

INFOWATCH

# InfoWatch Traffic Monitor 4.1

Installation and Configuration Guide

INFOWATCH TRAFFIC MONITOR 4.1

# Installation and Configuration Guide

© ZAO “InfoWatch”
Tel/Fax +7 (495) 229-00-22
http://www.infowatch.com
Revision date: 24/12/2015

# TABLE OF CONTENTS


INTRODUCTION ..... 5
Who Should Read this Guide ..... 5
Guide Structure ..... 5
Additional Documentation ..... 5
General Conventions ..... 6
Technical Support ..... 6

CHAPTER 1. INFOWATCH TRAFFIC MONITOR OVERVIEW ..... 7
1.1. InfoWatch Traffic Monitor Features ..... 7
1.2. InfoWatch Traffic Monitor Standard and InfoWatch Traffic Monitor Enterprise ..... 8
1.3. InfoWatch Traffic Monitor Components ..... 8

CHAPTER 2. GETTING READY TO INSTALL ..... 10
2.1. System Deployment Schemas ..... 10
2.1.1. Receiving Copies of SMTP Traffic from a Mail Server ..... 10
2.1.2. SMTP Traffic Interception ..... 12
2.1.3. Intercepting a Traffic Copy through the Sniffer ..... 13
2.1.4. Intercepting HTTP Traffic Transmitted over ICAP ..... 17
2.1.5. Receiving Objects Intercepted by InfoWatch Device Monitor ..... 19
2.1.6. Receiving Objects Obtained from DeviceLock ..... 21
2.1.7. Revision of Files from the Corporate Network ..... 22
2.2. Hardware and Software Requirements ..... 24
2.2.1. Sniffer ..... 25
2.2.2. IW ICAP Module ..... 25
2.2.3. IW Crawler ..... 26
2.2.4. Management Console ..... 27

CHAPTER 3. INSTALLING AND CONFIGURING THE SYSTEM ..... 28
3.1. Server Components Installation ..... 28
3.2. Configuring the Traffic Monitor Server ..... 37
3.2.1. Checking Processes Autorun ..... 37
3.2.2. Configuring Time Synchronization Server ..... 38
3.2.3. Traffic Monitor Cluster with a Single Analysis Subsystem ..... 39
3.2.4. Server Configuring with Web-Console for “All-in-one” Architecture ..... 40
3.2.4.1. Configuring Addresses of Time Synchronization Server ..... 40
3.2.4.2. Configuring Notifications from Monitoring Subsystem ..... 41
3.2.4.3. Installing the License ..... 41
3.2.5. Traffic Monitor Server Configuring for Distributed Architecture ..... 42
3.2.5.1. Configuring Date and Time Synchronization ..... 42
3.2.5.2. Configuring Connection to the Oracle DBMS Server ..... 43
3.2.5.3. Installing the License ..... 43
3.2.6. Installing and Configuring the Remote Database Management Module ..... 44
3.2.6.1. Installing the Client of the Remote Database Management Module (a Branch Office) ..... 44
3.2.6.2. Installing the Server of the Remote Database Management Module (the Headquarter Office) ..... 46
3.3. Traffic Interceptors Settings ..... 48
3.3.1. Configuring Blind Carbon Copies Forwarding ..... 48
3.3.2. Integration of Traffic Monitor Server with Postfix ..... 49

3.3.3. Configuring Sniffer ... 51
3.3.3.1. Configuring Traffic Monitor Server as Sniffer ... 51
3.3.3.2. Configuring Traffic Monitor Server to Receive Copy of Traffic from Sniffer ... 52
3.3.3.3. Creating Traffic Monitor Cluster ... 53
3.3.4. Installing and configuring the IW ICAP Module ... 54
3.3.4.1. Configuring proxy for Integration with Active Directory ... 55
3.3.4.2. Recommendations for Configuring ICAP for Blue Coat SG Series ... 56
3.3.4.3. Recommendations on SQUID Configuring ... 57
3.3.5. Installing and Configuring the Crawler ... 57
3.3.5.1. Installing Crawler Server and Scanner ... 58
3.3.5.2. Configuring Network Access Rules ... 61
3.4. Configuring the Monitoring Subsystem for Distributed Architecture ... 62
3.4.1. Configuring Time Synchronization Server Address ... 62
3.4.2. Configuring Connection with Servers ... 62
3.4.3. Configuring Activation Thresholds for Load Indicator ... 64
3.4.4. Configuring Services Autorun ... 65
3.4.5. Configuring Notification Engine ... 65
3.4.5.1. Configuring Notifications of Threshold Exceeding for Indicators ... 65
3.4.5.2. Configuring Sending Notification Mails via Postfix ... 66
3.5. Installing the Management Console ... 66
3.6. Configuring the Settings for Analyzing and Monitoring Objects ... 67

CHAPTER 4. UPDATING THE SYSTEM ... 69
4.1. The Order of Updating ... 69
4.2. Creating Database Backup ... 71
4.2.1. Defining the Size of Backup ... 71
4.2.2. Checking the Backup Storage ... 71
4.2.3. Creating Backup Directories ... 72
4.2.4. Creating Recovery Aid Files ... 72
4.2.5. Collecting a List of Files to Backup ... 73
4.2.6. Stopping IWTM System ... 74
4.2.7. Stopping Oracle Database ... 74
4.2.8. Copying Database Files to the Backup Storage ... 74
4.3. Restoring the Database from the Backup ... 74
4.4. Updating a Database Schema ... 75
4.5. Modifying Files of New Version ... 76

CHAPTER 5. UNINSTALLING THE SYSTEM ... 78
5.1. Database Scheme ... 78
5.2. Remote Database Management Module ... 79
5.3. IW ICAP Module ... 79
5.4. Traffic Monitor Server ... 79
5.5. Sniffer ... 80
5.6. Management Console ... 80

APPENDIX 1. TROUBLESHOOTING ... 81

APPENDIX 2. THIRD-PARTY LICENSES ... 82

GLOSSARY ... 83

# INTRODUCTION

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

## Who Should Read this Guide

The guide is intended for users with the following skills:

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

## Guide Structure

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

- *InfoWatch Traffic Monitor Overview (page 7).*

  This chapter contains a general description of the System.

- *Getting Ready to Install (page 10).*

  This chapter describes the hardware and software requirements for running the System and the procedure for installing the System's components.

- *Installing and Configuring the System (page 28).*

  This chapter contains recommendations for installing the System's components and describes the installation process. This chapter also describes rules for obtaining and installing a license key.

- *Updating the System (page 69).*

  This chapter explains how to update the System's components.

- *Uninstalling the System (page 78).*

  This chapter provides information on how to uninstall the components of the System.

- *Troubleshooting (page 81).*

  The appendix describes problems that may arise while the System is being installed and configured and provides troubleshooting tips.

- *Third-Party Licenses (page 82).*

  This appendix contains license agreements for third-party software components of this System.

## Additional Documentation

For more information see the following documents:

- *"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 Traffic Monitor. Administration Guide"*

  This document describes how to administrate the System (database, server part).

- "*InfoWatch Device Monitor. User Guide*"

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

# 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.) | Click the **Start** button. |
| *Italics* | Italics indicate tables, examples and descriptions, specifically the names and values of object attributes. | After running a *Forbidden* query |
| `The Courier New font` | The font indicates file names, program code examples, values of configuration files parameters, examples of settings. | To verify that Traffic Monitor is running use the following commands:<br>`service iw-trafmon status`<br>`service iw-caserv status` |
| `The COURIER NEW font(UPPER CASE)` | This font is used in the descriptions of configuration files and indicates file sections (in square brackets), variables and parameters.<br>When used in database description, it indicates SQL keywords, PL/SQL instructions, data types and privileges | The autorun parameters 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/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 7).*
- InfoWatch Traffic Monitor Standard and InfoWatch Traffic Monitor Enterprise *(i.1.2 on page 7).*
- InfoWatch Traffic Monitor Components *(i.1.3 on page 8).*


## 1.1. InfoWatch Traffic Monitor Features

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

InfoWatch Traffic Monitor Main Features:

- Interception of the SMTP traffic. It's possible to intercept the traffic (or the copy of traffic) relayed by a mail relay server, or the copy of the traffic that passes through the hardware with the CISCO SPAN features support.
- Interception of the HTTP traffic. It's possible to intercept the traffic passing through an ICAP-supporting proxy server, or the copy of the traffic that passes through the CISCO SPAN-enabled equipment.

