should be opened.

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



Connection	Port	Comments
Crawler scanner – Crawler server	TCP 6556	
Crawler server – БД IWTM	TCP 1521	
Management Console – Crawler server	TCP 6557	
Crawler scanner – DNS server	UDP 53	
Crawler scanner – workstations and file servers	TCP 139 TCP 445	
Crawler scanner – IWTM server	TCP 4101	Configured in the IWTM server configuration file `tm.conf`, `[EXPRESSD]` section, `Listen-Port` setting (see i. 5.2.20 at page 61)
Crawler scanner – SharePoint file storage (MS SQL server)	TCP 1443	

If any system components belong to different domain controllers then Crawler needs Domain Trust setting for controllers in such a system. However it should be taken into account that farness of Crawler scanner from scanned objects can significantly increase network load. That's why we recommend to deploy a computer where Crawler scanner works so that it was located in the network segment maximally near to scanned segments.

3.2. Crawler Configuration Files

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

- **Crawler server** – `InfoWatch.Crawler.Server.exe.config`. Located in the same directory as executed file `InfoWatch.Crawler.Server.exe` (default – `C:\Program Files (x86)\InfoWatch\Crawler\Server` for 32-bit systems and `C:\Program Files (x86)\InfoWatch\Crawler\Server` v). See details in i. 3.2.1 at page 26.
- **Crawler scanner** – `InfoWatch.Crawler.Scanner.exe.config`. Located in the same directory as executed file `InfoWatch.Crawler.Scanner.exe` (default – `C:\Program Files (x86)\InfoWatch\Crawler\Scanner` for 32-bit systems and `C:\Program Files (x86)\InfoWatch\Crawler\Scanner` for 64-bit systems). See details in i. 3.2.2 at page 27.

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

3.2.1. Configuration File of Crawler Server

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

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

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

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

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

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

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

  > **Note:**
  >
  > If you need to change an account used for server start, then prior to first server service starting enter DB password to the `NewDbPassword` field as encoded password can be decoded only by user encoded it. See more details i 3.2.1.1 at page 26.

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

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

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

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

1. At the computer where Crawler server works, in the list of Windows services, find `iw_crawler_server` service and stop it.

2. In the server configuration file `InfoWatch.Crawler.Server.exe.config` (see details in i 3.2.1 at page 26), in `NewDbPassword` setting enter a password of IWTM schema owner account, used for database connection. Save modified configuration file.
3. Return to `iw_crawler_server` service and call it **Properties** (**Actions -> Properties** or select it in the context menu opening by right-click at the service string). At the **Log On** tab specify settings of account used for starting the Crawler server's service.
4. Run server's service.

3.2.2. Configuration File of Crawler Scanner

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

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

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

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

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

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

It is strongly recommended not to change other settings.

3.3. Crawler Log Files

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

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

Changing log files location

Location of log files is defined in configuration files (`InfoWatch.Crawler.Server.exe.config` and `InfoWatch.Crawler.Scanner.exe.config`: see i 3.2 at page 26), `<configuration>` section, value for `<listeners>` setting, for example:

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

Configuring Crawler log level

Log level is defined in configuration files (`InfoWatch.Crawler.Server.exe.config` and `InfoWatch.Crawler.Scanner.exe.config`: see i 3.2 at page 26), `<specialSources>` section, value for `<allEvents switchValue="All" name="All Events">` setting. By default the **All** value is set: all the events are logged. You can change this value to one of the following (listed in order of details decreasing): **All**, **Verbose**, **Information**, **Warning**, **Error**, **Critical**, **Off**.

CHAPTER 4. ADMINISTRATING A DATABASE

This chapter covers the following topics:

- *Routine Database Maintenance (i. 4.1 on page 29).*
- *Tablespaces in InfoWatch Traffic Monitor Database (i. 4.2 on page 30).*
- *Managing Daily Tablespaces (i. 4.3 on page 31)*
- *Database Backup (i. 4.4 on page 37).*

4.1. Routine Database Maintenance

> **Note:**
>
> Do not power DB server off with power button: in certain cases this may cause the DB corruption.

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

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

   ```
   service iw-trafmon stop
   ```

3. Make sure TM processes autorun is not configured:

   ```
   ll /etc/cron*
   crontab -l
   ```

   If `crontab` file contains this setting, it should be disabled for the time of schedule maintenance.
4. Retrieve list of scheduled jobs from database server. For this purpose run the following query in sqlplus using schema owner account:

   ```
   select JOB_NAME, STATE
   from user_scheduler_jobs u
   where u.enabled = 'TRUE'
   ```

5. 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.
6. 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;
   /
   ```

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

    ```
    service iw-trafmon start
    ```

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

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

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

12. Enable running previously disabled jobs:

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

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

4.2. Tablespaces in InfoWatch Traffic Monitor Database

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

The type of tablespace	Purpose
Main	Storing of the settings that are needed for the analysis and processing of the objects (configuration, tags, colors, etc.). Managing the System using the Management Console (roles, user accounts, etc.)
Daily	Storing of objects, intercepted within one day. Storing of information on the results of the analysis and processing of the objects (analyzed object categories, terms, etc.)

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

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

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

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

4.2.1. Statuses of Daily Tablespaces

> **Note:**
> List of daily TS and their current status can be found in Management Console (the **Database Usage** section).

The list of tablespace statuses and status codes is provided in the following table.

Status Code	Name	Description
1	ReadWrite	Is assigned to each new daily TS. You can add, modify, or delete data stored in the daily TS (for example, sampling of objects on request, assigning the object tags, etc.)
2	Offline	Is assigned during the procedure of disabling the daily TS from the database. Users can not access the data until the TS will not be restored
3	Restored	The status is assigned to a tablespace that is restored from an archive Users can view and modify data stored in the TS (the selection of objects on request, assigning the object tags, etc.)
4	InProgress	Intermediate states. Used in procedures to disable and restore daily TS. The time when a daily TS remains in one of the statuses depends on the size of the disconnected TS and also on the productivity and load of a database server. The maximum time is 1 hour. Exceeding the limit indicates an error. To solve this problem consult technical support service
5	ReadOnly	
6	PreparedForOffline	

The following table contains various transitions between the statuses of daily tablespaces. The «+» sign means that the transition is possible. Sign «-» marks the impossible transitions.

Initial status	Target status					
	ReadWrite	ReadOnly	Offline	Restored	InProgress	PreparedForOffline
ReadWrite	-	+	-	-	+	-
ReadOnly	-	-	-	-	+	-
Offline	-	-	-	-	-	+
Restored	-	-	-	-	+	-
InProgress	-	-	-	-	-	+
PreparedForOffline	-	-	+	+	-	-

4.3. Managing Daily Tablespaces

This section covers:

- *Configuring Location of Files within File System (i. 4.3.1 on page 32).*
- *Indexing Data in Daily Tablespaces (i. 4.3.2 on page 32).*
- *Archiving Daily Tablespaces (i. 4.3.3 on page 34)*
- *Restoring Daily Tablespaces (i. 4.3.4 on page 35).*

- *Deleting Daily Tablespaces (i. 4.3.5 on page 36).*

4.3.1. Configuring Location of Files within File System

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

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

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

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

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

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

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

…

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

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

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

Warning!

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

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

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

Note:

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

4.3.2. Indexing Data in Daily Tablespaces

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

Note:

You can stop or launch the job manually, if necessary (see i. 4.1 on page 29).

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

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

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

20 minutes. At heavy load of the database this verification should be performed periodically, at intervals of several hours.

The change of indexing interval

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

To change the interval of indexing, run the script:

```
DECLARE
   v_start_date date;
   v_repeat_interval VARCHAR2(100);
BEGIN
   v_start_date := SYSDATE;
   v_repeat_interval := 'FREQ=MINUTELY; INTERVAL=10';
   dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
   dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
COMMIT;
END;
/
```

where:

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

Some examples of using the script are provided below.

Example 1. Reindexing starts once a minute

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

Example 2. Reindexing starts once every two hours

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

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

```
DECLARE
   v_start_date DATE;
```

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

4.3.3. Archiving Daily Tablespaces

Warning!

1. In addition to the regular way described, you can configure automatic backup of daily tablespaces using a special utility included in the distribution package of the System. For more details on using the utility, see Appendix A, page 78.
2. If the months or years are used as the time interval, it is recommended to use the maximum value of the interval in calculations. For a month - 31 days. For a year - 366 days. For example, to remove the daily TS older than 4 years specify the interval 366 * 4 = 1464 days in the job IWDROPAGE

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

Step 1. Selecting daily tablespaces and data files

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

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

Warning!

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

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

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

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

Note:

The full list of status codes and values is provided in table 3.

Step 2. Disconnecting Daily Tablespaces from the Database

> **Warning!**
>
> It is strongly recommended not to disable daily TS when the IWADDPARTS, IWDROP, IWREADIONLY jobs are running as it may cause the data loss.

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

```
BEGIN
   -- Procedure call
   part.part_disconnect(.tablespace_date., true);
COMMIT;
END;
/
```

where `.tablespace_date.` is a date of interception of objects stored in a tablespace. You can view this date by running a query for creating a list of daily TS which must be archived. For example, the procedure call for a daily TS storing the objects intercepted on February 3, 2012 appears as follows:

```
BEGIN
   -- Procedure call
   part.part_disconnect(TO_DATE('03.02.2012','dd.mm.yyyy'),
    true);
COMMIT;
END;
/
```

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

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

Step 3. Moving Datafiles

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

To get a list of data files for all disconnected tablespaces, run the query described in step 2.

4.3.4. Restoring Daily Tablespaces

> **Warning!**
>
> A tablespace can only be restored in the database schema, from which it was disconnected (even if this schema was updated). It is prohibited to reinstall database schema, from which the tablespace was turned off, as in this case you cannot restore the tablespace.

Step 1. Verifying permits for restoring data

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

Step 2. Moving data files

To restore a daily TS, you must move data files of this tablespace from a data carrier to the selected folder.

Step 3. Connecting the daily tablespace

> **Warning!**
>
> Do not connect daily TS during IWADDPARTS, IWDROP jobs. This may cause the data loss.

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

```
BEGIN
   part.part_restore(.tablespace_date., .path_to_the_datafile.);
COMMIT;
END;
```

```
/
```

> **Warning!**
>
> Data files must contain "/" in the beginning and in the end of their path.

If, for example, you need to connect daily TS which stores the objects intercepted on February 3, 2012, to the `/u01/oracle/data/` folder, call the following procedure:

```
BEGIN
   part.part_restore(to_date('03.02.2012','dd.mm.yyyy'), '/u01/oracle/data/');
COMMIT;
END;
/
```

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

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

4.3.5. Deleting Daily Tablespaces

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

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

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

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

> **Note:**
>
> If the archived daily TP can not be restored (because the information in it was removed from the database), then you can delete the data files of the daily TP from the archive.

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

Setting the interval of daily TS deletion

By default, IWDROP procedure performs deletion of all daily tablespaces created more than 100 days ago. To change this interval, run the following script under the account of the database schema owner:

```
BEGIN
   part.set_drop_part_date_lag('drop_interval');
COMMIT;
END;
/
```

where `drop_interval` is a number of days to pass from TS creation till TS deletion.

Enabling procedure autorun according to schedule

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

```
BEGIN
```

```
      dbms_scheduler.enable('IWDROP');
   COMMIT;
   END;
/
```

To disable procedure autorun, run the following script:

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

Manual run

If you need an immediate launch of procedure for deletion of daily TS (e.g., due to file system space shortage), see Appendix B, page 83 – deletion interval was changed, but the next launch of the job will not happen soon), run the following script:

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

4.4. Database Backup

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

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

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

This section further covers:

- *Creating Database Backup (i. 4.4.1 on page 37).*
- *Restoring the Database from the Backup (i. 4.4.2 on page 41).*

4.4.1. Creating Database Backup

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

- *Defining the Size of Backup (i. 4.4.1.1 on page 37);*
- *Checking the Backup Storage (i. 4.4.1.2 on page 38);*
- *Creating Backup Directories (i. 4.4.1.3 on page 38);*
- *Creating Recovery Aid Files (v4.4.1.4 on page 38);*
- *Collecting a List of Files to Backup (v 4.4.1.5 on page 39);*
- *Stopping IWTM System (v4.4.1.6 on page 40);*
- *Stopping Oracle Database (v4.4.1.7 on page 41);*
- *Copying database Files to the Backup Storage (i. 4.4.1.8 on page 41).*

4.4.1.1. Defining the Size of Backup

To define backup:

1. Log the computer that hosts database, as **oracle** user.

2. Open Oracle SQL*Plus and log as **sysdba**:

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

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

3. Wait for **Connected** message.
4. Copy (or enter) the following SQL queue to the command prompt:

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

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

   ```
   SQL> exit
   ```

4.4.1.2. Checking the Backup Storage

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

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

To define the hard disk free space

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

```
OS> df -h
```

Make shure this number is bigger than database size.

4.4.1.3. Creating Backup Directories

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

To create directory structure for backup:

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

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

3. Create subdirectories:

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

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

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

4.4.1.4. Creating Recovery Aid Files

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

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

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

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

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

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

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

   Wait for **Connected** message.
3. Copy (or enter) the following SQL queue to the command prompt:

   ```
   SQL> alter database backup controlfile to trace;
   ```
4. To find the directory in which the trace file was created, enter:

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

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

   Exit Oracle SQL*Plus:

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

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

   Press CTRL+C to exit view.
6. Create a copy of **spfile** (**pfile**):

   ```
   OS> sqlplus / as sysdba
   SQL> CREATE PFILE from SPFILE;
   ```
7. To find the directory in which the pfile file was created, enter:

   ```
   SQL> show parameter PFILE
   ```

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

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

   Exit Oracle SQL*Plus:

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

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

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

   ```
   controlfilebackupMMDDYY.trc
   ```

4.4.1.5. Collecting a List of Files to Backup

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

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

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

   Wait for **Connected** message.
3. Create the list of directories to backup using following SQL commands:

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

The output is like:

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

4. Exit Oracle SQL*Plus:

```
SQL> exit
```

4.4.1.6. Stopping IWTM System

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

To stop IWTM system:

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

```
OS> service iw-trafmon stop
OS> service iw-caserv stop
```

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