  > **Note:**
  >
  > When integrated with a Blue Coat proxy server, the system can only intercept the HTTPS traffic if the proxy server processes the HTTPS traffic as the HTTP traffic.

- Intercept a copy of ICQ traffic (OSCAR protocol) transmitted through the equipment supporting the CISCO SPAN features. When ICQ connects through HTTP, the System intercepts ICQ traffic similarly to HTTP traffic.

  > **Warning!**
  >
  > Interception and analysis of the encrypted ICQ traffic, including SSL, is not supported.

- Scanning files in corporate network (network file shares, workstation's local disks, SharePoint 2007 file storage) using Crawler subsystem.
- Analyze the Skype traffic, shadow copies of files and print jobs, traffic which received with HTTPS (analyzing by the System such as HTTP-traffic) protocol, FTP protocol, Jabber client (XMPP protocol) and Mail.Ru Agent (MPP protocol). Interception of such types of data exists 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 Standard and InfoWatch Traffic Monitor Enterprise

Starting with InfoWatch Traffic Monitor 3.5, there are two editions of the System: Traffic Monitor Standard and Traffic Monitor Enterprise.

**InfoWatch Traffic Monitor Standard** has lower software & hardware requirements that Traffic Monitor Enterprise (for more details see i. 2.2 on page 22).

Traffic Monitor Standard also has some limitations of functionality, specifically the following:

- Objects interception is only available in copy mode;
- When specified database object storage size is exceeded, the objects are regularly deleted from the database. You can set protection against such removal.

For more details on these features see *"InfoWatch Traffic Monitor. User Guide"* document.

**InfoWatch Traffic Monitor Enterprise** provides the full set of System features.

# 1.3. InfoWatch Traffic Monitor Components

| InfoWatch Traffic Monitor subsystem | Subsystem features |
|---|---|
| Processing subsystem | Retrieving significant information from intercepted objects, determining attachment formats and transferring retrieved tests to Analysis subsystem. |
| Analysis subsystem | Analysis of text data retrieved from intercepted objects (texts of e-mails, messages, queries as well as text, retrieved from attachments).<br>Consists of the following modules: Text Objects Detection module, Linguistic Analysis module, Digital Fingerprints Detection module |
| Traffic Interception subsystem | Interception and transfer of traffic for processing: objects or copies of objects.<br>Consists of the following modules: Sniffer, Crawler, Device Monitor & DeviceLock Adapter modules |
| Policies Application subsystem | Based on results of Analysis & Processing subsystems operations system is making a decision on violation or non-violation of informational security by intercepted object. It also associates object recipient or sender data with reference records on employees & workstations.<br>Consists of the following modules: Active Directory Integration module, Decision Making module |
| Storage subsystem | Storage of intercepted objects data, analysis and policy application results, and ability of viewing stored information using management console queries. Is a database.<br>Consists of the following modules: Remote Database Management module, Uploading Objects to Database module, System Settings Storage module, Objects Storage module |
| Monitoring subsystem | Feature of remote tracking performance indicators of servers where InfoWatch Traffic Monitor components & related services are installed. Developed based on Nagios software.<br>For more details on how to install and use this subsystem see *«InfoWatch Traffic Monitor. Administration Guide"* |

| InfoWatch Traffic Monitor subsystem | Subsystem features |
|---|---|
| Management Console subsystem | Provisioning graphic user interface used to administrate, configure and use Traffic Monitor.<br><br>Consists of the following modules: User Rights Management module, Configuration Management module, User Analysis module, Reporting module. |

# CHAPTER 2. GETTING READY TO INSTALL

This chapter covers the following topics:

- *System Deployment Schemas (i.2.1 on page. 10).*
- *Hardware and Software Requirements (i.2.2 on page. 22).*

## 2.1. System Deployment Schemas

This section contains description of most general System:

- *Receiving Copies of SMTP Traffic from a Mail Server (i. 2.1.1 on page 10)*
- *SMTP Traffic Interception (i. 2.1.2 on page 12)*
- *Intercepting a Traffic Copy through the Sniffer (i. 2.1.3 on page 13)*
- *Intercepting HTTP Traffic Transmitted over ICAP (i. 2.1.4 on page 17)*
- *Receiving Objects Intercepted by InfoWatch Device Monitor (i. 2.1.5 on page 19)*
- *Receiving Objects Obtained from DeviceLock (i. 2.1.6 on page 21)*
- *Revision of Files from the Corporate Network (i. 2.1.7 on page 22).*

### 2.1.1. Receiving Copies of SMTP Traffic from a Mail Server

The simplest schema. Provides control of outbound data from corporate mail delivery system. Blind carbon copies (BCC) are sent to Traffic Monitor.

**Variant 1.** The System is installed in an office which has no branch offices.

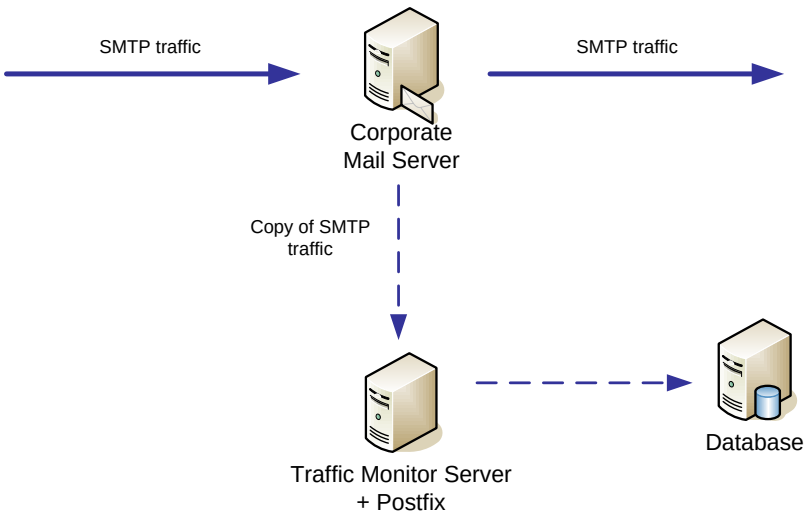



Figure 1. Intercepting a copy of SMTP traffic

**Variant 2.** SMTP-traffic intercepted in branch offices is delivered to the headquarter office over a narrow-band channel. In the headquarter office, SMTP traffic is saved to the database.

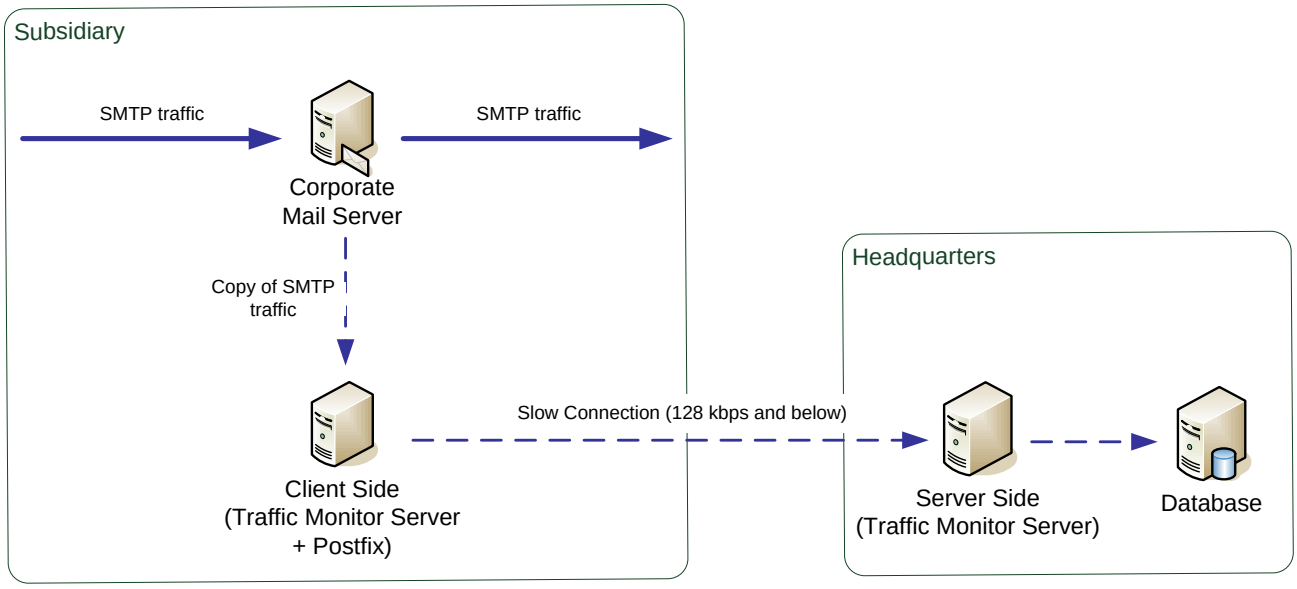



Figure 2. Transmitting a copy of SMTP traffic from a branch office to the headquarter office

The general deployment procedure for both variants is described below. It's only Traffic Monitor Server that is installed differently.

## Step 1. Checking hardware and software requirements to the System

Make sure that the environment where the System will be deployed meets these hardware and software requirements:

- Server part - i. 2.2 on page. 22
- Management Console - i. 2.2.4 on page 27.

## Step 2. Configuring blind carbon copies forwarding

On the mail server configure forwarding of blind carbon copies of SMTP-messages (BCC) to Traffic Monitor server. Example of configuration for Microsoft Exchange Server 2007 and 2010 is given on i. 3.3.1 on page 48.

## Step 3. Installing and configuring the Traffic Monitor server

1. Install and configure Oracle along with Traffic Monitor DB (i. 3.1 on page 28)
2. Install server components of Traffic Monitor (i. 3.1 on page 28).
3. Make sure the `iw_smtpd` process autorun is enabled (i. 3.2.1 on page 37).
4. Install license for SMTP-traffic interceptor (i. 3.2.5.3 on page 43).
5. Configure the integration of Traffic Monitor server with Postfix (i.3.3.2 on page 49).
6. If the System is deployed according to Figure 2 (data from the branch offices to the headquarter is transferred over narrow-band channels, not less than 128 Kb/s)
   - In each branch office, where you need to intercept SMTP traffic, install the client part of the remote database management module to the computer with Traffic Monitor server (see i. 3.2.6.1 on page 44).
   - In the headquarter office install the server part of the remote database management module to the computer with Traffic Monitor server (see i. 3.2.6.2 on page 46).

## Step 4. Installing the Management Console

1. Install the Management Console (i.3.5 on page 57).

2. In Management Console configure the settings for analyzing and processing objects on the Traffic Monitor Server (preparing a configuration and uploading it to configuration server, creating database of reference documents, advanced settings).
3. In the object processing script, set the **Copy** transport mode for *Smtp* interceptor.

For more information on configuring these settings, see i. 3.6 on page 67 and *"InfoWatch Traffic Monitor. User Guide"* document.

## 2.1.2. SMTP Traffic Interception

The schema provides control of outbound data from corporate mail delivery system. Traffic Monitor server is used as relay-server (blocking mode).

**Variant 1**. The System is installed in an office which has no branch offices.

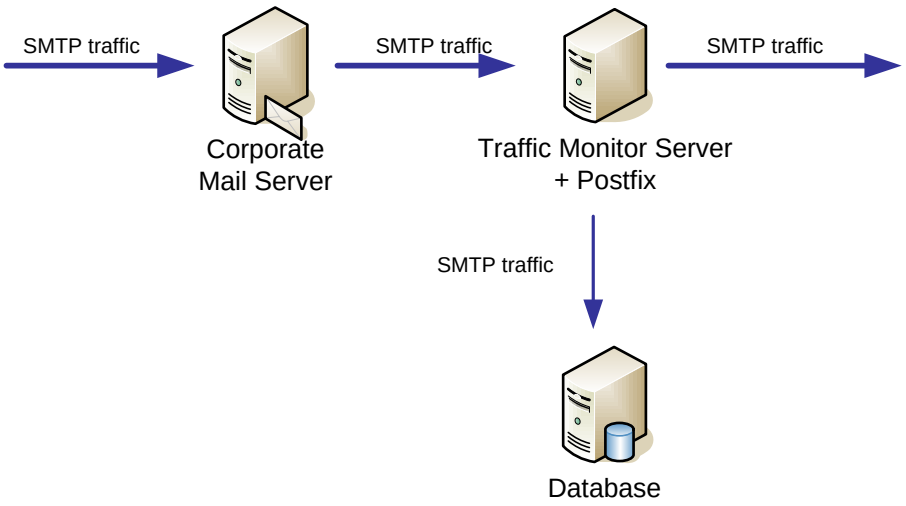



Figure 3. SMTP traffic interception

**Variant 2**. SMTP-traffic intercepted in branch offices is delivered to the headquarter office over a narrow-band channel. In the headquarter office, SMTP traffic is saved to the database.

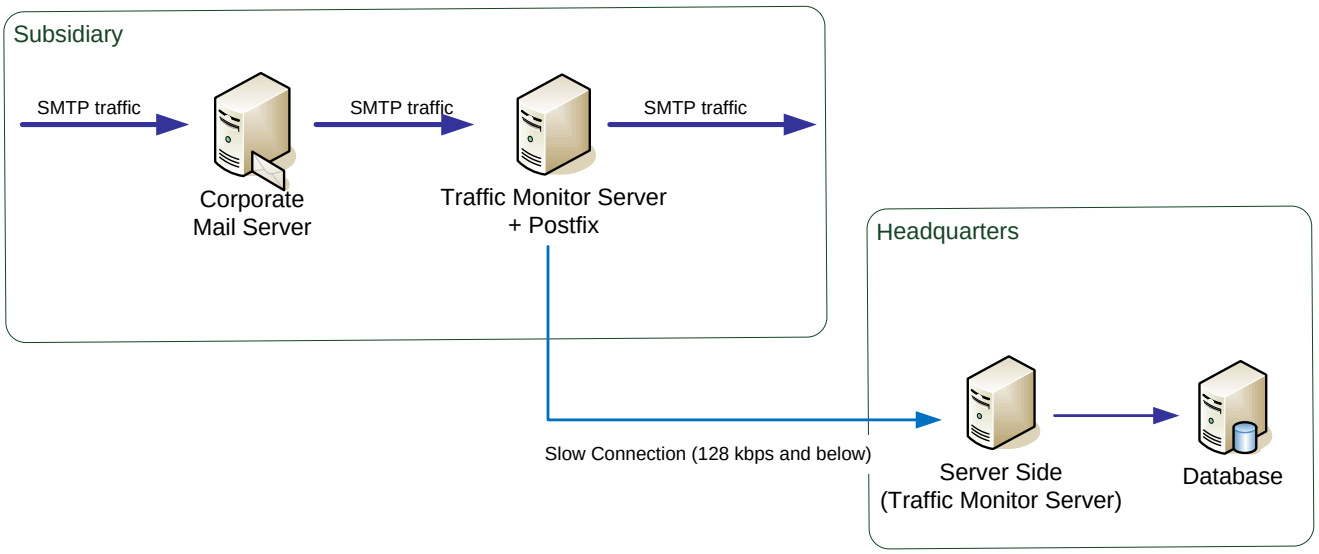



Figure 4. Transmitting SMTP traffic from a branch office to the headquarter office

The general deployment procedure for both variants is described below. It's only Traffic Monitor Server that is installed differently.

### Step 1. Checking hardware and software requirements to the System

Make sure that the environment where the System will be deployed meets these hardware and software requirements:

- Server part - i. 2.2 on page. 22
- Management Console - i. 2.2.4 on page 27.

### Step 2. Configuring Postfix settings

Postfix mail server should be installed prior Traffic Monitor server installation. See the pricedure description in i. 3.3.2 on page 49.

### Step 3. Installing and configuring the Traffic Monitor server

1. Install and configure Oracle along with Traffic Monitor DB schema using **IWDBX** kickstart option (i. 3.1 on page 28)
2. Install server components of Traffic Monitor (i. 3.1 on page 28).
3. Install license for SMTP-traffic interceptor (i.3.2.5.3 on page 43).
4. Make sure `iw_smtpd` and `iw_deliverd` processes autorun is enabled (i. 3.2.1 on page 37).
5. Configure the integration of Traffic Monitor server with Postfix (i.3.3.2 on page 49).
6. If the System is deployed according to Figure 4 (data from the branch offices to the headquarter is transferred over narrow-band channels, not less than 128 Kb/s)
   - In each branch office, where you need to intercept SMTP traffic, install the client part of the remote database management module to the computer with Traffic Monitor server (see i. 3.2.6.1 on page 44).
   - In the headquarter office install the server part of the remote database management module to the computer with Traffic Monitor server (see i. 3.2.6.2 on page 46).