```
OS> service iw-trafmon start
OS> service iw-caserv start
```

4.4.1.7. Stopping Oracle Database

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

To stop Oracle database:

1. On the computer that hosts the database, log on as the ***oracle*** user.
2. In the command prompt, enter:

   ```
   OS> dbshut $ORACLE_HOME
   ```

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

   ```
   OS> dbstart $ORACLE_HOME
   ```

4.4.1.8. Copying database Files to the Backup Storage

1. Please make sure all Oracle services are stopped. If Oracle services are not stopped, backup files can be damaged and unusable for the restoring.
2. On the computer that hosts the database, copy directories (and their content) using previously created directories list (see i. 4.4.1.5 on page 39).

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

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

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

4.4.2. Restoring the Database from the Backup

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

- If the database was damaged due to system failure or user fault, restore old database. For example, if any essential file was occasionally deleted, you can restore the database to the state when this file existed: see i. 3.4.2.1 on page 35.
- If old database cannot be used any more, create a new one and recover data there: see i. 3.4.2.2 on page 35.

4.4.2.1. Restoring at the Same Database

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

To restore the database by creating a new one:

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

d. Rename **control01.ctl** file located in **/opt/IWTM_Backup_Files/Oradata/** directory to **control02.ctl** and copy it to **/u01/app/oracle/flash_recovery_area/iwtm/** directory

e. Check permissions.

If necessary change them:

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

4. Start database:

```
OS> dbstart $ORACLE_HOME
```

4.4.2.2. Restoring at the New Database

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

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

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

5. Generate spfile

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

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

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

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

CHAPTER 5. ADMINISTRATING THE SERVER END OF INFOWATCH TRAFFIC MONITOR

This chapter covers the following topics:

- *Traffic Monitor Server Processes (i. 5.1 on page 43)*
- *Configuring the Traffic Monitor Server Settings (tm.conf File) (i. 5.2 on page 47)*
- *Configuring OCR Usage for Interceptors (tm_ocr.conf File) (i. 5.3 on page 64)*
- *Configuring the Work with HTTP-Requests Transmitted by ICAP Protocol (icap.conf File) (i. 5.4 on page 65)*
- *Configuring the Processing of Attachments and Archives (detector.conf File) (i. 5.5 on page 66)*

5.1. Sample document database synchronization across multiple servers

> **Important!**
>
> Sample document database synchronization could be performed if you use two or more Traffic Monitor servers.

If there are two or more Traffic Monitor servers used in the System, there are different logics of sample document database updating could be used:

- *Master* server – main server, which updates the sample document database (executing **db_CA.pl** script). System can include only one *Master* server;
- *Slave* server – secondary server, which copying the *Master* server sample document fingerprints. *Slave* server works with sample document database by exchanging of service information, which confirms the sample document database settings relevance (executing the **db_CA_lite.pl** script). System can include one or more *Slave* server.

All servers in the system are configured to work as the main (*Master*) by default, so it is necessary to synchronize the sample document database across multiple servers.

To synchronize the sample document database across multiple servers:

1. Select which server will be used as the *Master*.

   > **Note:**
   >
   > Other server would be used as *Slave* servers.
   >
   > The choice of the server's working logic (*Master* or *Slave*) depends on the system administrator's preference and doesn't require steps of additional setting, except those specified in the subsection.

2. At *Slave* server (servers):
   a) Log in as **root**.
   b) In the **/etc/crontab** file delete the string

      ```
      * * * * * root /usr/local/infowatch/tm3/bin/scripts/db_CA.pl&>/dev/null
      ```

      Slave server would stop running the **db_CA.pl** script.

   c) Run the command:

      ```
      service crond restart
      ```

Scheduled tasks on a server would be updated.

3. At *Master* server:
   a) Log in as **root**.
   b) Run the command:

```
ssh-keygen
```

```
ssh-copy-id -i /root/.ssh/id_rsa <server_Slave>,
```

where `<server_Slave>` - IP-address of *Slave* server.

> **Important!**
>
> The `ssh-copy-id <server_Slave>` command must be executed for every *Slave* server using in the System.

   c) Run the command:

```
/usr/local/infowatch/tm3/bin/scripts/db_CA.pl
```

- *Configuring the Maximum Size of Added Sample Document (casdbcfg.conf file) (i. 5.7 on page 68)*
- *Configuring filtering rules for Sniffer (i. 5.9 on page 70)*
- *Management of Loading Objects to Remote Database (i. 5.10 on page 71)*
- *Archiving a Mail Queue Directory (i. 5.11 on page 74)*
- *Logging of System Work (i. 5.12 on page 74)*
- *Moving of Objects between Queues (iw_qtool Utility) (i. 5.13 on page 75)*
- *Loading an Object Queue (i. 5.14 on page 76)*
- *Recovering the System after Failures (i. 5.15 on page 77).*

5.2. Traffic Monitor Server Processes

This section covers:

- *List of Traffic Monitor Server Processes (i. 5.2.1 on page 43)*
- *Using Traffic Monitor Server Processes (i. 5.2.2 on page 45)*
- *Verification of the Results of Configuration Update (iw_updater Process) (i. 5.2.3 on page 46)*

5.2.1. List of Traffic Monitor Server Processes

Processes files are located at the following path:

```
/usr/local/infowatch/tm3/bin/process_name
```

Process name	Description of the process and path to the file
iw_smtpd	Process that received SMTP-messages. For integration with the Postfix mail server it receives incoming messages from Postfix. If there is no integration with Postfix, it receives the incoming mail from the corporate mail server or mail client (depending on the settings of your mail system). Receives incoming messages in SMTP format, converts SMTP envelope data to the XML context. Then it transfers SMTP-message and XML context to the **iw_messed** process.

Process name	Description of the process and path to the file
iw_messed	The process of processing SMTP-mails. Extracts data from an SMTP e-mail. Then extracted data is added to the XML context, received from **iw_smtpd**. The prepared XML context (containing the data extracted from the envelope and the e-mail) is transferred to the subsystem of analysis and decision making for analysis. After the analysis **iw_messed** transfers the allowed SMTP messages to the mail system component that delivers mail (only in the normal and transparent transport modes). For integration with Postfix mail server this component is Postfix. If there is no integration with Postfix, then the component depends on the settings configured in your mail system: it can be a corporate mail server or a mail client. Besides, a copy of screened SMTP message is delivered to the **iw_dbloader** daemon that saves is to the database.
iw_deliverd	Mails delivery process. Delivers SMTP e-mails to recipients, if the delivery of an e-mail is allowed from the Management Console (only in the normal and transparent transport modes). This process also delivers the SMTP-mails, that for any reason (e.g., due to absence of communication with the mail relay-server or mail client) were not delivered by the **iw_messed** process.
iw_expressd	Processing of objects obtained from the InfoWatch Device Monitor and DeviceLock systems. Upon receipt of the data (shadow copy of the file, print job) from InfoWatch Device Monitor or the shadow copy of the file from the DeviceLock Adapter it generates XML-context from the received object. Then, the XML context is sent to the subsystem of analysis and decision making. After the analysis a shadow copy of the file is transferred to the **iw_dbloader** daemon that saves it to the database.
iw_proxy	The process that receives a copy of the traffic (HTTP, ICQ, SMTP). To receive each type of traffic a separate copy of **iw_proxy** is launched. Receives an object (ICQ message, HTTP request, SMTP e-mail). Creates the XML context from the received object. Then, the XML context is sent to the subsystem of analysis and decision making. After the analysis a copy of the object is delivered to the **iw_dbloader** for stacking in a database.
iw_casd	The process of the Content Analysis subsystem. The **iw_casd** process receives plain text queries from the analysis and decision making subsystem for content analysis. When the analysis is completed, the query result is returned to the subsystem of analysis and decision making.
iw_updater	The process that loads a configuration from the database to the Traffic Monitor Server.
iw_dbloader	The process that loads objects into the database. Receives objects (verified by the analysis and decision making subsystem) from the **iw_messed, iw_expressd, iw_proxy processes**. Loads the delivered objects into the database.
iw_sniffer	The process that receives a copy of the traffic (HTTP, ICQ, SMTP).
iw_icap	The process of processing HTTP-traffic. Receives HTTP requests from the ICAP client. Extracts data from an HTTP requests. Then, the extracted data is added to the XML context. Then, the XML context is sent to the subsystem of analysis and decision making for analysis. When the analysis is finished it sends the response to the ICAP-client to allow/deny the delivery of the HTTP-request. It also transfers HTTP-request to **iw_dbloader** process that saves it to the database.
iw_qmover_client	It works on the Traffic Monitor Server, installed at a branch office. Sends intercepted objects to headquarter office database.
iw_qmover_server	It works on the Traffic Monitor Server, installed in the headquarters office. Receives objects from the client installed at the branch office. It also sends objects to the **iw_dbloader** process that saves it to the database.
iw_warpd	Manages the processes of retrieving data from archives, attached to the intercepted objects.

Process name	Description of the process and path to the file
iw_adlibitum	Manages the processes of receiving the relevant data from the Active Directory server.

5.2.2. Using Traffic Monitor Server Processes

All Traffic Monitor Server processes (except **iw_sniffer** and **iw_updater**) are run under the account of Traffic Monitor Server owner. The **iw_sniffer** and **iw_updater** are run under *root* user.

> **Note:**
>
> The owner of Traffic Monitor Server is specified in the `/usr/local/infowatch/tm3/etc/tm.conf` file, the `[GENERAL]` section, the `user` setting.

During the run-time Traffic Monitor Server processes status is checked by `iw-autorestart.sh` script added to the `/etc/crontab` file during installation. Once a minute **crond** daemon runs **iw-autorestart.sh** script. If for any reason one or more Traffic Monitor Server processes are stopped the `iw-autorestart.sh` script restarts them.

The Traffic Monitor Server processes are managed using `iw-trafmon` and `iw-caserv` files located in `/etc/rc.d/init.d` folder. `iw-trafmon` and `iw-caserv` files are autorun scripts for run levels 2, 3, 4, 5.

The `iw-trafmon` script is responsible for launching the following processes: **iw_smtpd**, **iw_messed**, **iw_expressd**, **iw_deliverd**, **iw_proxy**, **iw_dbloader**, **iw_updater**, **iw_sniffer, iw_icap, iw_qmover_server, iw_qmover_client, iw_warpd, iw_adlibitum**.

> **Notes:**
>
> 1. To intercept a copy of traffic using Sniffer (ICQ- HTTP-, SMTP-traffic) the separate **iw_proxy** processes are launched.
> 2. The **iw_icap** process is only available after installing ICAP integration module.
> 3. **The iw_qmover_server, iw_qmover_client** processes are only available after installation of remote database management module. Each process is launched on the respective end (in branches – **iw_qmover_client**, in headquarter office – **iw_qmover_server**).

The `iw-caserv` script is responsible for launching the CAS-related **iw_casd** process.

Start keys for `iw-trafmon` and `iw-caserv` scripts:

Start key	Purpose
`start`	run the processes
`stop`	stop the processes
`restart`	restart the processes
`status`	view the processes status

Examples of commands

Action	Command
Restart the Content Analysis subsystem processes	`service iw-caserv restart`
Verify the status for Traffic Monitor server processes	`service iw-trafmon status`
Verify the status of the Content Analysis subsystem processes	`service iw-caserv status`

Action	Command

Warning!

PID-files are stored in `/usr/local/infowatch/tm3/run` folder. If an error occurs, you must delete it all PID files before starting the processes.

Changing the settings of the autorun for the processes

For each process managed by `iw-trafmon` script, you can specify autorun settings in `/usr/local/infowatch/tm3/etc/tm.conf` file, `[AUTO_RESTART]` section.

Before changing the settings of the autorun process, stop the processes:

```
service iw-trafmon stop
```

For processes that must run automatically, enter the value:

```
autorestart = On
```

For other processes, enter the value:

```
autorestart = Off
```

After changing the autorun process, run:

```
service iw-trafmon start
```

Running of the processes manually

For Traffic Monitor Server processes to start correctly, the Oracle DBMS environment variables must be specified in advance (see *"InfoWatch Traffic Monitor. Installation and Configuration Guide"* document).

When started manually, all the processes (except **iw_proxy**) are running with `tm.conf` file settings:

```
/usr/local/infowatch/tm3/bin/process_name -c full_path_to_the_tm.conf_file
```

Example:

```
/usr/local/infowatch/tm3/bin/iw_dbloader -c /usr/local/infowatch/tm3/etc/tm.conf
```

For the iw_proxy process, it is necessary to specify the type of interceptor (icq, http, or smtp):

```
/usr/local/infowatch/tm3/bin/iw_proxy -with full_path_to_tm.conf –m interceptor_type
```

Example:

```
/usr/local/infowatch/tm3/bin/iw_proxy -with /usr/local/infowatch/tm3/etc/tm.conf –m icq
```

5.2.3. Verification of the Results of Configuration Update (iw_updater Process)

For the System to operate correctly, the same configuration must be loaded to all the instances of the Traffic Monitor Server. At the same time, a situation may occur when the configuration is not completely updated on one or several servers. In this case two versions with *Active* status will be displayed in Management Console, *Configuration versions* section, for a long period of time (over 15 min after update starts).

To solve this problem, take the following steps:

1. Ascertain the servers where an error has occurred. To do so, check the `/usr/local/infowatch/tm3/etc/tmserver_version.dat` file at each instance of the Traffic Monitor server.
2. Configuration version specified in this file must be the same as the loaded configuration version. If the versions differ, configuration was not updated on this server.

Note:

If the `tmserver_version.dat` file is absent, there's no previously loaded configuration on the server.

3. To check the `iw_updater`, process status run the following command:

   ```
   service iw-trafmon status
   ```

4. Do one of the following:

   If `iw_updater` is running, restart Traffic Monitor server processes:

   ```
   service iw-trafmon restart
   ```

   If `iw_updater` is stopped, run Traffic Monitor server processes:

   ```
   service iw-trafmon start
   ```

5. Load this configuration to servers once again (see "*InfoWatch Traffic Monitor*. *User Guide"*).

If the configuration loading error occurs again, check the system log /var/log/messages. If you cannot fix an error, then you must consult the customer support service.

5.3. Configuring the Traffic Monitor Server Settings (tm.conf File)

All Traffic Monitor Server components use the same `/usr/local/infowatch/tm3/etc/tm.conf` configuration file.

> **Warning!**
>
> The `tm.conf` configuration file contains a number of settings that you shouldn't change. The settings are not described in this document.
>
> Some settings contained in the configuration file are specified during installation of Traffic Monitor Server (see *"InfoWatch Traffic Monitor*. *Installation and Configuration Guide"* document).

Sections of the configuration file are described in the subsections:

- *The [GENERAL] Section (i. 5.3.1 on page 48).*
- *The [AUTO_RESTART] Section (i. 5.3.2 on page 48).*
- *The [SMTPD] Section (i. 5.3.3 on page 50).*
- *The [MESSED] Section (i. 5.3.4 on page 50).*
- *The [DELIVERD] Section (i. 5.3.5 on page 51).*
- *The [QUEUE] Section (i. 5.3.6 on page 51).*
- *The [SNIFFER] Section (i. 5.3.7 on page 52).*
- *The [HTTP] Section (i. 5.3.8 on page 52).*
- *The [ICQ] Section (i. 5.3.9 on page 53).*
- *The [SMTP] Section (i. 5.3.10 on page 54).*
- *The [PROXY] Section (i. 5.3.11 on page 54).*
- *The [PROXY_ICQ] Section (i. 5.3.12 on page 55).*
- *The [PROXY_HTTP] Section (i. 5.3.13 on page 55).*
- *The [PROXY_SMTP] Section (i. 5.3.14 on page 57).*
- *The [CAS] Section (i. 5.3.15 on page 58).*
- *The [ENCODE_DETECTOR] Section (i. 5.3.16 on page 60).*
- *The [DBLOADER] Section (i. 5.3.17 on page 60).*
- *The [FILTER] Section (i. 5.3.18 on page 61).*
- *The [ORACLE] Section (i. 5.3.19 on page 61).*
- *The [EXPRESSD] Section (i. 5.3.20 on page 61).*

- *The [EXTRACTOR] Section (i. 5.3.21 on page 62).*
- *The [UPDATER] Section (i. 5.3.22 on page 63).*
- *The [WARPD] Section (i. 5.3.23 on page 63).*
- *The [ADLIBITUM] Section (i. 5.3.24 on page 64).*

5.3.1. The [GENERAL] Section

The `[GENERAL]` section contains general settings:

Setting	Description
`User`	Name of the user who owns InfoWatch Traffic Monitor (account used to run the Traffic Monitor Server processes). The default value is `iwtm`. **Warning!** It is strongly recommended not to change the value of `User` setting, as it may cause System failure. If you do need to change the setting, reinstall the Traffic Monitor sever using the installer (see *«InfoWatch Traffic Monitor. Installation and Configuration Guide"* document).
`Group`	The group to which the owner of the Traffic Monitor belongs. The default value is `oinstall`
`Root`	The path to the System root directory. The default value is `/usr/local/infowatch/tm3`.
`VersionFile`	The path to a file containing information about the version of the configuration loaded on the Traffic Monitor server. The default value is `etc/tmserver_version.dat`
`UserScript`	Path to the script file specifying the object analysis and processing for the subsystem of analysis and decision making. The script is located in the directory `etc/scripts/user.lua` (the path is specified relative to the current directory - System root directory)
`ContextRules`	The path to the file containing the rules of message context change. Default value: `/etc/rules.xml`
`ContextCustomRules`	Path to the file containing rules of message context change. Default value: `etc/custom_rules.xml`
`SampleDocumentsSync`	Specifies whether this server compiles reference documents (running script `db_CA.pl`): `Off`/`On`. Default value: `Off`. `On` should be used on the only one System server.

5.3.2. The [AUTO_RESTART] Section

The `[AUTO_RESTART]` section contains settings necessary for processes autorun. The autorun is possible for the processes:

- iw_warpd
- iw_adlibitum;
- iw_sniffer;
- iw_messed;
- iw_deliverd;
- iw_smtpd;

- iw_expressd;
- iw_proxy ICQ;
- iw_proxy HTTP;
- iw_proxy SMTP;
- iw_dbloader,
- iw_updater;
- iw_icap;
- iw_qmover_client;
- iw_qmover_server.

Note:

The `iw_icap` process is only displayed in the autorun section when ICAP integration module is installed.

The `iw_qmover_server and iw_qmover_client` processes are only displayed in the autorun section if the remote database management module is installed. Moreover that process is displayed that corresponds to the module (client or server).

For every process there is the same set of settings:

Setting	Description
`autorestart`	Automatic control of process launching (`On` value). If no process launch management is required, set the value to `Off`.
`command`	The command for starting the process
`args`	Commands arguments

Rules of configuring the autorun settings:

Enable autorun for all processes that will operate on this instance of the Traffic Monitor server. For example, if you want to run the `iw_smtpd, iw_messed` and `iw_dbloader` processes, these processes must be configured to autorun (`autorestart` = `On`).

Note:

The initial configuration of the autostart of the processes is running when you install the Traffic Monitor Server. The list of processes that need to run varies depending on the implementation scheme. Basic implementation schemes, and lists the processes contained in document *"InfoWatch Traffic Monitor*. *Installation and Configuration Guide".*

Disable the autorun for the unlicensed processes that intercept traffic (iw_smtpd, iw_proxy, iw_expressd). It reduces the number of records in the log.

Warning!

Before changing autorun process settings, stop Traffic Monitor Server processes:

```
service iw-trafmon stop
```

This is necessary for the correct change of the settings.

5.3.3. The [SMTPD] Section

The `[SMTPD]` section contains settings for configuring the **`iw_smtpd`** process (interception of SMTP-traffic from mail relay-server):

Setting	Description
`Daemon`	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On.
`LogLevel`	Logging level. `0(`only errors are logged`)` - 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
`MaxThreads`	Maximum number of threads for parallel running of the **iw_smtpd** process. Default value if 8. Increasing the number of threads improves process performance but also increases memory consumption.
`MaxMsgSize`	Maximum e-mail message size (in bytes). The default value is 10240000.
`Domain`	Full domain name of the host SMTP-server used for identification within the mail protocol. It is advisable to use the name of TM server where **iw_smtpd** process is running.
`CoreDumpSize`	Memory dump size (in bytes). The setting is used to debug errors. The recommended value is `-1` (the memory dump size is not limited). The value `0` indicates that logging is disabled. The default value is -1.
`ListenAddr`	Address of the server network interface where the listening process is running. Specified when installing.
`ListenPort`	Server port where the listening process is running. Specified when installing.

5.3.4. The [MESSED] Section

The `[MESSED]` section contains settings for **`iw_messed`** process (delivery of SMTP-mails when integrating with mail relay-server):

Setting	Description
`Daemon`	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On.
`LogLevel`	Logging level: `0(`only errors are logged`)`- 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
`MaxThreads`	Maximum number of threads for parallel running of the **iw_messed** process. Default value if 8. Increasing the number of threads improves process performance but also increases memory consumption.
`CoreDumpSize`	Memory dump size (in bytes). The setting is used to debug errors. The recommended value is `-1` (the memory dump size is not limited). The value `0` indicates that logging is disabled. The default value is -1.
`Relay`	Full domain name of the mail relay-server that the letter is forwarded to, used for identification within mail protocol. Specified when installing.
`RelayPort`	The port of mail relay-server that the letter is forwarded to. Specified at installation.
`HeloDomain`	Value of the `HELLO` command in SMTP dialog. The default value is `smtp.company.com`.

Setting	Description
Timeout	Time during which the attempts to deliver SMTP-mails are being made in seconds. After this time, a letter is transmitted to the database. The default value is 1200.
OCR	Idle setting. Configuring of text recognition in raster images (OCR) for SMTP objects is performed in tm_ocr.conf file (see i. 5.4 on page 64). Details on OCR are described in the *«InfoWatch OCR for IWTM 4.1. Installation Guide»* document.

5.3.5. The [DELIVERD] Section

The [DELIVERD] section contains settings for the **iw_deliverd** process (delivery of SMTP-mails to recipients when integrating with mail relay-server):

Setting	Description
Daemon	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On.
LogLevel	Logging level: 0(only errors are logged)- 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
MaxRetries	Maximum number of retries to deliver an e-mail message. The default value is 3.
RetryTimeout	Timeout (in seconds) between message delivery attempts (the default value is 10)
CoreDumpSize	Memory dump size (in bytes). The setting is used to debug errors. The recommended value is -1 (the memory dump size is not limited). The value 0 indicates that logging is disabled. The default value is -1.
CheckPeriod	Timeout interval (in seconds) between checking for new mail. The default value is 5.
HeloDomain	Value of the HELLO command in SMTP dialog. The default value is smtp.company.com.
Relay	Full domain name of the mail relay-server, used for identification within mail protocol. Specified at installation. It is recommended to use the name of TM server where the **iw_deliverd** process is running.
RelayPort	Port of the mail relay server. Specified at installation.
Timeout	Time during which the attempts to deliver SMTP-mails are being made in seconds. The default value is 1200.

5.3.6. The [QUEUE] Section

The [QUEUE] section contains object queue settings:

Setting	Description
Db	The path to queue of objects loaded into the database; the queue is used by *iw_dbloader* process. The default value is *./queue/db* (the path is specified relative to the current directory, which is the System root directory).
Smtp	The path to the queue of SMTP mails, used by the *iw_smtpd* and *iw_messed* processes. The default value is *./queue/smtp* (the path is specified relative to the current directory, which is the System root directory).

Setting	Description
Error	The path to the queue of objects that were not processed due to an error disabling further processing. This queue consists of the objects with errors occurred when the processes if the Traffic Monitor Server received them or when the objects were loaded to the database. The default value is ./queue/error (the path is specified relative to the current directory, which is the System root directory).
CheckPeriod	Waiting interval (in milliseconds) between checking for new e-mails in the queue of incoming SMTP messages. The default value is 1000.

5.3.7. The [SNIFFER] Section

The [SNIFFER] section contains settings of the **iw_sniffer** process:

Setting	Description
Daemon	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On.
LogLevel	Logging level: 0(only errors are logged)- 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
Host	IP-address of the host waiting for the proxy connection
Port	Port of the host waiting for the proxy connection
Clusters	List of interceptor types described in the following sections. Default value: http,icq,smtp
LibraryPath	The path to the dynamic libraries of interception. The default value is /usr/local/infowatch/tm3/lib
InterceptorLib	Path to the library of the interceptor. The default value is libtmcap_interceptor.so

5.3.8. The [HTTP] Section

[HTTP] section specifies settings of intercepting http-traffic using Sniffer:

Setting	Description
Interface	Network interface that will be sending the copies of the messages. You can specify one of the following values: eth0, eth1, etc. The default value is eth0. **Note:** receiving different types of traffic from one network interface is allowed
OpenTimeout	Time to keep connection alive (in seconds) if no packages are transmitted. Default value is 600.
LiveTimeout	Timeout (in seconds) when the connection status will be changed to ESTABLISHED. If the status is not changed, connection will be automatically terminated. The default value is 86400.
CloseTimeout	Time to keep the connection alive (in seconds) when the status is changed to *TIME_WAIT.* The default value is 300.
QueueMemorySize	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 default value is 4194304.

Setting	Description
Balancer	Balancing type (distribution of traffic between multiple instances of the Traffic Monitor Server). Possible values: • Connection. An instance of Traffic Monitor Server is selected for each new TCP connection. Thus all instances of the Traffic Monitor Server are used by turn. • SrcIp. Traffic is distributed between multiple instances of Traffic Monitor Server based on client IP address. This means that all the data received from the same IP address of the client will be delivered to the same instance of the Traffic Monitor Server. The default value is SrcIp
RulesTableFile	Path to file where http-traffic sniffer filtering settings are specified (for more details, see i. 5.9 on page 70). The default value is /etc/http.rules

5.3.9. The [ICQ] Section

[ICQ] section specifies settings of intercepting ICQ-traffic using Sniffer:

Setting	Description
Interface	Network interface that will be sending the copies of the messages. You can specify one of the following values: eth0, eth1, etc. The default value is eth0. **Note:** receiving different types of traffic from one network interface is allowed
OpenTimeout	Time to keep connection alive (in seconds) if no packages are transmitted. Default value is 600.
LiveTimeout	Timeout (in seconds) when the connection status will be changed to ESTABLISHED. If the status is not changed, connection will be automatically terminated. The default value is 86400.
CloseTimeout	Time to keep the connection alive (in seconds) when the status is changed to *TIME_WAIT.* The default value is 300.
QueueMemorySize	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 default value is 4194304.
Balancer	Balancing type (distribution of traffic between multiple instances of the Traffic Monitor Server). Possible values: • Connection. An instance of Traffic Monitor Server is selected for each new TCP connection. Thus all instances of the Traffic Monitor Server are used by turn. • SrcIp. Traffic is distributed between multiple instances of Traffic Monitor Server based on client IP address. This means that all the data received from the same IP address of the client will be delivered to the same instance of the Traffic Monitor Server. The default value is SrcIp
RulesTableFile	Path to file where icq-traffic sniffer filtering settings are specified (for more details, see i. 5.9 on page 70). The default value is /etc/icq.rules

5.3.10. The [SMTP] Section

[SMTP] section specifies settings of intercepting http-traffic using sniffer^

Setting	Description
`Interface`	Network interface that will be sending the copies of the messages. You can specify one of the following values: eth0, eth1, etc. The default value is eth0. **Note:** receiving different types of traffic from one network interface is allowed
`OpenTimeout`	Time to keep connection alive (in seconds) if no packages are transmitted. Default value is 600.
`LiveTimeout`	Timeout (in seconds) when the connection status will be changed to ESTABLISHED. If the status is not changed, connection will be automatically terminated. The default value is 86400.
`CloseTimeout`	Time to keep the connection alive (in seconds) when the status is changed to *TIME_WAIT.* The default value is 300.
`QueueMemorySize`	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 default value is 4194304.
`Balancer`	Balancing type (distribution of traffic between multiple instances of the Traffic Monitor Server). Possible values: • `Connection`. An instance of Traffic Monitor Server is selected for each new TCP connection. Thus all instances of the Traffic Monitor Server are used by turn. • `SrcIp`. Traffic is distributed between multiple instances of Traffic Monitor Server based on client IP address. This means that all the data received from the same IP address of the client will be delivered to the same instance of the Traffic Monitor Server. The default value is `Connection`.
`RulesTableFile`	Path to file where smtp-traffic sniffer filtering settings are specified (for more details, see i. 5.9 on page 70). The default value is `/etc/smtp.rules`

5.3.11. The [PROXY] Section

The `[PROXY]` section contains general settings of **`iw_proxy`** process:

Setting	Description
`Daemon`	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On.
`LogLevel`	Logging level: `0`(only errors are logged)- 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
`CoreDumpSize`	Memory dump size (in bytes). The setting is used to debug errors. The recommended value is `-1` (the memory dump size is not limited). The value `0` indicates that logging is disabled. The default value is -1.
`MaxThreads`	Maximum number of threads for parallel running of the **iw_proxy** process. Default value if 32. Increasing the number of threads improves process performance but also increases memory consumption.

Setting	Description
MaxFiles	The number of opened files. The default value is 0 – in this case, the value specified in the operating system settings is used (the default is 1024). To improve the performance for a large volume of traffic you can increase this value. When you change the setting you need to set a value greater than the system. For high-loaded systems we recommend using the value 8000.
Module	Interceptor type (icq, http or smtp). The default value is not specified (void)

5.3.12. The [PROXY_ICQ] Section

The [PROXY_ICQ] section contains settings for processing copies of ICQ messages, received from Sniffer:

Setting	Description
MessageWindow	The number of dialogue messages, at which the ICQ-dialog is saved in a file queue. The default value is 10.
ListenPort	The server port to which the messages are sent. The default value is 5191.
DialogTimeout	Time interval (in minutes), after which the expiration and from the moment of the last interception of ICQ-message you need to save the dialog to the file queue. The default value is 5.
DialogBytesCount	The size of the dialog (in bytes), at which the ICQ-dialog is saved in a file queue. The default value is 500.
FakeFileTransferPort	The port, which blocks the attempts to transfer files after redirection to it. The default value is 62225.
DataPoolPageCount	Maximum number of data pages (4 Kb) for connection processing. The default value is 65536.

Settings necessary for receiving data from Sniffer:

Setting	Description
SnifferClusterID	The ID of the cluster in which this instance of the Traffic Monitor Server will be included. This setting is specified as a string. For example, icq
SnifferHost	IP-address of Traffic Monitor Server instance, where **iw_sniffer** process is running
SnifferPort	The port used by iw_sniffer process to receive incoming connections

5.3.13. The [PROXY_HTTP] Section

The [PROXY_HTTP] contains settings required for processing HTTP-requests, as well as ICQ-messages (when intercepting ICQ over HTTP), received from Sniffer:

Setting	Description
MinText	Minimum volume of text (in bytes) that will have its contents analyzed. The default value is 10 bytes. Configuring this setting can reduce load to CAS. This can be achieved by skipping content analysis of the text that is small enough to transmit meaningful messages.

Setting	Description
MinHeader	The minimum volume of text (in bytes) for one block of variable in the URL encoding, which will be forwarded to the content analysis server. Default value is 10.
SetCp1251	Using windows 1251 charset instead of mac-cyrillic when the text encoding in HTTP request is identified automatically. The default value is On. If your software supports windows-1251 charset, it is recommended to keep the setting enabled (On value). The charset may be identified incorrectly. Specifically when Cyrillic text volume is rather small, the mac-cyrillic charset may be selected in place of windows-1251.
SkipNegotiate	Disables the saving of HTTP-requests with NTLM Type 1 to the queue (necessary to eliminate duplicate queries). The default value is On. While implementing scheme of implementation, when HTTP-traffic copy is intercepted via Sniffer, it must take the Off value.
MaxMemoryBlock	The maximum amount of POST-query (in kilobytes) that can be stored in memory. Blocks of a larger size will be loaded into temporary files. The default value is 4096.
LogBlock	A record in the system log of messages about blocking the intercepted HTTP-requests. The logging is enabled if the value On is specified. The logging is disabled by default – Off value
CharsetDetection	Method of determining the encoding of the text. Default value is 0. In this case, the encoding is determined by the usual method. After extraction in the context, the texts of some POST-queries may be displayed incorrectly. To fix this problem you can set value to 1
StatusCheck	Setting the delivery status of HTTP-request (displayed in the Management Console), depending on the status code returned by a web or proxy server. If the value is set to On code analysis is performed, which enables a more accurate display of the delivery status for HTTP-request. The default value is On.
AuthContext	Disables the saving in queue the HTTP-requests without authentication. Possible values: • 0 – saves your queries without authentication; • 1 – queries with proxy response "407" are not saved, • 2 – queries with NTLM Type 1, or without the *Proxy-Authorization* header are not saved. In this case the SkipNegotiate setting has no value set: The system functions as if the value was set to On. The default value is 2.
SkipStat4XX	Disables saving HTTP-requests to HTTP-queue with proxy response in *"4XX"* format, where *XX* – any numbers. The default value is On.
IcqFilter	Ability to intercept ICQ-messages (if the value On is enabled), sent via proxy (over HTTP). By default the function is disabled – the value is set to On
IcqKnownServers	IP ranges for ICQ servers when intercepting the ICQ over HTTP. Several ranges are listed, separated by commas, for example: "205.188.251.0/24:443, 64.12.30.0/24:443, 205.188.8.8:443"
MessageWindow	The number of dialogue messages, at which the ICQ-dialog is saved in a (when intercepting the ICQ over the HTTP) file queue. The default value is 10.

Setting	Description
DecodeHttpContent	Enabling the unpacking of query contents where Content-Encoding header is present with gzip, deflate or compress value. The default value is On
ExtractHttpEntity	Enabling the procedure of extracting text from the encoded content of the query by external unpackers. This procedure applies in case of failures of internal decoding procedure using zlib. The default value is Off
DialogTimeout	Time interval (in minutes), after which expiration and from the moment of the last interception of message you need to save the ICQ-dialog to the file queue (when intercepting ICQ over HTTP). The default value is 5.
DialogBytesCount	The size of dialogue (in bytes), at which the ICQ-dialog is saved in a (when intercepting the ICQ over the HTTP) file queue. The default value is 500.
FakeFileTransferPort	The port, which blocks the attempts to transfer files after redirection to it. The default value is 62225.
DataPoolPageCount	Maximum number of data pages (4 Kb) for connection processing. The default value is 65536.
WCGAuthCache	Indicates whether authorization data caching feature required for WebSense WSG integration is included. To enable caching set the value to On. The default value is Off
WCGAuthTTL	Authorization information caching time if WCGAuthCache (in sec) setting is enabled. The default value is 900.

Settings necessary for receiving data from Sniffer:

Setting	Description
SnifferClusterID	The ID of the cluster in which this instance of the Traffic Monitor Server will be included. This setting is specified as a string. For example, http
SnifferHost	IP-address of Traffic Monitor Server instance, where **iw_sniffer** process is running
SnifferPort	The port used by iw_sniffer process to receive incoming connections

5.3.14. The [PROXY_SMTP] Section

The [PROXY_SMTP] section contains settings for processing SMTP messages, received from Sniffer:

Setting	Description
MaxMsgSize	The size of SMTP-message (in bytes) above which the message is not processed by the System. The default value is 52428800.
DataPoolPageCount	Maximum number of data pages (4 Kb) for connection processing. The default value is 65536.

Settings necessary for receiving data from Sniffer:

Setting	Description
SnifferClusterID	The ID of the cluster in which this instance of the Traffic Monitor Server will be included. This setting is specified as a string. For example, smtp

Setting	Description
SnifferHost	IP-address of Traffic Monitor Server instance, where **iw_sniffer** process is running
SnifferPort	The port used by iw_sniffer process to receive incoming connections

5.3.15. The [CAS] Section

The [CAS] section contains settings:

Setting	Description
Daemon	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On
LogLevel	Logging level: 0 (only errors are logged) - 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
SocketBacklog	The maximum number of processes which could be contained in the processing queue. Default value is 32.
CoreDumpSize	Memory dump size (in bytes). The setting is used to debug errors. The recommended value is -1 (the memory dump size is not limited). The value 0 indicates that logging is disabled. The default value is -1.
ListenAddr	Address of the network interface of content analysis server, on which the process of listening to requests for text processing, coming from the subsystem analysis and decision making, has started. The default value is 127.0.0.1.
ListenPort	Port of the content analysis server where the listening process is running. The default value is 4201.
BaseVerFile	Path to the file containing configuration data currently used by CAS. The default value is etc/cas_version.dat (path is specified relative to the current directory, which is the System root directory).
LangDetOntoloy	Path to the classification ontology file. The default value is cas/lang.ont.bin

Linguistic analysis technology settings (*Classifier*):

Setting	Description
CLLib	Path to linguistic analysis library. Default value is lib/libclassifier.so
CLSrcXmlBase	Path to the XML database. The default value is cas/base.xml
CLSearchLimit	Maximum number of terms that are returned in search result. 0 - disable; -1 - no limits for number of returned terms. Default value is 10.
CLNiokrOntologyPrefix	File prefixes in classification ontology. The default value is cas/onto.
CLSpellingCorrector	Enabling (On) or disabling (Off) of detecting the terms which in the intercepted text have any errors or misprints: differences to one symbol with the term are detected (substitution, shift, absence, excess symbol). The function is enabled by default (On)
CLTransliteration	Enabling (On) or disabling (Off) of detecting the transliterated terms. By default the text normalization is provided according to transliteration rules (On)

Setting	Description
CLTransliterationTable	Path to the transliteration table, according to which the text normalization is provided; default value and a file itself shouldn't be changed.

The settings of digital fingerprints technology (*Copyright Analysis*):

Setting	Description
CALib	Path to the digital fingerprints library. The default value is lib/libch_copyanalysis.so
CADB	Path to the digital fingerprints library database. The default value is cas/ca_db.
CATempDB	Path to the temporary digital fingerprints database. The default value is cas/ca_temp_db
CASearchLimit	Maximum number of terms that are returned in search result. 0 - disable; -1 - no limits for number of returned terms. Default value is 10.
CARelLimit	Relevance threshold: percent of coincidence of text data from analyzed object with reference document, sufficient to consider the object as coincident with this reference document. Valid values - from 0 to 100. Default value is 10.
CABinRelLimit	Relevance threshold: percent of coincidence of binary data from analyzed object with reference document, sufficient to consider the object as coincident with this reference document. Valid values - from 0 to 100. Default value is 10.
CABinLMin	Minimal length of binary data fragment for which the digital fingerprints detection can actuate. Default value is 23.
CABinLMax	Maximum length of binary data fragment for which the digital fingerprints detection can actuate. Default value is 111.
CAMinTextSize	Minimal text quantify of text which can be used for creating text digital fingerprint, in bytes. Default value is 100 bytes.
IMEnabled	Enabling (value On) or disabling (value Off) the stamp detection. Default value is Off.

Settings of the text objects detection technology:

Setting	Description
TOSearchLimit	Maximum number of terms that are returned in search result. 0 - disable; -1 - no limits for number of returned terms. The default value is 10.