### Step 4. Installing the Management Console

1. Install the Management Console (i.3.5 on page 57).
2. In Management console configure the settings for analyzing and processing objects on the Traffic Monitor Server (preparing a configuration and uploading it to configuration server, creating database of reference documents, advanced settings).
3. In the object processing script, set the ***Normal*** or ***Transparent*** transport mode for *Smtp* interceptor.

For more information on configuring these settings, see i. 3.6 on page 67 and *"InfoWatch Traffic Monitor. User Guide"* document.

## 2.1.3. Intercepting a Traffic Copy through the Sniffer

Traffic (SMTP, HTTP, ICQ) goes through a CISCO switch that has a SPAN port. A copy of traffic is delivered to the Sniffer. Sniffer delivers the copy of traffic to Traffic Monitor Server for analysis and uploading to the database.

To improve performance you can create clusters of Traffic Monitor servers. One cluster can contain up to 2 instances of Traffic Monitor Server. It is not advised to use more than 3 clusters.

> **Warning!**
>
> When you use a cluster, the speed of the network connection between the Sniffer and the Traffic Monitor Server must be twice as fast as the speed of delivery of traffic to the Sniffer.

Several variants of deployment are possible.

**Variant 1.** A copy of traffic is intercepted and analyzed on the same computer (see Figure 5). A cluster is not created. The System will be installed in an office which has no branch offices.

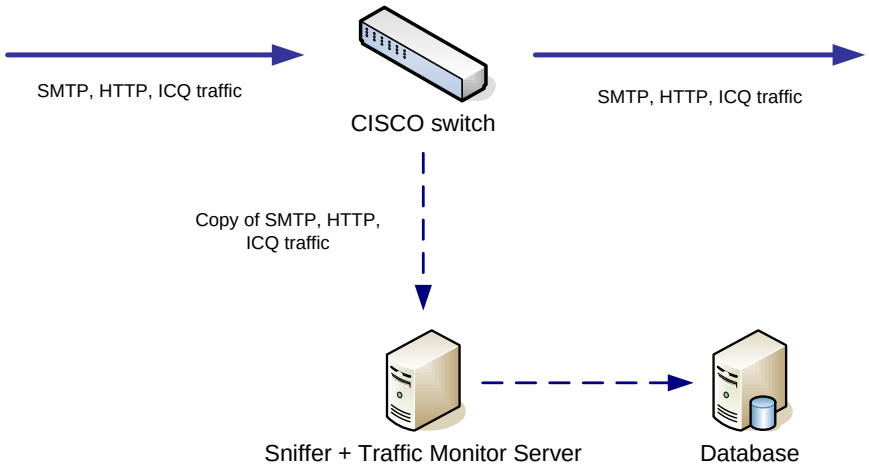



Figure 5. Intercepting and analyzing traffic on the same computer

**Variant 2.** A copy of traffic is intercepted and analyzed on different computers; clusters are not used (see Figure 6). The System will be installed in an office which has no branch offices.

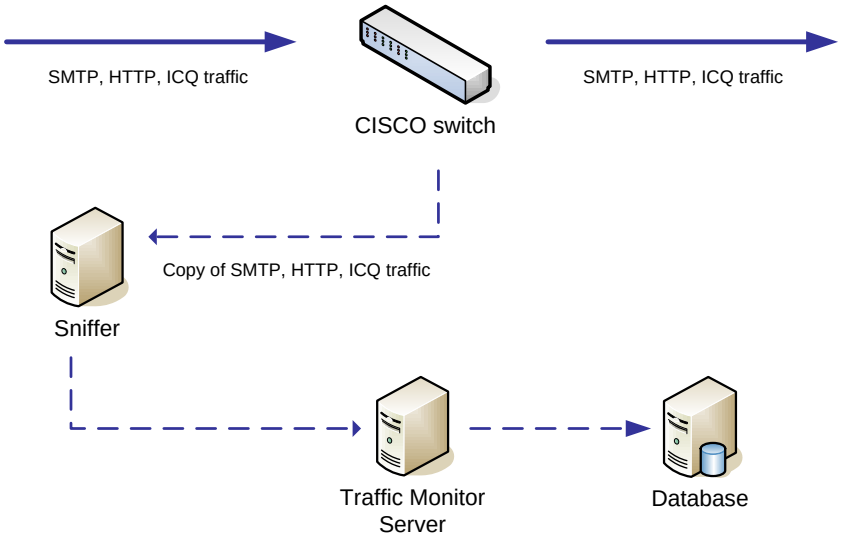



Figure 6. Intercepting and analyzing a copy of traffic on different computers

**Variant 3.** A copy of traffic is intercepted and analyzed on different computers. To improve performance, a cluster was created containing 2 instances of Traffic Monitor Server (see Figure 7). The System will be installed in an office which has no branch offices.

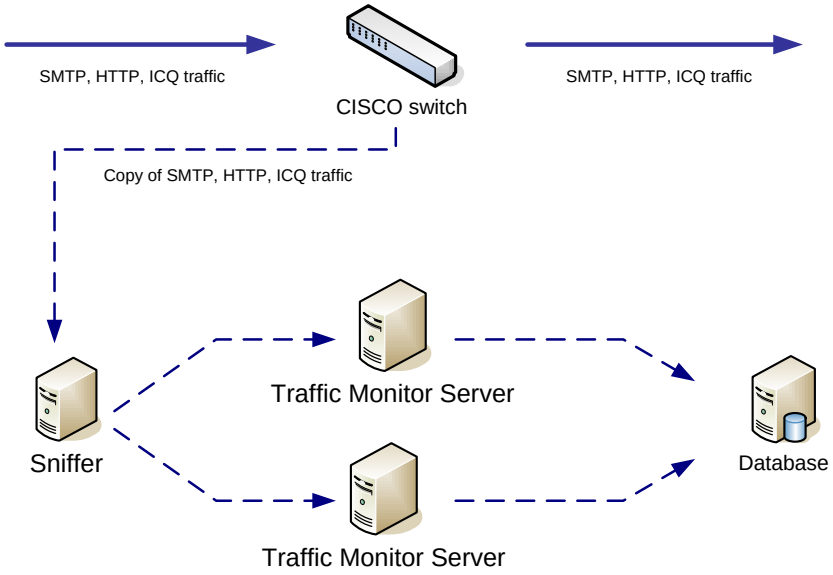



Figure 7. A cluster containing 2 instances of Traffic Monitor Server

**Variant 4.** A copy of traffic is intercepted and analyzed on different computers. A cluster is not created. The copy of traffic is delivered from a branch office to the headquarter office over a narrow-band channel. In the headquarter office, a copy of traffic is loaded to the database (see Figure 8).

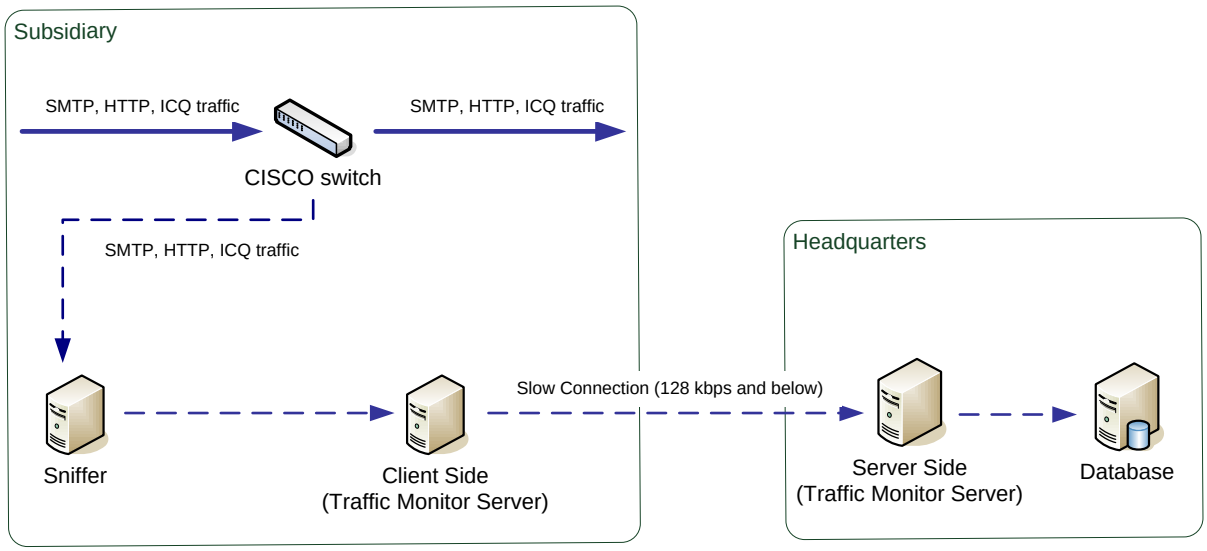



Figure 8. Intercepting a copy of traffic with the Sniffer and uploading it to a remote database

The general deployment order for all of these variants is described below. It's only Traffic Monitor Server that is installed differently.

## Step 1. Checking hardware and software requirements to the System

Make sure that the environment where the System will be deployed meets these hardware and software requirements:

- Server part - i. 2.2 on page. 22
- Sniffer - i. 2.2.1 on page 24
- Management Console - i. 2.2.4 on page 27

## Step 2. Installing and configuring the Traffic Monitor server and Sniffer

**Variant 1** (see Figure 5). Traffic is intercepted and analyzed on the same computer. Increased productivity is not required (clusters are not needed). The System will be installed in an office which has no branch offices:

1. Install and configure Oracle along with Traffic Monitor DB schema using **IWDBX** kickstart option (i. 3.1 on page 28)
2. Install server components of Traffic Monitor using **IWTMX** kickstart option (i. 3.1 on page 28).
3. Configure Traffic Monitor Server as Sniffer (i. 3.3.3.1 on page 51, variant 2).
4. Configure parameters for receiving the traffic copy from the Sniffer (i. 3.3.3.2 on page 52)
5. Install licenses for required interceptors (i.3.2.5.3 on page 43).

**Variant 2** (see Figure 6). Traffic is intercepted and analyzed on different computers. Increased productivity is not required (clusters are not needed). The System will be installed in an office which has no branch offices:

1. On one computer:
   - Install Traffic Monitor server using **IWTMX** kickstart option (i. 3.1 on page 28)
   - Configure Traffic Monitor server as Sniffer (i. 3.3.3.1 on page 51, variant 1).
2. On second computer:
   - Install server components of Traffic Monitor using **IWTMX** kickstart option (i. 3.1 on page 28).
   - Install licenses for required interceptors (i.3.2.5.3 on page 43).
   - Configure parameters for receiving the traffic copy from the Sniffer (i. 3.3.3.2 on page 52).
3. On third computer:
   - Install and configure Oracle along with Traffic Monitor DB schema using **IWDBX** kickstart option (i. 3.1 on page 28)

**Variant 3** (see Figure 7). Traffic is intercepted and analyzed on different computers. The System's productivity must be increased (clusters are needed). The System will be installed in an office which has no branch offices:

1. Install and configure Oracle DBMS Server with Traffic Monitor database schema (i. 3.1 on page 28, **IWDBX** option).
2. On the computer for Sniffer:
   - Install Traffic Monitor server using **IWTMX** kickstart option (i. 3.1 on page 28)
   - Configure Traffic Monitor server as Sniffer (i. 3.3.3.1 on page 51, variant 1).
3. On the other computer, install an instance of Traffic Monitor server cluster:

Install Traffic Monitor server using **IWTMX** kickstart option (i. 3.1 on page 28).

Install licenses for required interceptors (i.3.2.5.3 on page 43).

Configure parameters for receiving copy of traffic from Sniffer (i. 3.3.3.2 on page 52).

Specify cluster parameters (i.3.3.3.3 on page 52).

4. Repeat i. 3 to add another instance of Traffic Monitor Server to the cluster.

> **Warning!**
>
> If you use Digital Fingerprints Detection module, only one Analysis subsystem may function within the System.
>
> If the System contains multiple instances of Traffic Monitor Server, you must configure Analysis subsystem in one Traffic Monitor server instance only (see i. 3.2.3 on page 39).

**Variant 4** (see Figure 8). Traffic is intercepted and analyzed on different computers. Increased productivity is not required (clusters are not needed). The System will be installed in the headquarter office and its branch offices.

*In each branch office, where you need to intercept a copy of traffic:*

- On the computer for Sniffer:
  1. Install Traffic Monitor server using **IWTMX** kickstart option (i. 3.1 on page 28)

2. Configure Traffic Monitor server as Sniffer (i. 3.3.3.1 on page 51, variant 1).

- On the computer for branch Traffic Monitor server:
  1. Install Traffic Monitor server using **IWTMX** kickstart option (i. 3.1 on page 28).
  2. Install licenses for required interceptors (i.3.2.5.3 on page 43).
  3. Install and configure the client part of remote DB interaction module (i. 3.2.6.1 on page 44).
  4. Configure parameters for receiving copy of traffic from Sniffer (i. 3.3.3.2 on page 52).

*In the headquarter office:*

1. Install and configure Oracle along with Traffic Monitor DB schema using **IWDBX** kickstart option (i. 3.1 on page 28)
2. Install server components of Traffic Monitor using **IWTMX** kickstart option (i. 3.1 on page 28).
3. Install licenses for required interceptors (i.3.2.5.3 on page 43).
4. Install and configure the server part of remote DB interaction module (see i. 3.2.6.2 on page 46).

### Step 3. Installing the Management Console

1. Install the Management Console (i.3.5 on page 57).
2. In Management Console configure the settings for analyzing and processing objects on the Traffic Monitor Server (preparing a configuration and uploading it to configuration server, creating database of reference documents, advanced settings).
3. In the object processing script, set the ***Copy*** transport mode for interceptors receiving a copy of traffic from Sniffer (*Smtp, Http, Icq*).

For more information on configuring these settings, see i. 3.6 on page 67 and *"InfoWatch Traffic Monitor. User Guide"* document.

# 2.1.4. Intercepting HTTP Traffic Transmitted over ICAP

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

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

In this scheme Traffic Monitor server requires installation of special IW ICAP module.

The scheme supports *Normal* or *Transparent* transport mode. In *Normal* transport mode analysis results will be returned to SQUID proxy after processing in Traffic Monitor: permission or ban for further transfer of intercepted data.

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

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

**Variant 1.** The System is installed in an office which has no branch offices (see Figure 9).

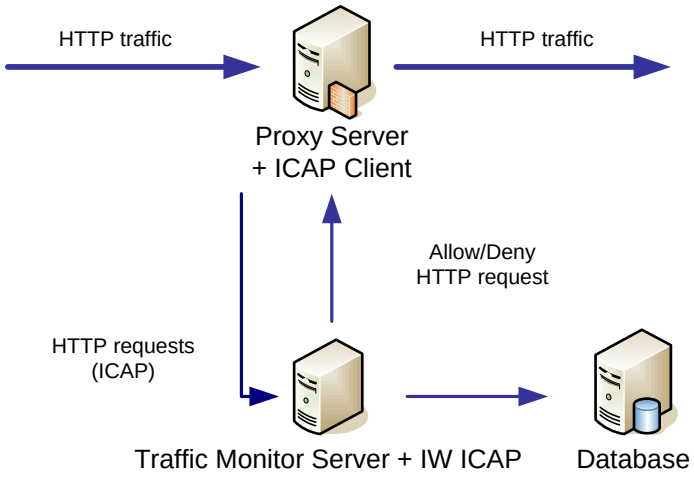



Figure 9. Intercepting HTTP Traffic Transmitted over ICAP

**Variant 2**. HTTP traffic is intercepted, analyzed and filtered in a branch office. The intercepted HTTP traffic is delivered to the headquarter office over a narrow-band channel. In the headquarter office, a copy of traffic is loaded to the database (see Figure 10).