TONiokrSrcActiveList	Path to the file containing list of active text objects.
TOUsrObjs	Path to the file containing list of user text objects.
TOLib	Path to the library of text objects. The default value is lib/libch_tobjdetector.so
TOPhoneCountryCodes	Path to the file containing a list of telephone area codes for various countries. The default value is cas/do_phone_country.txt
TOPhoneCityCodes	Path to the file containing a list of telephone area codes for various cities. The default value is cas/do_phone_city.txt
TOSkillaObjects	Path to the folder containing links to destinations of compiled text objects

Setting	Description
TOSkillaSource	Path to the folder containing links to destinations of source text objects
TOAllSource	Path to the folder containing links to destinations of all source text objects, including user ones
TOAllObjects	Path to the folder containing links to destinations of all compiled text objects, including user ones
ICEnabled	Enabling (value On) or disabling (value Off) the Russian ID detection. Default value is Off.
FAEnabled	Enabling (value On) or disabling (value Off) the filled forms detection. Default value is Off.
TAEnabled	Enabling (value On) or disabling (value Off) the DB uploading detection. Default value is Off.

5.3.16. The [ENCODE_DETECTOR] Section

The [ENCODE_DETECTOR] section contains settings used to define the encoding of the text

Setting	Description
NIOKR	The choice of the InfoWatch encoding detector instead of the Mozilla detector. The On value means usage of InfoWatch technology; Off – Mozilla. The default value is Off

5.3.17. The [DBLOADER] Section

The [DBLOADER] section contains settings used to configure **iw_dbloader** daemon:

Setting	Description
Daemon	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On
LogLevel	Logging level: 0(only errors are logged)- 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
CoreDumpSize	Memory dump size (in bytes). The setting is used to debug errors. The recommended value is -1 (the memory dump size is not limited). The value 0 indicates that logging is disabled. The default value is -1.
MaxThreads	Maximum number of threads for parallel running of the **iw_dbloader** process. Default value if 8. Increasing the number of threads improves process performance but also increases memory consumption.
CacheSize	Number of DB object IDs to cache (in one process copy) Default value is 32.
XMLValidityCheck	Setting that determines the need to verify the formation of context: Yes – verification is enabled; No – verification is disabled. The default value is No.
XMLSchemaFile	The path to the file with the rules of forming the context. The default value is etc/message.xsd

Setting	Description
MaxTextinContext	Maximum number of texts in one object. If texts number exceeds setting value, object is not saved in the database but transferred to the error queue. The default value is 65535.

5.3.18. The [FILTER] Section

The [FILTER] section contains general settings of Content Analysis subsystem:

Setting	Description
Server	Address of the network interface, which connects all processes working with content analysis server. The default value is 127.0.0.1.
Port	Port, which connects all processes, working with content analysis server. The default value is 4201.

5.3.19. The [ORACLE] Section

The [ORACLE] section contains settings used to connect with database server:

Setting	Description
Username	The name of the Linux user account
Password	The password of the Linux user account
Connstr	String for connecting to the database server (server alias from the tnsnames.ora file).

5.3.20. The [EXPRESSD] Section

The [EXPRESSD] section contains settings for **iw_expressd** process:

Setting	Description
Daemon	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On
LogLevel	Logging level: 0 (only errors are logged) - 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
CoreDumpSize	Size of the memory dump (in bytes). The setting is used to debug errors. The recommended value is -1 (the memory dump size is not limited). The value 0 indicates that logging is disabled. The default value is -1.

Setting	Description
MaxThreads	Maximum number of threads for parallel running of the **iw_expressd** process. Default value if 4. Increasing the number of threads improves process but also increases memory consumption. **Warning!** For correct reception of objects from InfoWatch Device Monitor and DeviceLock systems, specify the same number of processing threads set on InfoWatch Device Monitor server (or in DeviceLock Adapter settings). NumberOfConnections setting in InfoWatch.DeviceMonitor.Server.exe.config and InfoWatch.DeviceLockAdapter.exe.config configuration files respectively, is responsible for setting the number of processing threads for InfoWatch Device Monitor and DeviceLock Adapter (for more details see "*InfoWatch Device Monitor. Installation and Configuration Guide"* and *"InfoWatch DeviceLock Adapter. Administration Guide"*).
ListenAddr	Address of the network interface of the server on which the process of listening to objects received from the systems InfoWatch Device Monitor and DeviceLock is running. The default value is 0.0.0.0.
ListenPort	Server port where the listening process is running. The default value is 4101.
MaxLoadAvg	Maximum load to the system where the **iw_expressd** process is running (threshold value specified in nominal units). If the system load equals or exceeds the specified threshold value the **iw_smtpd** daemon stops receiving messages. When the load to the system decreases, e-mails will be received again. The default value is 10.
CheckPrintMonitor	Enabling (**On** value) or disabling (**Off** value) the text extraction from print job shadow copies obtained from Device Monitor. Default value is **Off**. **Warning!** When integrated with InfoWatch Device Monitor 3.4, and 4.0 in case of OCR extractors usage, you should specify **CheckPrintMonitor = On**. When integrated with Infowatch Device Monitor 4.0 without OCR extractors you should specify **CheckPrintMonitor = Off**.
OCR	Configuring of text recognition in raster images (OCR) is performed in tm_ocr.conf file (see i. 5.4 on page 64). Details on OCR are described in the *«InfoWatch OCR for IWTM 4.1. Installation Guide*» document. **Warning!** If OCR = Off then TXT files are forwarded directly to the content analysis. This variant is suitable if OCR extractors are not used or you need to reduce Traffic Monitor server loading.
DmOCR, DlaOCR, CrawlerOCR, SkypeOCR, XmppOCR, MmpOCR, FtpOCR	Configuring of text recognition in raster images (OCR) for different types of interceptors is performed in tm_ocr.conf file (see i. 5.4 on page 64). Details on OCR are described in the *«InfoWatch OCR for IWTM 4.1. Installation Guide*» document.

5.3.21. The [EXTRACTOR] Section

The [EXTRACTOR] section contains settings used to extract files from archives and attachments:

Setting	Description
DetectorPath	Path to the file containing the database of signatures that are needed to specify the attachment and archive types. The default value is etc/detector.conf (path is specified relative to the current directory, which is the System root directory)
PrintDetectorPath	Path to the file containing Print Monitor extractors settings for expressd. The default value is etc/detector_prn.conf (path is specified relative to the current directory, which is the System root directory)

Setting	Description
TempDir	Path to the directory that temporarily stores the extracted files. The default value is tmp (path is specified relative to the current directory, which is the System root directory).

5.3.22. The [UPDATER] Section

The [UPDATER] section contains settings required to load configuration from the database to Traffic Monitor Server:

Setting	Description
Daemon	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On
LogLevel	Logging level: 0 (only errors are logged) - 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
CoreDumpSize	Memory dump size (in bytes). The setting is used to debug errors. The recommended value is -1 (the memory dump size is not limited). The value 0 indicates that logging is disabled. The default value is -1.
cas_script	Path to the script file defining restart of content analysis services. The script is located in etc/cas_reload.sh folder (path is specified relative to the current directory, which is the System root directory)
tmserver_script	Path to the script file defining restart of all TM server services except content analysis & Active Directory synchronization services. The script is located in etc/tmserver_reload.sh folder (path is specified relative to the current directory, which is the System root directory)
activedirectory_script	Path to the script file defining restart of Active Directory synchronization services. The script is located in etc/tmserver_reload.sh folder (path is specified relative to the current directory, which is the System root directory)

5.3.23. The [WARPD] Section

The [WARPD] section contains settings of processes of retrieving data from archives, attached to the intercepted objects:

Setting	Description
Daemon	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On
LogLevel	Logging level: 0 (only errors are logged) - 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
CoreDumpSize	Memory dump size (in bytes). The setting is used to debug errors. The recommended value is -1 (the memory dump size is not limited). The value 0 indicates that logging is disabled. The default value is -1.
MaxThreads	Maximum number of threads for parallel process running. Default value if 1. Increasing the number of threads improves process performance but also increases memory consumption.

5.3.24. The [ADLIBITUM] Section

The [ADLIBITUM] section contains settings of the processes of retrieving relevant data from the Active Directory:

Setting	Description
Daemon	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On
LogLevel	Logging level: 0(only errors are logged) - 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
ErrorDelay	The delay time after an unsuccessful attempt of synchronization until the next synchronization attempt, in seconds.

5.4. Configuring OCR Usage for Interceptors (tm_ocr.conf File)

The tm_ocr.conf configuration file located in the /usr/local/infowatch/tm3/etc/ directory defines the operation of text recognition in bitmap images (OCR) for different interceptors. If in link to the tm_ocr.conf is specified for necessary processes (iw_messed and iw_expressd and iw_warpd) in the tm.conf configuration file (see more info in i. 5.3.2 on page 48), then during processing the intercepted images the settings from tm_ocr.conf file will be applied instead of analogous parameters from tm.conf file.

The detailed information on the procedure of OCR installation and configuration see in the *«InfoWatch OCR for IWTM 4.1. Installation Guide*» document.

5.4.1. The [*MESSED*] Section

The [MESSED] section of tm_ocr.conf file contains the OCR setting which is used for enabling (On value) or disabling (Off value) OCR usage for files received from SMTP Monitor. The default value is On.

5.4.2. The [*EXPRESSD*] Section

The [MESSED] section of tm_ocr.conf file defines if monitors will use OCR or not. The default value for all settings except CheckPrintMonitor and OCR is Off. To enable OCR usage for files received from certain interceptor, change the value of the corresponding setting to On.

Setting	Description
CheckPrintMonitor	Using OCR for files received from Print Monitor. **Warning!** If the system is integrated with Infowatch Device Monitor version 3.4 then you need to specify CheckPrintMonitor = On regardless of OCR usage.
OCR	Using OCR for files received from Print Monitor. Depending on used InfoWatch Device Monitor version, the Print Monitor interceptor can transfer print jobs either in TXT format (text extraction is performed by means of Device Monitor) or in PDF format or both files (TXT + PDF). In first two cases the OCR setting value do not influence to the system operation.

	Warning! If `OCR = Off` then TXT files are forwarded directly to the content analysis. This is recommended to decrease Traffic Monitor server loading
`DmOCR`	Using OCR for files received from Device Monitor
`DlaOCR`	Using OCR for files received from DeviceLock Adapter
`CrawlerOCR`	Using OCR for files received from Crawler interceptor
`SkypeOCR`	Using OCR for files received from Skype Monitor
`XmppOCR`	Using OCR for files received from XMPP Monitor
`MmpOCR`	Using OCR for files received from MMP Monitor
`FtpOCR`	Using OCR for files received from FTP Monitor

5.4.3. The [*EXTRACTOR*] Section

The `[EXTRACTOR]` section of `tm_ocr.conf` file defines settings used for file extraction from archives and attaches:

Setting	Description
`DetectorPath`	Path to the file containing the database of signatures that are needed to specify the attachment and archive types. The default value is `etc/detector_ocr.conf` (path is specified relative to the current directory, which is the System root directory) Configuring of this file is described in the *«InfoWatch OCR for IWTM 4.1. Installation Guide»* document
`TempDir`	Path to the directory that temporarily stores the extracted files. The default value is `tmp` (path is specified relative to the current directory, which is the System root directory).

5.5. Configuring the Work with HTTP-Requests Transmitted by ICAP Protocol (icap.conf File)

> **Note:**
>
> The `icap.conf` file is only created after installation of ICAP integration module.

The settings for interaction with ICAP server are configured in `/usr/local/infowatch/tm3/etc/icap.conf` file, `[ICAP]` section:

Setting	The description and examples of configuring
`Daemon`	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On
`LogLevel`	Logging level. `0` (only errors are logged) - 8 for debug information. Corresponds to the syslog logging level. Default value is 3.
`CoreDumpSize`	Memory dump size (in bytes). The setting is used to debug errors. The recommended value is `-1` (the memory dump size is not limited). The value `0` indicates that logging is disabled. The default value is -1.

Setting	The description and examples of configuring
MaxFiles	The number of opened files. The default value is 0 – in this case, the value specified in the operating system settings is used (the default is 1024). To improve the performance for a large volume of traffic you can increase this value. When you change the setting you need to set a value greater than the system. For high-loaded systems we recommend using the value 8000.
ListenPort	Port on which the ICAP-server listens the HTTP-requests from the proxy server with ICAP-client. You can use the ports with numbers starting from 1025. Default value is 1344
PathTemporary	Path to the temporary file storage of ICAP-server (default value is /usr/local/infowatch/tm3/temp/icap)
error_html	Path to the HTML file that contains the message displayed in the web browser window if the user query was blocked by the System. The default value is etc/error.html (path is specified relative to the current directory, which is the System root directory).
min_text_length	Minimal size of text (in bytes) that will have its contents analyzed. The default value is 5 bytes. Configuring this setting can reduce load to CAS. This can be achieved by skipping content analysis of the text that is small enough to transmit meaningful messages.
min_data_length	Minimal size (in bytes) of url-encoded variable that will be included into the text block to be sent to CAS for analysis. The default value is 10 bytes.
LogBlock	Logging level setting value at least 4 (LogLevel=4). A record in the system log of messages about blocking the intercepted HTTP-requests. The default value is 0: logging is disabled
LogTimer	A record in the system log of messages about the time for processing the HTTP-requests. The logging is enabled, when the value is set to 1. Default value is 0 – logging is disabled.
disable_ipv6	Disabling (disable_ipv6 = 1) end enabling (disable_ipv6 = 0) of the IPv6 protocol connecting support. The support is enabled by default. While the IPv6 support is disconnected, the daemon iw_icap will be started and work in a regular mode only if the option is enabled (disable_ipv6 = 1).

5.6. Configuring the Processing of Attachments and Archives (detector.conf File)

Configuration file /usr/local/infowatch/tm3/etc/detector.conf stores the database of signatures used to define the file types when unpacking attachments and archives.

The [common] section is intended for configuring the general settings:

Setting	Description
Timeout	Timeout (in seconds) to complete file processing. Default value is 1800
Minfilesize	Minimum file size (in bytes) to be unpacked. This restriction allows increasing system performance by eliminating the extraction of small files. Default value is 10

Setting	Description
FilenameCharsets	If the encoding in the file name differs from the standard (ANSI, UTF), the file will be processed as appropriate to the encoding specified in this setting. Multiple values are listed separated by a comma; the System will consistently try to process the file in the listed encodings until it finds the appropriate one. Default value is "cp1251,cp866"
DefaultTextCharset	If encoding of file content differs from the standard one (ANSI, UTF), the file is will be processed as appropriate to encoding specified in this setting. Values are enumerated comma separated; the System tries to process the file in enumerated encodings sequentially while finds the appropriate one. Default value is "UTF-8"
Speed	Assumptive operation speed of extractor, in KB/s, per 1 GHz of processor. Default value is "100"
NeedLogLevel	Log level - from 0 (only errors are logged) to 8 for debug info. Corresponds to syslog levels. Default value is 0.

If common setting Timeout and MinFileSize values are not suitable for any type of files, you should include these settings in the section for relevant types of files with other values.

Other sections contain signatures used to detect the types of files in attachments and archives. Each section contains the same setting set:

Setting	The description and examples of configuring
Ext	Archive file extension. This optional setting is required for correct functioning of some archives requiring the presence of correct input file extension **Example** Ext = arj
Name	Format name. Used to accurately determine the name of the format to extract the file. To determine / refine the format may also include a list of names: "defaultname, name1(code1), name2(code2)" In this case format is determined based on the code (*codeN*), assigned to the file when extracting. For example, if the unpacking is completed with the *code1* code the file is expected to be in *name1* format. A list of names may also include a default name (*defaultname*), that is assigned where the code is not assigned: **Example 1 (one name of the format)** text/xml **Example 2 (list of the format names)** "application/arj, UNKNOWN(9), text/encrypted(4)" By default the file format is defined as application/arj. Two other specific cases: archive format is unknown (*UNKNOWN*), the archive is encrypted (*text/encrypted*)

Setting	The description and examples of configuring

Sign	The format signature that is the pattern for succession of values (bytes) with the initial displacement and masks. This succession is required for unambiguous definition of the file format based on contents.
	The signature may contain up to 16 triads of the following kind:
	`[OFFSET]:BYTE_VALUE/[MASK]`
	A string signature is also valid, for example, `"BZh"`, for BZIP2. This signature identifies the specified sequence of bytes from 0 offset. Search of string signatures is not case sensitive.
	The `OFFSET` setting is optional. The default value of the setting for the first byte is `0`; for all the subsequent bytes it is increased by one. Offset may be specified with "?" symbol – search of sample in the first N bytes of the file. For example, to search for the pattern in the first 500 bytes of the file, set the offset to `'500?'`.
	The `MASK` setting is also optional; its default value is `0xFF`.
	Example (WAV header signature):
	`Sign = "'RIFF', 0x8: 'WAVEfmt'"`
	Starting from 0 offset the sequence `'R'`, `'I'`, `'F'`, `'F'` is located; further on, from offset 8 the `'W'`, `'A'`, `'V'`, `'E'`,`'f'`, `'m'`, `'t'` sequence is required.

Comment	Commentary with explanations, for example, an indication of the archiver version being used: `Comment = "bzip2 v. 1.0.x"`
Extract	Command line for extracting files. For example, `Extract = "/usr/bin/bzip2 -f -dc ${SRC} > ${OUTDIR}/${SRC}"` where `${OUTDIR}` is the directory to unpack the archive to and `${SRC}` is the name of the file to be decompressed.
Exclude	If the setting is enabled (`On`), unpacking of the object is performed, but archiver is not added to the XML-object context. This allows not to display the fictive containers in the context of the object such as MS-TNEF. This setting is disabled by default (`Off`)
CaseInsensitive	A character that, when processing the file, it will not be case sensitive.
CreatesTags	A character that during the processing using Traffic Monitor extractors, the extraction of metadata from a file occurs.

5.7. Sample document database synchronization across multiple servers

> **Important!**
>
> Sample document database synchronization could be performed if you use two or more Traffic Monitor servers.

If there are two or more Traffic Monitor servers used in the System, there are different logics of sample document database updating could be used:

- *Master* server – main server, which updates the sample document database (executing **db_CA.pl** script). System can include only one *Master* server;

- *Slave* server – secondary server, which copying the *Master* server sample document fingerprints. *Slave* server works with sample document database by exchanging of service information, which confirms the sample document database settings relevance (executing the **db_CA_lite.pl** script). System can include one or more *Slave* server.

All servers in the system are configured to work as the main (*Master*) by default, so it is necessary to synchronize the sample document database across multiple servers.

To synchronize the sample document database across multiple servers:

4. Select which server will be used as the *Master*.

> **Note:**
>
> Other server would be used as *Slave* servers.
>
> The choice of the server's working logic (*Master* or *Slave*) depends on the system administrator's preference and doesn't require steps of additional setting, except those specified in the subsection.

5. At *Slave* server (servers):
   d) Log in as **root**.
   e) In the **/etc/crontab** file delete the string

   ```
   * * * * * root /usr/local/infowatch/tm3/bin/scripts/db_CA.pl&>/dev/null
   ```

   Slave server would stop running the **db_CA.pl** script.

   f) Run the command:

   ```
   service crond restart
   ```

   Scheduled tasks on a server would be updated.

6. At *Master* server:
   d) Log in as **root**.
   e) Run the command:

   ```
   ssh-keygen
   ```

   ```
   ssh-copy-id -i /root/.ssh/id_rsa <server_Slave>,
   ```

   where `<server_Slave>` - IP-address of *Slave* server.

   > **Important!**
   >
   > The `ssh-copy-id <server_Slave>` command must be executed for every *Slave* server using in the System.

   f) Run the command:

   ```
   /usr/local/infowatch/tm3/bin/scripts/db_CA.pl
   ```

5.8. Configuring the Maximum Size of Added Sample Document (casdbcfg.conf file)

Configuration file `/usr/local/infowatch/tm3/etc/casdbcfg.conf` contains a value of max size of the sample document which can be used for digital fingerprint creation (see details on sample documents in «*InfoWatch Traffic Monitor. User Guide*»).

Default max file size is 128 Mb:

```
CAMaxFileSize = 128
```

However this setting can be changed only through the database.

To change maximally acceptable size of downloaded sample document:

1. Connect to the database server under DB schema owner:

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

   where `db_login` and `db_password` are name and password of DB schema owner and `tns_name` is a name of TNS service.

   If the check was successful the response will:

   ```
   SQL>
   ```

2. Run the following script:

   ```
   begin
      sp_ca_max_file_size_set(128);
   commit;
   end;
   /
   ```

   where instead of 128 specify necessary acceptable file size, in megabytes. To remove constraint specify «-1».

As a result, the value of `CAMaxFileSize` setting in `casdbcfg.conf` file will be changed as well.

5.9. Configuring filtering rules for Sniffer

Using a Sniffer scheme you can configure your System to transfer only packages sent to specific addresses and ports for processing in Traffic Monitor. These rules are set separately for each type of traffic and are contained in `icq.rules`, `http.rules` and `smtp.rules` files of `/usr/local/infowatch/tm3/etc/` directory.

`File contents is a set of rules used as criteria to check package matching.`

Each rule has the follong format:

```
aaa.bbb.ccc.ddd[/number_of_bits] *|port1,port2,port3-port4 ACCEPT|DROP
```

where:

- `aaa.bbb.ccc.ddd` – host or subnet IP address
- `Number_of_bits – number of bits, if none is specified, is equal to` 32 (i.e. to run the rule package IP must be exactly as specified).
- `port1,port2,port3-port4` – port list: ranges delimited with commas are listed with a hyphen. If a "*" is specified instead of port list, packages from all ports are accepted.
- `ACCEPT` – if the condition is met the package is accepted and transferred for further processing.
- `DROP` – if the condition is met further package processing is stopped, and it is not transferred neither to Traffic Monitor server, nor to database.

Strings with comments start with '#' symbol.

Filtering is performed in the following order:

Package IP address and port are verified for rule matching: from the first to the last string.

If the IP address is matched by mask and the port is within the specified range, the operation set in the rule is applied: package is accepted and transferred for further processing (ACCEPT), or its processing is stopped (DROP).

If IP address or port doesn't meet the condition, the verification is performed based on the next string.

If none of the rule file conditions is met, further package processing is stopped, and it's not transferred neither to Traffic Monitor server, nor to database.

Example:

Let the package sent to 10.1.0.1, port 22, be verified based on the following rules:

```
# Reception of packages sent to port 3128 on the server 10.0.1.128
10.0.1.128 3128 ACCEPT
# Drop the rest of 10.0.1.* subnet flow
```

```
10.0.1.0/24 * DROP
# Receiving all data sent to standard ports and proxies in 10.*.*.* subnet
10.0.0.0/8 1-1023,3128,8080 ACCEPT
# All other packages are dropped
```

As a result the third rule is applied to the package, and the package is transferred for further processing in Traffic Monitor.

5.10. Management of Loading Objects to Remote Database

Loading of objects to the remote database is used when an organization has one or more branches, and the traffic which is intercepted in the branches should be stored in a central office. Then, after the analysis, the objects of the branches are transmitted to the database of the central office. Data transmission occurs over a slow communication channels (from 128 Kbit/s).

The additional module is installed to implement the scheme of interaction with a remote database on the Traffic Monitor Server. The client end is installed at the branches; the server part of the remote database management module is installed in the central office.

The main deployment schemes during the work with remote database are described in *"Installation and Configuration Guide".*

This section further covers:

- *Settings of Receiving Objects at Server End (i. 5.10.1 on page 71).*
- *Settings of Sending Objects at Client End (i. 5.10.2 on page 72).*
- *Configuring the Bandwidth of the Data Transmission Channel (Client) (i. 5.10.3 on page 72).*
- *Viewing the Statistical Information on Loading of Objects to a Remote Database (i. 5.10.4 on page 73).*

5.10.1. Settings of Receiving Objects at Server End

The `/usr/local/infowatch/tm3/etc/qmover.conf` file located at the server-end (object downloader), `[QMOVER_SERVER]` section, specifies settings of accepting objects from clients:

Setting	Description
`Daemon`	Starts in daemon mode (`On` value) or as a standard process (`Off` value). The default value is `On`
`LogLevel`	Log level: `0`(only errors are logged) - 8 for debug information. Corresponds to the syslog logging level. Default value is 1.
`ListenerPort`	Port, which will listen the incoming objects. The default value is 16888.
`Clients`	List of remote clients, transferring objects to the server: `Clients = "client_1 client_2 … client_N"` The settings for each client are set in the separate `[client_N]` section: • `IP`. IP address for client N. • `QueuePath`. The path to the queue where files received from the client N are delivered.

5.10.2. Settings of Sending Objects at Client End

The client end `/usr/local/infowatch/tm3/etc/qmover.conf` file (object interceptor) in `[QMOVER_CLIENT]` section contains settings for objects queue transmission to remote database:

Setting	Description
`Daemon`	Starts in daemon mode (On value) or as a standard process (Off value). The default value is On
`LogLevel`	Logging level. `0` (only errors are logged) - 8 for debug information. Corresponds to the sys-log logging level. Default value is 1.
`ListenerIP`	IP-address of the server-loader, which will listen the incoming objects. The default value is `127.0.0.1`.
`ListenerPort`	Port of the server-loader, which will listen the incoming objects. The default value is 16888.
`Window`	The window size (in frames). The default value is 100.
`MaxFrameSize`	Maximum frame size (in bytes). The default value is 1400. Note: It is not recommended to set the frame size greater than the maximum frame size (MTU) of the routers that are between the client and the server.
`QueuePath`	Path to the local queue of objects, which must be forwarded to a remote server. The default value is `queue/db/`

5.10.3. Configuring the Bandwidth of the Data Channel (Client)

By default, the bandwidth is 128 Kbit/s. You can configure the bandwidth to be changed automatically at different time periods. It will be set on the client end (the interceptor of objects) using the utility:

```
/usr/local/infowatch/tm3/bin/iw_qmover_channel__width_setter
```

The bandwidth can be varied from 128 Kbit/s through 2 Mbit/s.

To set bandwidth limitations:

on sender server end (*client*) configure crond to run the `iw_qmover_channel_width_setter` utility at the specified intervals.

The utility is run with the mandatory settings:

```
iw_qmover_channel__width_setter <bandwidth>
```

where `Bandwidth` is the bandwidth value (kbit/s) to be set.

Example

There is a channel whose bandwidth is 256 Kbit/s. 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%.

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

Interval	Bandwidth	
	Percent of the bandwidth	Equivalent in Kbit/s
9 AM to 6 PM	50%	128

Interval	Bandwidth	
	Percent of the bandwidth	Equivalent in Kbit/s
6 PM to 9 AM	100%	256

2. Add these commands to cron:

```
00 9 * * * /usr/local/infowatch/tm3/bin/iw_qmover_channel_width_setter 128
00 18 * * * /usr/local/infowatch/tm3/bin/iw_qmover_channel_width_setter 256
```

5.10.4. Viewing the Statistical Information on Loading of Objects to a Remote Database

You can view the statistical information on loading of objects into a remote database on the client and the server.

To display statistical information on the work of the client,

run the command:

```
killall –SIGUSR2 iw_qmover_client
```

After running the command, the following information will be recorded to the system log on the client end:

Log record	Value
stat: started at	Time of launching `iw_qmover_client daemon`
stat: works on … file queue	The path to the queue of objects prepared for transfer to the server
stat: bytes sent: … objects sent: …	The volume of objects sent (in bytes) The number of objects sent
stat: bytes recv: … file ACKs recv: … object NAKs recv: …	The volume of server acknowledgments (in bytes) Number of objects successfully received by the server-loader (*server*) The number of commands for re-processing of objects
stat: uses bandwidth … kbit/s	Bandwidth (kbit/s), occupied by the client at the current moment
stat: connected to server <IP-address> or stat: currently disconnected from server <IP-address>	Client connected to a server-loader with the specified IP-address or disconnected from the server-loader

To display statistical information on the work of the server,

run the command:

```
killall –SIGUSR2 iw_qmover_server
```

After running the command, the following information will be recorded to the system log:

Log record	Value
stat: started at	Start time of service (listener), which is listening objects received from the client

Log record	Value
For each client	
stat: client <IP-address> work on … file queue	The path to the file queue to which the objects received from the client with the given IP-address will be loaded
stat: status is CONNECTED or stat: status is DISCONNECTED	The status of connection with client (*client*): connected (CONNECTED) or disconnected (DISCONNECTED)
stat: bytes recv … objects recv …	The volume of objects received (in bytes) The number of objects received
stat: bytes sent … file ACKs sent … file NAKs sent …	The volume of acknowledgements (in bytes) sent to the client Number of objects successfully received by the server-loader (*server*) Number of requests for retransmission of the object

5.11. Archiving a Mail Queue Directory

If errors occur in the incoming SMTP mail queue, you must archive the SMTP mail queue folder and save it for further analysis. Then delete the folder. The location of the mail queue folder is specified in `/usr/local/infowatch/tm3/etc/tm.conf` configuration file in the `[Queue]` section, as a value for `Smtp` setting. The settings of `tm.conf` file are described in i. 5.3 on page 47.

5.12. Logging of System Work

Logging into the InfoWatch Traffic Monitor Server is enabled by the tools of the syslog logging system. The logging subsystem corresponds to *local1*.

For more information on using the syslog logging system, consult the syslog documentation.

Configuring Extended Logging

> **Warning!**
>
> Keep in mind that an increase in the logging level (`LogLevel`) may dramatically reduce System performance.

To configure extended logging for one or several processes of Traffic Monitor Server:

1. In the `tm.conf` file set the required level value (at least 3) for `LogLevel` setting.
2. Enable recording messages with corresponding logging level to the system log `/etc/syslog.conf`. For this purpose you should add the following value to the string for `/var/log/messages`:

   ```
   *.debug;
   ```

3. After the system log is changed, restart the syslog service:

   ```
   service syslog restart
   ```

Log files

Log files are located in the following directories:

- `/var/log/messages` (general log)
- `/var/log/maillog` (analyzing queries and responses from SMTP servers)
- `/var/log/tm.log` (only if system is integrated with Tivoli)

You can also find the complete information on the system operation through the Oracle database: **v_sys_log** table.

Using Sosreport utility for collecting system information

Sosreport utility is a standard Linux utility designed for collecting detailed information on the system: hardware specifications, list of installed packages, actual settings and so on.

To collect information on the system:

1. Close all running applications.
2. Run under root:

   ```
   [root@iwdb ~]# sosreport --batch
   ```

   Do not run any applications; do not make any settings till collecting process ends.

As a result, `/tmp` directory contains file of the form `/tmp/sosreport-iwdb.777777777-57831-7fee1d.tar.bz2`. You can send this file to the Technical Support Service, for example.

5.13. Moving of Objects between Queues (iw_qtool Utility)

The need to move the objects from one queue to another can occur when:

- Objects from branches are uploaded to headquarters office database via narrow-band channel (upload module is used to upload to remote database). Each branch has its own local object queue (local queue), that's why to upload to the database you need to move objects to a common server queue (global queue).
- The objects are not loaded to the database (see Appendix C on page 87).

The **iw_qtool** utility is used to move objects from one queue to another. The order for moving objects is as follows. The oldest objects from the source queue are moved to the beginning of the receiving queue, thus the new objects will be moved to the end of the receiving queue. When the operation is completed, the number of moved objects is displayed.

> **Note:**
>
> You need to run the `iw_qtool` utility under InfoWatch Traffic Monitor owner's account. The name of the owner is specified in the `/usr/local/infowatch/tm3/etc/tm.conf` file, the `[GENERAL]` section, `user` setting.

The commands for using the `iw_qtool` utility:

Command name	Description, syntax, examples

`stat`	Shows the number of objects in a queue.
	Syntax:
	`iw_qtool stat queue_name`
	Example (viewing statistics on queue of objects to be loaded into the database):
	`/usr/local/infowatch/bin/iw_qtool stat /usr/local/infowatch/queue/db`

`Move`	Moves objects from one queue to another. **Warning!** In the process of moving the objects this utility creates temporary files in the current directory. That's why in this case it is recommended to run the `iw_qtool` utility from the `/usr/local/Infowatch/tm3` folder. Syntax: `iw_qtool move source_queue receiving_queue [number_of_objects]`

Command name	Description, syntax, examples
	Settings: • `source_queue` – full name of the queue where you want to move objects from. If the queue does not exist, the utility finishes running with an error; • `receiving_queue` – full name of the queue where you want to move the objects to. If the queue does not exist, it will be created when the utility is running. • `number_of_objects` – limit for the number of objects to be moved (optional setting). If the setting is not specified, then all the objects in the source queue will be moved. *Example (moving objects from errors queue to the db queue):* `iw_qtool move /usr/local/infowatch/tm3/queue/errors /usr/local/infowatch/tm3/queue/db`

`Put`	Puts a single object to the queue
	Warning! To run the command, you must have write privileges for current directory.
	Syntax:
	`iw_qtool put receiving_queue xml_object_file object_file`
	Settings:
	• `receiving_queue` – full name of the queue where the object should be put. If the queue does not exist, the utility finishes running with an error;
	• `xml_object_file` – full name of the XML object file. If the specified file does not exist, the utility finishes running with an error.
	• `object_file` – full name of the object data file. If the specified file does not exist, the utility finishes running with an error.
	The example (putting of objects to the db queue):
	`iw_qtool put /usr/local/infowatch/tm3/queue/db /home/iwtm/000000000.dat.xml /home/iwtm/000000000.dat`

5.14. Loading an Object Queue

To load the existing object queues:

1. Stop Traffic Monitor Server processes:

   ```
   service iw-trafmon stop
   ```

2. Disable autorun for iw_proxy, iw_smtpd and iw_expressd interceptor processes in `/usr/local/infowatch/tm3/etc/tm.conf` file, section `[AUTO_RESTART]`:

   ```
   autorestart = Off
   ```

3. Start Traffic Monitor processes

   ```
   service iw-trafmon start
   ```

4. Wait until all the objects in the file queue are processed. To do this, you can monitor contents of the directories with queues (for their location see i. 5.3.6 on page 51).

> **Note:**
>
> On completion of the update process, make sure that the interceptors are running and process autorun is enabled in the configuration file.

5.15. 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. Close all instances of the Management Console.
2. Stop the processes of the Traffic Monitor Server by running the command:

   ```
   service iw-trafmon stop
   ```

3. Move all objects from the queues where errors occur to the normal ones. To perform the procedure use iw_qtool utility (see i. 5.13 on page 75).
4. When these operations are completed, check the connection to the Oracle DBMS by running the command:

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

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

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

   ```
   SQL>
   ```

5. Run the Traffic Monitor Server processes by running the commands:

   ```
   service iw-trafmon start
   ```

After the Traffic Monitor Server is started, check the system log for errors. The path to the system log:

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

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

APPENDIX A. INSTRUCTIONS FOR USING THE AUTOARCHIVE UTILITY

The autoarchive utility is designed for archiving tablespaces in the database schema (version 3.4.1 or higher).

> **Warning!**
>
> Do not run the database jobs manually while the autoarchive utility is working: IWADDPARTS, IWTM_SYNC_INDEXES, IWDROP. This may cause the data loss.

This manual describes the following:

- *Setting the Archiving Options (i. A.1 on page 78).*
- *Starting the Autoarchiving (i. A.2 on page 79).*
- *Determining the Environment Variables (i. A.3 on page 79).*
- *Repeated automatic archiving of restored tablespace (i. A.4 on page 81).*
- *Error messages (i. A.5 on page 81).*

A.1. Setting the Archiving Options

Autoarchive setup is performed with `autoarchive.conf` configuration file. The configuration file consists of strings in the following format: `parameter=value`.

Configuration file settings:

Setting	Description
`database`	The line of connections to the DB (tnsname).
`username`	Name of the user. The necessary setting.
`password`	Password. The necessary setting.
`age`	The age of tablespaces in days: the tablespaces which were created earlier are subject to the archiving. The necessary setting. **Example:** if setting value is set to 5, the tablespaces created at least 5 ago will be archived. **Note:** if setting value is set to 0, all tablespaces including the current date tablespace will be archived.
`dest_dir`	The folder for archiving. The necessary setting.
`log_info`, `log_errors`	Output options for informational messages and error messages. To adjust the output messages in a file as a setting value, specify a file name. If the setting is not specified or missing, the messages will be displayed on the console. To disable display of all types of messages, set the setting value to `/dev/null`, for example: `log_info=/dev/null`
`job_timeout`	Timeout waiting for unfinished jobs of the database in seconds. The default value is `7200` (i.e. 2 hours).

An example of the configuration file:

```
database=
```

```
username=iw_test
password=xx1234
age=3
dest_dir=./1/
```

A.2. Starting the Autoarchiving

To start the autoarchiving you must have the following rights:

- rights of the database schema owner (necessary for work with the job and getting the tablespaces with their files).
- unix users must have read and right privileges for files, tablespaces and archive folders. You can use your account or create a separate Oracle user with appropriate privileges.

To run the script manually,

enter the following command:

```
$ perl autoarchive autoarchive.conf [simulate]
```

where:

- `autoarchive.conf` - configuration file (required setting);
- `simulate` - optional setting, running the script in test mode: there will be no real changes in the database, but the stop, search of tablespaces and files for archiving will be performed, and then the jobs will be allowed to run.

To configure the autoarchive to run automatically on a schedule,

create a job specifying the startup time in cron (for details, see man 5 crontab).

The script should run at night, not earlier than 1 hour after the start of the last of the Oracle daily jobs. These jobs include `IWADDPARTS` and `IWDROP`.

A.3. Determining the Environment Variables

In some cases, to access the database the script may require to specify the environment variables. This may be indicated by error messages displayed when you try to run the script (see i. A.5 on page 81). In this case, you must specify the environment variables in the string running the script.

In general, the command line to run the script looks like this:

```
ORACLE_HOME=<value for ORACLE_HOME> LD_LIBRARY_PATH=<value for SO-library> perl -I<value
for pm-module 1> -I<value for pm-module 2> ./autoarchive autoarchive.conf
```

For more details on how to get the environment variables, see i. A.3.1 on page 79 and i. A.3.2 on page 80.

Example of the string for starting autoarchive specifying environment variables:

```
ORACLE_HOME=/u01/app/oracle/product/11.2.0/db_1
LD_LIBRARY_PATH="/u01/app/oracle/product/11.2.0/dbhome_1/lib"                    -
I/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi                        -
I/u01/app/oracle/product/11.2.0/db_1/lib ./autoarchive autoarchive.conf
```

A.3.1. Searching the paths to the modules

When you run the autoarchive it might be necessary to specify the location of pm-modules and SO-libraries, for the work of DBI perl-module which has the access to the database.

To find and display the paths to the modules use a special `autoarchive-autodetect` script.

Note: if the search should include the files that have appeared since the last index, then before running the script, do the indexing manually (see `man updatedb`).

An example of the result of the autoarchive-autodetect script:

```
Using locate to find modules...
{
```

```
 LD_LIBRARY_PATH="/u01/app/oracle/product/11.2.0/dbhome_1/lib"
}
 perl
{
 -I/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi
{
 -I/u01/app/oracle/product/11.2.0/dbhome_1/lib
```

Using the paths to the modules that are displayed as a result of the script, you can create a command line for running the script:

Example 1:

```
LD_LIBRARY_PATH="/u01/app/oracle/product/11.2.0/dbhome_1/lib" -
I/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi -
I/u01/app/oracle/product/11.2.0/dbhome_1/lib ./autoarchive autoarchive.conf
```

Example 2 ($ORACLE_HOME environment variable is installed on the PC):

```
LD_LIBRARY_PATH=$ORACLE_HOME/lib perl -
I$ORACLE_HOME/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi-I$ORACLE_HOME/lib
./autoarchive autoarchive.conf
```

A.3.2. Setting the ORACLE_HOME environment variable

In some cases, for the work of DBI perl modules it is also required to set the `ORACLE_HOME` environment variable. If it is not set, the error message will display when you try to launch autoarchiving (see i. A.5 on page 81).

In this case, in the beginning of the string for running autoarchive, you must specify the environment variable `ORACLE_HOME`. It usually equals `LD_LIBRARY_PATH` without the last `/lib` (see i. A.3.1 on page 79).

Example:

```
ORACLE_HOME="/u01/app/oracle/product/11.2.0/dbhome_1"
LD_LIBRARY_PATH="/u01/app/oracle/product/11.2.0/dbhome_1/lib" -
I/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi -
I/u01/app/oracle/product/11.2.0/db_1/lib ./autoarchive autoarchive.conf
```

A.3.3. Fast launch of autoarchiving

For convenient launch you may create a shell-file with complete command line to run the script `autoarchive`, or set environment variables in advance.

Example 1 (in bash):

```
export ORACLE_HOME="/u01/app/oracle/product/11.2.0/dbhome_1"
export LD_LIBRARY_PATH="/u01/app/oracle/product/11.2.0/dbhome_1/lib"
export PERL5LIB="/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi"
```

Example 2:

```
export ORACLE_HOME=/u01/app/oracle/product/11.2.0/dbhome_1
export LD_LIBRARY_PATH=$ORACLE_HOME/lib
export PERL5LIB="/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi"
```

After completing these settings, the autoarchive can be started using the short string:

```
./autoarchive autoarchive.conf
```

A.4. Repeated automatic archiving of restored tablespace

If previously archived tablespace was restored (see i. 4.3.4 on page 35), repeated automatic archiving of this TS will not be performed as described above.

To automatically archive the restored TS you need to run the following script as a schema owner.

```
BEGIN
   update tbs_list
      set status = 1
      where part_date = tablespace_date;
COMMIT;
END;
/
```

A.5. Error messages

Below you will find the descriptions of possible errors that may appear in the script.

Error text	Reason, actions

/u01/app/oracle/product/11.2.0/dbhome_1/perl/lib/site_perl/5.10.0/i686-linux-thread-multi/auto/DBI/DBI.so: undefined symbol: Perl_Istack_sp_ptr	Check the version of perl DBI using the following command:
	`rpm –q perl-DBI`
	If the package is missing or has a version lower than 1.52, perform the installation using the following command:
	`rpm –i perl-DBI`

Can't locate DBI.pm in @INC (@INC contains: [long list here]) at autoarchive BEGIN failed--compilation aborted at ...	The paths to the pm-modules are not set or incorrect.
install_driver(Oracle) failed: Can't load '[...]Oracle.so' for module DBD::Oracle: libclntsh.so.11.1: cannot open shared object file: No such file or directory at /usr/lib/perl5/5.8.8/i386-linux-thread-multi/DynaLoader.pm line at (eval 1) line 3 Compilation failed in require at (eval 1) line 3. Perhaps a required shared library or dll isn't installed where expected at autoarchive.pl line	The LD_LIBRARY_PATH is not set or incorrect
ORACLE_HOME environment variable not set! DBI connect('database','username',...) failed: (UNKNOWN OCI STATUS 1804) OCIInitialize. Check ORACLE_HOME and NLS settings etc. at autoarchive DBI Connect error: (UNKNOWN OCI STATUS 1804) OCIInitialize. Check ORACLE_HOME and NLS settings etc. at autoarchive	The ORACLE_HOME environment variable is not set
DBI connect('iwtm','iwtm_578',...) failed: (UNKNOWN OCI STATUS 1804) OCIInitialize. Check ORACLE_HOME and NLS settings etc. at autoarchive DBI Connect error: (UNKNOWN OCI STATUS 1804) OCIInitialize. Check ORACLE_HOME and NLS settings etc. at autoarchive	The ORACLE_HOME environment variable is set, but incorrect
DBI connect('iwtm','iwtm_578',...) failed: Error while trying to retrieve text for error ORA-12154	ORACLE_HOME environment variable is set,

(DBD ERROR: OCIServerAttach) at autoarchive DBI Connect error: Error while trying to retrieve text for error ORA-12154 (DBD ERROR: OCIServerAttach) at autoarchive	but incorrect

APPENDIX B. MONITORING INDICATORS

The following table lists all indicators used by monitoring subsystem to check System components status. Here the terms “check" means regular retrieval of indicator value and comparing this indicator value to a threshold value.

> **Warning!**
>
> If configuration files were modified, threshold values and check period may differ from the specified ones.

If all indicators point to critical values, this may indicate to physical unavailability of checked servers. Check their operations.

Service management (e.g. status check) is performed from `root` account.

> **Warning!**
>
> If you can’t solve the problem with actions recommended in the table, please contact InfoWatch Technical Support at support@infowatch.com.

Indicator name	Check	Values	Survey period	Actions when indicators threshold values are achieved
iwmon-services configuration file				
PING	Access to the host via `ping` command	– host unavailable – host available	5 min.	Check network equipment (commutation & settings) Check firewall settings
SSH	Host availability via ssh	– ssh unavailable – ssh available	10 min.	Check network equipment (commutation & settings) Check firewall settings Make sure that sshd service is running: `service sshd status`
Swap Usage	SWAP busy on host. Indicates RAM shortage	– free < 10% SWAP – free 10 - 20% SWAP – free >20% SWAP	5 min.	Find most memory consuming processes in processes table and take relevant actions.
Current Users	Number of users registered at the host	– >50 users – 20 - 50 – < 20 users	30 min.	Using `who` and `w` commands define users registered in the system and disconnect excessive users.
Total Processes	Free space running at the host	– >400 processes – 250 – 400 – < 250 processes	30 min.	In processes table find the most numerous processes using `ps` or `top` commands and take relevant actions.

Indicator name	Check	Values	Survey period	Actions when indicators threshold values are achieved
Root Partition	Free space in root file system	– free < 10% – free < 20% – free >=20%	30 min.	Check contents of root file system and free some space where possible. Otherwise connect add some extra disk space
/var Partition	Free space in file system `/var`	– free < 10% – free < 20% – free >=20%	30 min.	Check contents of /var file system and free some space where possible. Otherwise connect add some extra disk space

service ntpd state	Status of ntpd system service	– service not launched
		– service launched
			30 min.	Make sure that the service is running:
				`service servicename status`
				Start the service:
				`service servicename start`
				and enable its automatic launch:
				`chkconfig --list servicename`
				`chkconfig servicename on`
				where `servicename` is the name of service.
				In case of service launch failure eliminate the reason of failure and restart the service.

service crond state	Status of CRON system service	– service not launched – service launched	30 min.	
local postfix smtp	Status of Postfix system service	– service not launched – service launched	30 min.	
service syslog state	Status of syslog system service	– service not launched – service launched	30 min.	
TM Licence	Interceptors license date validity	– < 2 days – <= 2 weeks – >=20 weeks	24 hrs	Upgrade analysis subsystem license as described in “Installation and configuration guide” documents, section 3.3.3 ”Installing licenses for analysis subsys-tem”
TM queue SMTP	Number of objects in `smtp` queue	– >= 200 objects – < 10	30 min.	Check DB availability Make sure that dbloader is running Review alert_iwtm.log. messages log records (whether there are messages informing that DB is busy by running job, and can’t insert new objects (high CPU load may also be a symptom). In this case you may either wait until job is complete or (if job is hanging for more than 24 hrs), find and eliminate reasons of hanging and stop it from running.
TM queue Errors	Number of objects in `errors` queue	– >= 200 objects – < 10	30 min.	
TM queue DB	Number of objects in `db` queue	– >= 200 objects – < 10	30 min.	
TM coredump files	Availability of coredump files in TM folder	– at least coredump file available – no coredump files available	4 hrs	Upload coredump files and send them to InfoWatch support for further research
TM daemons state	TM service status	– at least one service not launched – all services launched	30 min.	Eliminate the reason of failure and start services

Indicator name	Check	Values	Survey period	Actions when indicators threshold values are achieved
CAS Licence	Analysis subsystem license date validity	– < 2 days – <= 2 weeks – >=2 weeks	24 hrs	Upgrade analysis subsystem license as described in “Installation and configuration guide” documents, section 3.3.2 ”Installing and upgrading licenses for interceptors”
Syslog Errors	Error records in system log Disabled by default (setting in configuration file is commented)	– at least one record available – no error records available	10 min.	Review errors in the system log, identify and eliminate reasons of errors.
iwmon-services-db configuration file				
DB Alert Log Errors	Error records in database `alert_iwtm.log` log	– at least one record available – no error records available	5 min.	Review errors in `alert_iwtm.log` log, find and eliminate reasons of errors.
DB Alert Log Size	Oracle log file (`alert_iwtm.log`) size	– < 100 Mb – <= 50 Mb – >= 50 Mb	5 min.	If the file size is growing too fast, find our and eliminate the reasons of its growth. Make a copy of log file and archive it. Reset the file: `> alert_iwtm.log`
Oracle Database Status	Availability of required DB Default `DB=iwtm`	– DB available – DB unavailable	10 min.	If server end of Traffic Monitor and DB are installed at different computers, check network equipment (commutation and settings) and firewall settings on TM server. If DB is installed on the same PC as the server end of Traffic Monitor, launch oracle service: `service oracle start`
DB v_sys_log Errors	Error records in `v_sys_log database` view	– at least one record available – no error records available	30 min.	Run the following SQL query: `select CONTENT, DATE_INSERT from v_sys_log where SEVERITY=('WARNING','ERROR');` Pass query results to InfoWatch Support Service for further research
Oracle TNS Status	TNS listener operation	– TNS listener not launched – TNS listener launched	10 min.	Make sure that the listener is running: Make sure that oracle service is registered with the listener Make sure there’re no networking issues between monitoring server and DB server.
/u01 partition	Free space in file system `/u01`	– under 10% free – over 20% free	10 min.	Check TS removal interval value (`drop_interval` setting for `drop_part_date_lag` setting) – see i. 2

Indicator name	Check	Values	Survey period	Actions when indicators threshold values are achieved
/u02 partition	Free space in file system `/u02`	– under 10% free – over 20% free	10 min.	on page 36. If required, decrease this value. Check contents of file system and free some space where possible. Otherwise connect add some extra disk space
iwmon-services-ntp configuration file				

NTP time	Time gap on server with template	– > 1 sec gap
		– 0,5 - 1 sec gap
		– time synchronized
			30 min.	Run synchronization:
				`service ntpd stop`
				`ntpdate <ip of ntp server>`
				`hwclock --systohc`
				In /etc/ntp.conf file specify IP address of ntp server for server setting.
				Start ntpd:
				`service ntpd start`

iwmon-services-loadavg configuration file				
Current Load	Load on relevant hosts group. Number of processes awaiting scheduling based on 4 physical CPU cores Activation threshold for a different number of cores is calculated proportionally.	– > 20.0,16.0,12.0 – 10.0,8.0,6.0 - 20.0,16.0,12.0 – < 10.0,8.0,6.0	30 min.	Adjust threshold values based on number of cores on the host.
iwmon-services-traffic configuration file				
Check Traffic	Database objects having SOURCE_IP of subnets specified in `check_command` parameter. Disabled by default (parameter in config file is commented)	– no objects from specified subnets available – at least one object from specified subnets available	1 hour	Check networks in traffic copy: 1. Send test messages from subnets 2. Check sending with `tcp dump` command. 3. Make sure that the check indicates object presence in DB. If the check is successful, increase the survey period to eliminate odd notifications
iwmon-services-dm configuration file				
Device Monitor Status	State of InfoWatch Device Monitor service. Disabled by default (setting is commented in the configuration file)	– service disabled – service enabled	10 min.	Check the service availability at the InfoWatch Device Monitor server directly.

APPENDIX C. TROUBLESHOOTING

When you run the iw_messed, iw_deliverd processes, a message that the Oracle DBMS dynamic libraries cannot be found is returned.

The `ORACLE_HOME` environment variable was incorrectly specified in the `iw-trafmon` autorun script.

Decision

Open the autorun script of the server part:

`/usr/local/infowatch/tm3/bin/scripts/iw-autorestart.sh`

Check the value for the `ORACLE_HOME` environment variable. This value should match the value for `ORACLE_HOME` specified during Oracle DBMS installation.

When you run the iw_messed, iw_deliverd processes, a message is displayed that you do not have privileges to load the dynamic libraries of Oracle DBMS.

The Traffic Monitor Server is installed incorrectly.

Decision

You must include user who owns Traffic Monitor Server (the account used to run Traffic Monitor Server processes) in the `oinstall` group (group of the owner of Oracle DBMS client installation). InfoWatch Traffic Monitor owner group is specified in `/usr/local/infowatch/tm3/etc/tm.conf file`, `[GENERAL] section` (see i. 5.3.1 on page 47).

The System performance reduces significantly or processing of the traffic stops completely

This may be caused by the following reasons:

The reason of the problem	Decision
The work of logwatch script of the operating system increases the load on the System processes. As a result, the speed of traffic processing reduces significantly.	There are two solutions for this problem: • For all Traffic Monitor Server processes set the logging level value (`LogLevel` setting in `tm.conf file`) to 0. • Disable the running of the `logwatch` script in `crond` (by default the script runs at 4 a.m. every day)
The logging level of Traffic Monitor Server is high for one or more processes	For all processes default logging level is recommended (see i. 5.3 on page 47). To verify the logging level check the values of `LogLevel` setting in the following files: • `usr/local/infowatch/tm3/etc/tm.conf` (`SMTPD`, `MESSED`, `DELEVERD`, `SNIFFER`, `PROXY`, `CAS`, `DBLOADER`, `EXPRESSD`, `UPDATER` sections); • usr/local/infowatch/tm3/etc/qmover.conf (`[QMOVER_server]`, `[QMOVER_client]` sections) • usr/local/infowatch/tm3/etc/icap.conf (ICAP section) If the logging level has been raised for one or more processes, lower it, it is recommended to return to the default value

The work of database was suddenly interrupted when loading an object into the database

If operation of the database is interrupted while loading the object to database, that object is placed to the `/usr/local/infowatch/tm3/queue/errors` queue. Such object will not be automatically loaded to the database later on.

Decision

Using the iw_qtool utility copy the object from the `/usr/local/infowatch/tm3/queue/errors` queue to the `/usr/local/infowatch/tm3/queue/db` queue.

Example:

```
iw_qtool move /usr/local/infowatch/tm3/queue/errors /usr/local/infowatch/tm3/queue/db
```

Note:

You need to run the `iw_qtool` utility under InfoWatch Traffic Monitor owner's account. The name of the owner is specified in the `/usr/local/infowatch/tm3/etc/tm.conf` file, the `[GENERAL]` section, `user` setting.

GLOSSARY

Active Directory

LDAP-compatible implementation of Microsoft smart directory service for Windows operating systems

Administrator

Pre-installed role and Management Console account that has privileges for managing other accounts and their rights. Also - system user performing installation, configuration and supporting operation of System. See also: Security Officer

Authorization engine

Transfer method and contents of user data that is passed by HTTP client to proxy

BCC

Blind Carbon Copy. Technique that enables sending a copy of message to another recipient (in addition to main recipient) without any indications to it in original message.

Cluster

Group of PCs sharing the same set of installed components which is arranged and used as a common resource. See also: Component

Component

System software unit that may be installed independently from other System parts

Copy mode

Transport Mode attribute value. In this mode only the copy of traffic is passed through the System, not the real traffic, therefore, the feature to block traffic with System tools is unavailable. See also: Transport Mode, Interception Mode

Daily tablespace

One of tablespace types in InfoWatch Traffic Monitor database. Used to store data intercepted within 24 hours (intercepted objects, analysis & object processing results). Daily TS are being created every day in such a way that the database always has a TS for the next two days.

Data Interception

Retrieval, parsing, classification and conversion of data (or copies of data) into context. Interception is performed for data passed via SMTP, HTTP, ICQ/OSCAR, IXP protocols. See also: Data Transfer Channel, Interceptor

Data Transfer Channel

Environment containing technical facilities for data transfer, software tools and data transfer protocols. Traffic Monitor supports intercepting data in the following data transfer channels: email (SMTP), web (HTTP), instant messengers (ICQ), shadow copies of files and workstations connection/disconnection events, print jobs.

DB

Database.

DBMS

Database management system

Device Monitor

Traffic interception module. Software designed for managing user access to peripherals and monitoring operations that involve copying files to removable storage media and sending them to printer.

DeviceLock

Software complex developed by ZAO “Smart Line Ink” that controls user access to peripherals and local PC ports

DeviceLock Adapter

Traffic interception module. Interceptor that passes shadow copies of files transferred to external data carriers and sent to printer, from Traffic Monitor from DeviceLock system (Smart Line Ink). See also: Device Monitor, Shadow copy, Interceptor, DeviceLock

ICAP

Internet Content Adaptation Protocol – protocol enabling control of inbound/outbound HTTP-traffic. Enables modifying HTTP requests contents (only outbound traffic within InfoWatch Traffic Monitor). See also: ICAP Client, ICAP Server

ICAP Client

Component installed on proxy supporting ICAP features. Passes HTTP request or response, encapsulated in ICAP-message, to ICAP server. Receives ICAP server response (skip/block HTTP-request). See also: ICAP

ICAP Server

Server component receiving HTTP requests encapsulated in ICAP message. Retrieves HTTP requests from ICAP message and pre-processes them. Passes response with processing results to ICAP client. See also: ICAP

InfoWatch Traffic Monitor

InfoWatch Traffic Monitor (IW TM) software complex. Designed for control of various informational data transfer channels (SMTP, HTTP, ICQ. In Traffic Monitor Enterprise – also data copied to removable data carriers and sent to printer). See also: Traffic Monitor Enterprise, Traffic Monitor Standard

Integration with Postfix

Configuring Postfix mail server usage as a relay server in the scheme of intercepting SMTP-traffic copy. See also: Postfix

Interception mode

Method of processing traffic by Traffic Monitor: processing real traffic or traffic copy. In the first case Traffic Monitor receives real traffic, and intercepted objects are only sent for further processing after they are processed and decision is made. In the second scenario Traffic Monitor received copy of traffic, and Traffic Monitor has no impact on sending intercepted objects. See also: Data Transfer Channel, Interceptor, Object

Interceptor

Software retrieving data from external clients, provisioning the data for further analysis and passing them to processing subsystem. See also: Data Transfer Channel

LDAP

Lightweight Directory Access Protocol – network protocol for access to X500 directory service using TCP/IP

LUN

Logical Unit Number – logical disk represented as “physical” disk in operating system.

Mail agent

Aka MTA (Mail Transfer Agent). Message forwarding agent, mail server – software that transfers mails between computers.

Management Console

Graphic user interface. Designed for managing InfoWatch Traffic Monitor (administrating the System, configuring settings, analyzing objects, etc.).

Normal transport mode

Transport Mode attribute value. In this mode real traffic is passed through the System, and the feature to block objects banned by the System is available. See also: Transport Mode, Interception Mode

Object

Data retrieved by the System from intercepted traffic (SMTP message, HTTP requests, ICQ messages) or from external systems (shadow copies of files and print jobs) and converted by processing subsystem into a internal view.

OSCAR

Open though not free network protocol that enables instant & offline messaging. It is used by ICQ and AIM instant messengers.

Postfix

Mail agent (MTA) that you can integrate to intercept and deliver SMTP traffic within the System. See also: Mail Agent

Print jobs

Information on sending data for printing together with printed document

Processing Objects

Intercepted object parsing procedure that converts the object into context and assigns some attributes to it.

Proxy

Service for transferring data between client computers and network servers. Used by the System during interception of HTTP traffic.

Relay-server

Broadcasting server. System may retrieve SMTP-traffic from a mail relay-server

Responsibility Zone

Way to divide intercepted objects which enables to limit access of Management Console users to them. The objects belonging to a certain responsibility zone are visible to the users who belong to this responsibility zone (provided that the user has privileges to view or/and handle the objects).

Security Officer

Pre-installed role and Management Console account that has all the privileges except managing users and roles. See also: Administrator

Shadow copy

A copy of the file which is created on a removable storage media. The copy is created only if the file is successfully saved to the removable storage device.

Sniffer

See also: Snuffer, Network traffic analyzer. Interceptor, InfoWatch Traffic Monitor component, retrieving data (SMTP, HTTP, ICQ traffic) of traffic copy, passing through SPAN-port of the switch and transferring them to processing subsystem. See also: Data Transfer Channel, Interceptor

SPAN

Switched Port Analyzer – technique that enables mirroring traffic from one port to another

SPAN-copy

Implementing interception mode for CISCO switch traffic copy. Enables operation of “Copy” transport mode. See also: Interception Mode, SPAN, Copy Mode,

System

See: InfoWatch Traffic Monitor

Traffic

Information flow within communication system. Within InfoWatch Traffic Monitor only outbound traffic is screened, that is passed via SMTP, HTTP and ICQ protocols.

Traffic Monitor Enterprise

InfoWatch Traffic Monitor edition that provides the full System functionality.

Traffic Monitor Server

Computer or aggregation of computers where InfoWatch Traffic Monitor components are located, except management console and database. See also: Management Console

Traffic Monitor Standard

InfoWatch Traffic Monitor edition that provides the limited System functionality. Specifically it enables interception of data in copy mode only. See also: Copy Mode

Transparent transport mode

Transport Mode attribute value. In this mode real traffic is passed through the System, but the feature to block objects banned by the System is unavailable. See also: Transport Mode, Interception Mode

Transport Mode

Object attribute specified in a script. It should consider implemented interception mode; determines the way of further delivery for the object. See also: Interception Mode, Copy Mode, Normal Transport Mode, Transparent Transport Mode

TS

Tablespace. Logical unit of data storage structure in Oracle DB that consists of one or more data files.