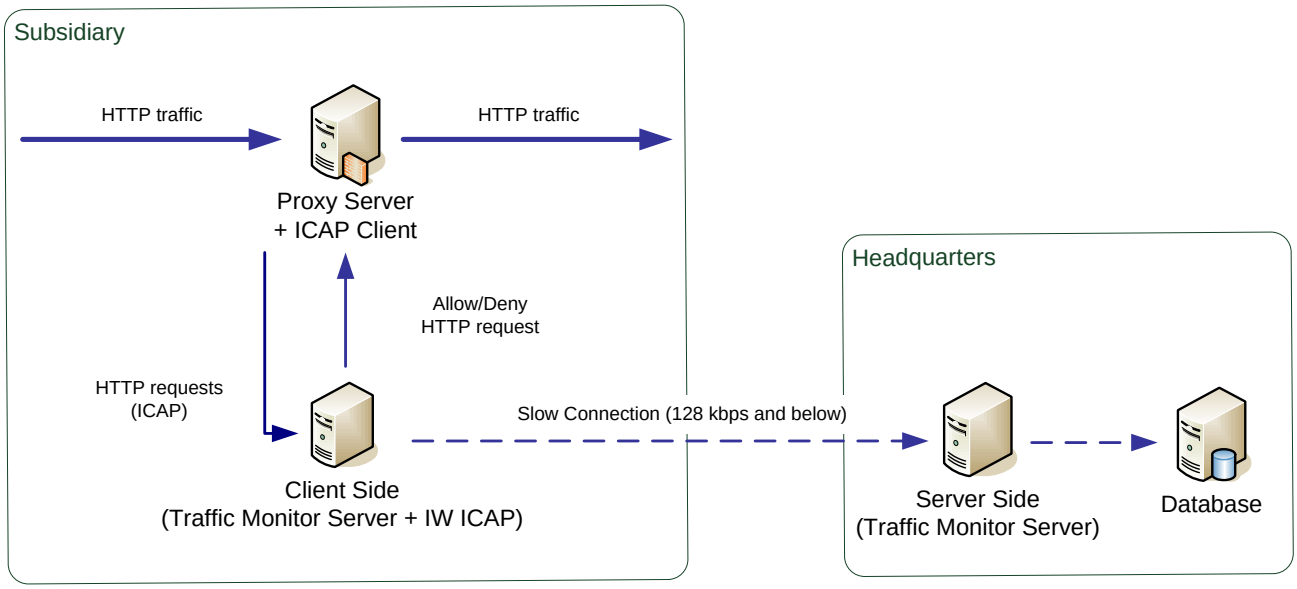



Figure 10. Intercepting HTTP traffic in a branch office and uploading the traffic to a remote database

The general deployment order for all of these variants is described below. It's only Traffic Monitor Server that is installed differently.

## Step 1. Checking hardware and software requirements to the System

Make sure that the environment where the System will be deployed meets these hardware and software requirements:

- Server part - i. 2.2 on page. 22.
- IW ICAP Module - i.2.2.2 on page 24
- Management Console - i. 2.2.4 on page 27

## Step 2. Installing and configuring the Traffic Monitor server

To set the system according to **Variant 1**, proceed as follows:

1. Install server components of Traffic Monitor (i. 3.1 on page 28).
2. Install license for HTTP-traffic interceptor (i.3.2.5.3 on page 43).
3. Install and configure Oracle along with Traffic Monitor DB schema using **IWDBX** kickstart option (i. 3.1 on page 28)
4. If the server performs interception, install and configure the IW ICAP module (see i. 3.3.4 on page 54).

To set the system according to **Variant 2**, proceed as follows:

1. Install server components of Traffic Monitor in headquarter office (i. 3.1 on page 28).
2. In the headquarter office install the server part of the remote database management module to the computer with Traffic Monitor server (see i. 3.2.6.2 on page 46).
3. Install and configure Oracle along with Traffic Monitor DB schema using **IWDBX** kickstart option (i. 3.1 on page 28)
4. Install server components of Traffic Monitor in branch office (i. 3.1 on page 28).
5. In each branch office, where you need to intercept SMTP traffic, install the client part of the remote database management module to the computer with Traffic Monitor server (see i. 3.2.6.1 on page 44).
6. If the server performs interception, install and configure the IW ICAP module (see i. 3.3.4 on page 54).

### Step 3. Installing the Management Console

1. Install the Management Console (i.3.5 on page 57).
2. In Management console configure the settings for analyzing and processing objects on the Traffic Monitor Server (preparing a configuration and uploading it to configuration server, creating database of reference documents, advanced settings).
3. In the object processing script, set the ***Normal*** or ***Transparent*** transport mode for *Http* interceptor.

For more information on configuring these settings, see i. 3.6 on page 67 and *"InfoWatch Traffic Monitor. User Guide"* document.

# 2.1.5. Receiving Objects Intercepted by InfoWatch Device Monitor

Objects (shadow copies of files, print jobs) intercepted by InfoWatch Device Monitor are delivered to Traffic Monitor server for analysis and uploading to the database.

**Variant 1.** The System is installed in an office which has no branch offices (see Figure 11).

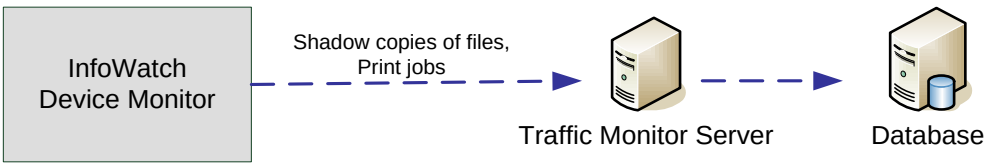



Figure 11. Objects are received from InfoWatch Device Monitor

**Variant 2.** InfoWatch Device Monitor system is installed in a branch office. Objects, intercepted by InfoWatch Device Monitor, are passed to Traffic Monitor Server for analysis. After that, the objects are delivered to the headquarter office. In the headquarter office objects are saved to database (see Figure 12).

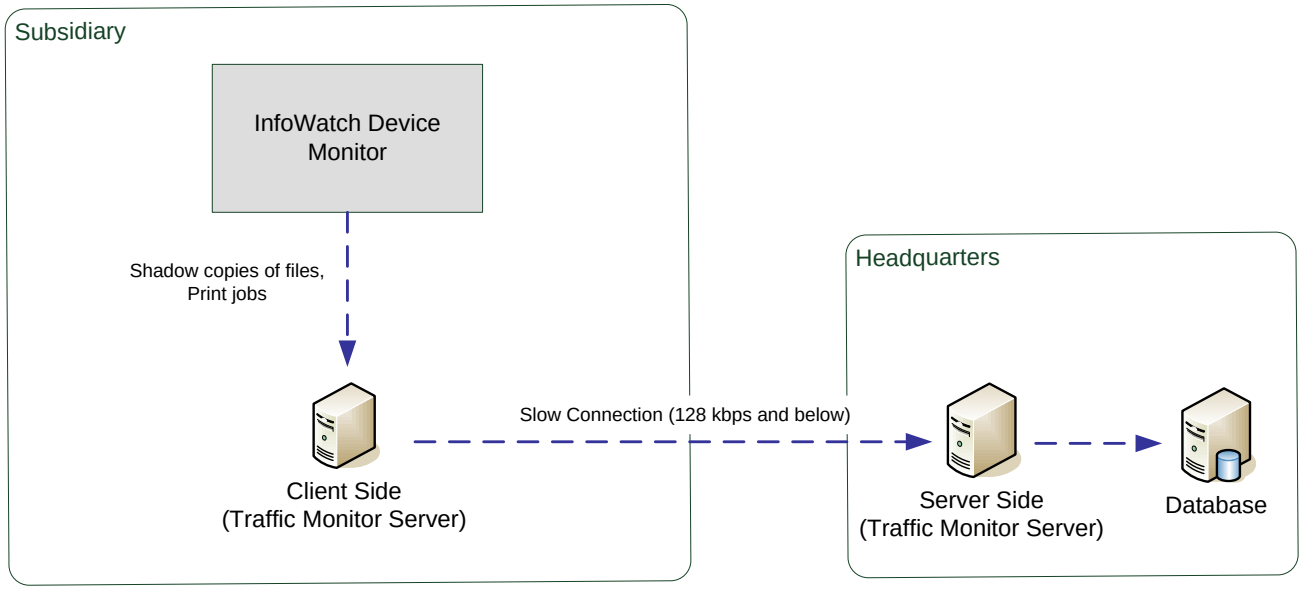



Figure 12. Receiving objects from InfoWatch Device Monitor and uploading the objects to a remote database

The general deployment order for all of these variants is described below. It's only Traffic Monitor Server that is installed differently.

## Step 1. Checking hardware and software requirements to the System

Make sure that the environment where the System will be deployed meets these hardware and software requirements:

- Server part - i. 2.2 on page. 22.
- Management Console - i. 2.2.4 on page 27.

## Step 2. Installing and configuring the Traffic Monitor server

To set the system according to **Variant 1**, proceed as follows:

1. Install server components of Traffic Monitor (i. 3.1 on page 28).
2. Install and configure Oracle along with Traffic Monitor DB schema (i. 3.1 on page 28)
3. Install Device Monitor and configure it to send shadow copies to Traffic Monitor (see "*InfoWatch Device Monitor. User Guide"* document).

To set the system according to **Variant 2**, proceed as follows:

1. Install server components of Traffic Monitor (i. 3.1 on page 28).
2. Install server components of Traffic Monitor in headquarter office (i. 3.1 on page 28).
3. In the headquarter office install the server part of the remote database management module to the computer with Traffic Monitor server (see i. 3.2.6.2 on page 46).
4. Install and configure Oracle along with Traffic Monitor DB schema (i. 3.1 on page 28)
5. Install server components of Traffic Monitor in branch office (i. 3.1 on page 28).
6. In each branch office, where you need to intercept SMTP traffic, install the client part of the remote database management module to the computer with Traffic Monitor server (see i. 3.2.6.1 on page 44).
7. Install Device Monitor and configure it to send shadow copies to Traffic Monitor (see "*InfoWatch Device Monitor. User Guide"* document).

### Step 3. Installing the Management Console

1. Install the Management Console (i. 3.5 on page 66).
2. In Management Console configure the settings for analyzing and processing objects on the Traffic Monitor Server (preparing a configuration and uploading it to configuration server, creating database of reference documents, advanced settings).
3. In the object processing script, set the *Copy* transport mode for *Device* interceptor.

For more information on configuring these settings, see *"InfoWatch Traffic Monitor. User Guide"* document.

The information on installation and configuring of the InfoWatch Device Monitor system see i. 3.6 on page 67 and i. 3.6 on page 67 and "*InfoWatch Device Monitor. User Guide*" document.

## 2.1.6. Receiving Objects Obtained from DeviceLock

Objects intercepted by the DeviceLock system are passed to Traffic Monitor Server for analysis and uploading to the database.

**Variant 1.** The System is installed in an office which has no branch offices (see Figure 13).

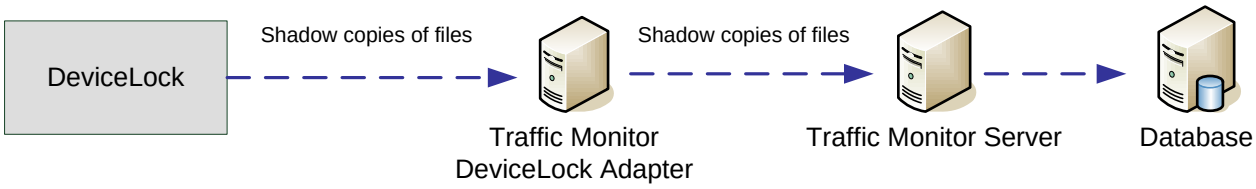



Figure 13. Objects are received from DeviceLock

**Variant 2.** DeviceLock system is installed in a branch office. Objects, intercepted by DeviceLock, are passed to Traffic Monitor Server for analysis. After that, the objects are delivered to the headquarter office. In the headquarter office objects are saved to database (see Figure 14).

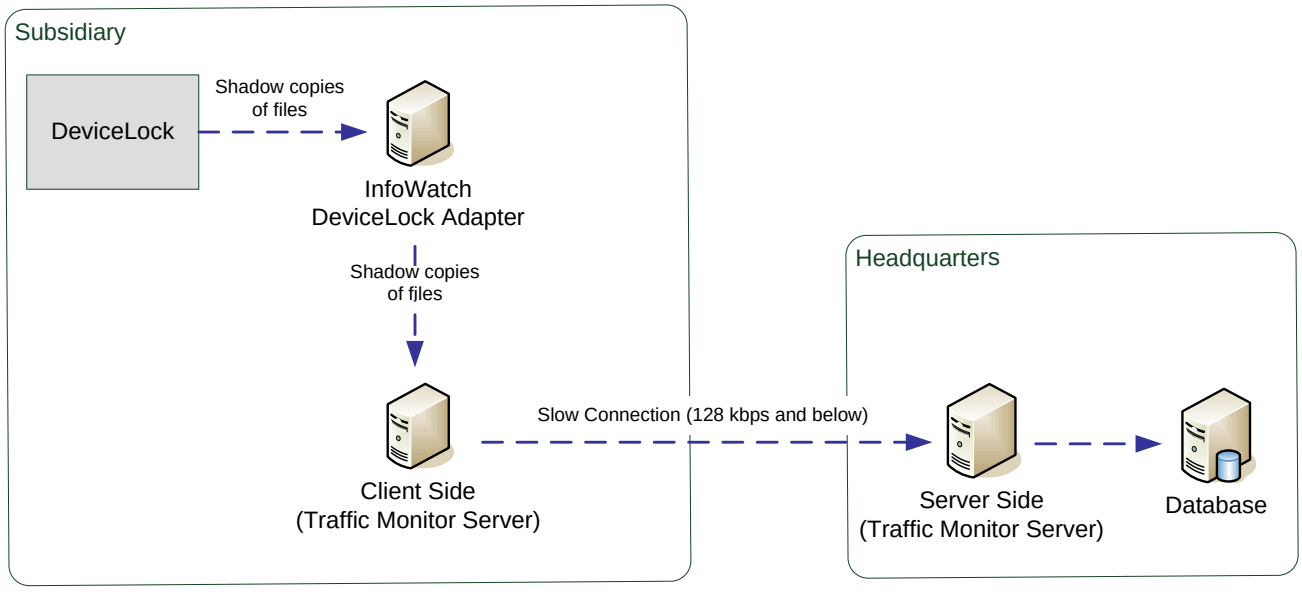



Figure 14. Receiving objects from DeviceLock in a branch office and uploading the objects to a remote database

The general deployment order for all of these variants is described below. It's only Traffic Monitor Server that is installed differently.

### Step 1. Checking hardware and software requirements to the System

Make sure that the environment where the System will be deployed meets these hardware and software requirements:

- Server part - i. 2.2 on page. 22.
- InfoWatch DeviceLock Adapter - see in "*InfoWatch DeviceLock Adapter. Installation and Configuration Guide*" document
- Management Console - i. 2.2.4 on page 27.

### Step 2. Installing and configuring the Traffic Monitor server

To set the system according to **Variant 1**, proceed as follows:

1. At each server that should receive objects, install and configure InfoWatch DeviceLock Adapter. Recommendations are provided in:

*"InfoWatch DeviceLock Adapter. Installation and Configuration Guide"*

*"InfoWatch DeviceLock Adapter. Administration Guide"*

2. Install server components of Traffic Monitor (i. 3.1 on page 28).
3. Install and configure Oracle along with Traffic Monitor DB schema (i. 3.1 on page 28)

To set the system according to **Variant 2**, proceed as follows:

1. Install server components of Traffic Monitor in headquarter office (i. 3.1 on page 28).
2. In the headquarter office install the server part of the remote database management module to the computer with Traffic Monitor server (see i. 3.2.6.2 on page 46).
3. Install and configure Oracle along with Traffic Monitor DB schema in the headquarter office (i. 3.1 on page 28)
4. Install server components of Traffic Monitor in branch office (i. 3.1 on page 28).
5. In each branch office, where you need to intercept SMTP traffic, install the client part of the remote database management module to the computer with Traffic Monitor server (see i. 3.2.6.1 on page 44).
6. At each server that should receive objects, install and configure InfoWatch DeviceLock Adapter. Recommendations are provided in:
   - "InfoWatch DeviceLock Adapter. Installation and Configuration Guide"
   - "InfoWatch DeviceLock Adapter. Administration Guide"

### Step 3. Installing the Management Console

1. Install the Management Console (i.3.5 on page 57).
2. In Management Console configure the settings for analyzing and processing objects on the Traffic Monitor Server (preparing a configuration and uploading it to configuration server, creating database of reference documents, advanced settings).
3. In the object processing script, set the *Copy* transport mode for *Dla* interceptor.

For more information on configuring these settings, see i. 3.6 on page 67 and *"InfoWatch Traffic Monitor. User Guide"* document.

# 2.1.7. Revision of Files from the Corporate Network

Crawler interceptor allows reviewing files located in the corporate network:

- Scanning network folders which are remote accessible using SMB protocol.
- Scanning local disks of workstations under Windows OS.
- Scanning documents stored in Microsoft SharePoint 2007.

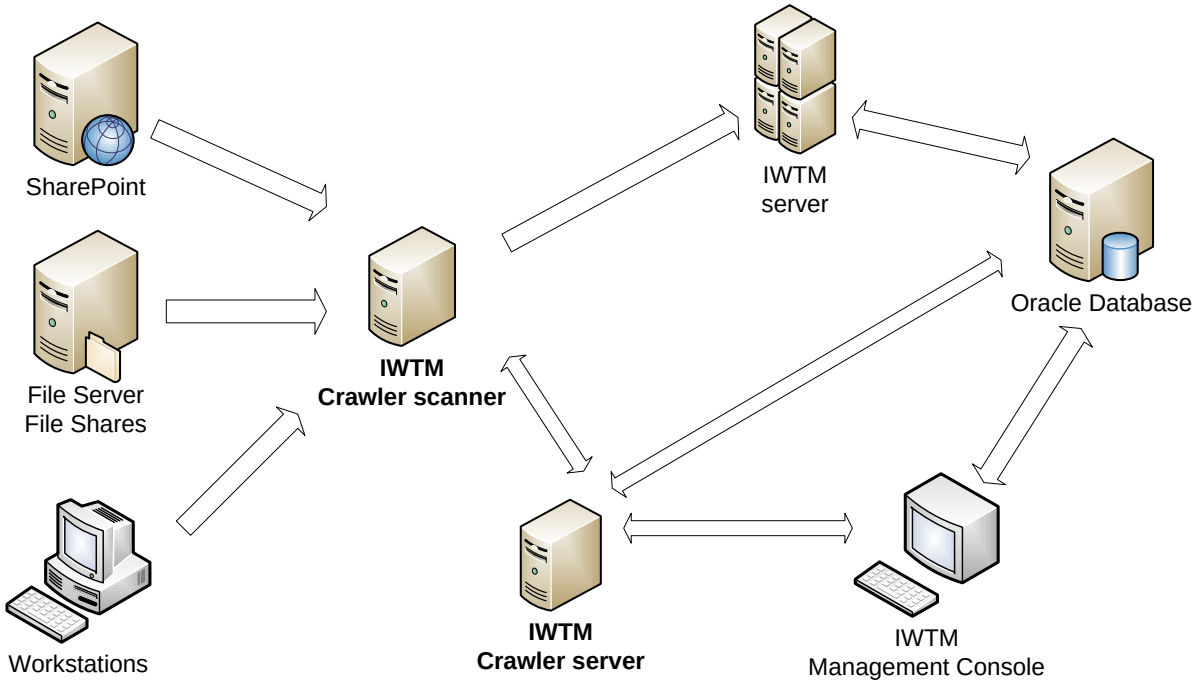



Figure 15. Scanning corporate network with IW Crawler

InfoWatch Crawler performs scanning in the following order:

1. Workstations, workstation groups, file servers or file storage listed in scanning task are reviewed if they have any available data.
2. Every found file satisfying search conditions is copied to the temporary directory of the scanner.
3. File is sent to InfoWatch Traffic Monitor server for analysis, where it is processed according to actual object processing script.

The general deployment procedure for the system with Crawler interceptor is given below.

## Step 1. Checking hardware and software requirements to the System

Make sure that the environment where the System will be deployed meets these hardware and software requirements:

- Server part - i. 2.2 on page. 22.
- Computer for Crawler server and computer for Crawler scanner - i. 2.2.3 on page 26
- Management Console - i. 2.2.4 on page 27.

## Step 2. Installing and configuring the Traffic Monitor server

Install server components of Traffic Monitor (i. 3.1 on page 28).

## Step 3. Installing and configuring the Crawler

Install and configure Crawler (i.3.3.5 on page 57).

## Step 4. Installing the Management Console

1. Install the Management Console (i. 3.5 on page 57).
2. In Management console configure the settings for analyzing and processing objects on the Traffic Monitor Server (preparing a configuration and uploading it to configuration server, creating database of reference documents, advanced settings).
3. Configure Management Console connection with Crawler server.

4. Check general parameters of Crawler scanner operation.
5. In the object processing script, set the *Copy* transport mode for *Crawler* interceptor. Make sure that there is a `CheckCrawlerPolicy(root)` funcion in the object processing script.

For more information on configuring these settings, see i. 3.6 on page 67 and *"InfoWatch Traffic Monitor. User Guide"* document.

# 2.2. Hardware and Software Requirements

Hardware configuration requirements of server and DBMS for **Traffic Monitor Enterprise** are defined based on selected deployment scheme and parameters of the network where the System is installed. For this reason equipment specification is determined individually for each case.

> **Warning!**
>
> For Traffic Monitor Enterprise the Traffic Monitor server and Oracle DBMS Server must be installed on different computers. In this case you shouldn't install or run applications (especially server applications), or use this computer as a file server on the computer acting as Oracle DBMS server.

To improve System performance you need to arrange as much individual physical I/O devices (volumes) as possible. This means decrease of data volume, but support of parallel I/O operations will be added as well as improved database bandwidth.

**Example:**

Initial 12-disk storage array may be arranged as follows:

- Three RAID 5 arrays containing 3 physical disks each – for daily tablespaces; in this case each file system should be located in a separate array;
- One RAID 1 array, containing 2 physical disks – for system files, main tablespace and temporary data files;
- One disk used for hot swap.

It is recommended to use the following parameters for caching setup: write cache – 80%, read cache – 20%.

**Traffic Monitor Standard** Oracle DBMS may be installed on the same computer as Traffic Monitor server. In this case software and hardware should comply with the requirements to Traffic Monitor server.

Traffic Monitor Standard typical server configuration is described based on aggregate inbound and outbound traffic speed of 100 Mbit/s (with limitation of at most 50 Mbit/s per traffic type) for utilized traffic volume:

- Server: support configurations, allowed for the Red Hat Enterprise Linux Server 6: see https://hardware.redhat.com/.

  HP ProLiant DL 320 G6 Server is recommended.
- Processor: Intel® Xeon® E5540 2.53 GHz.
- RAM: DDR3 2 GB + 1 GB per interceptor.
- Hard drive: SAS, 2 x 300 GB (10,000 rpm) with RAID 0.

Remote DB interaction module should be installed on the same computer as Traffic Monitor server: there is no additional requirement.

The requirements for other components are covered in following sections:

- Sniffer (i. 2.2.1 on page 25)
- IW ICAP Module (i. 2.2.2 on page 25)
- IW Crawler (i. 2.2.3 on page 26)
- Management Console (i. 2.2.4 on page 27)

# 2.2.1. Sniffer

### Network Equipment Requirements

Sniffer may receive a copy of traffic from the switch that supports SPAN (recommended model – Cisco Catalyst 2960 Series).

After switch is installed, configure SPAN port to operate in RX/TX mode as described in technical documentation of the switch.

### Hardware requirements

*Minimum requirements for 50 Mbit/s traffic:*

- Processor: 2.66 GHz Intel Core 2 DUO E6750
- RAM: 2 GB.

*The standard configuration of the Sniffer when the aggregate speed of upstream and downstream is 50 Mbit/s:*

- Server: support configurations, allowed for the Red Hat Enterprise Linux Server 6: see https://hardware.redhat.com/.

  The recommended configuration is HP ProLiant DL 360 G7 Server.
- Processor: dual core Intel® Xeon® E5502 1.87GHz.
- RAM: 4 GB DDR3
- Hard drive: SAS 300 GB (10,000 rpm).

*Network adapter requirements:*

| General requirements | Recommended network adapters |
|---|---|
| NAPI and *Promiscuous mode* support. | Intel Corporation 82540EM Gigabit Ethernet Controller<br>Broadcom Corporation NetXtreme II BCM5708 1GB |
| Gigabit Ethernet support | Intel PRO/1000 GT network adapters are allowed. |

The Sniffer must have at least two network adapters:

- A network adapter to receive a copy of traffic from one SPAN port of the CISCO switch. If traffic is received from multiple SPAN ports (and ports can be configured both on the same switch and on different switches), then a separate network adapter is required for each of the SPAN ports.
- A network adapter to interact with other network objects. Specifically, this adapter is required to send traffic to Traffic Monitor server or interact with the database (if Sniffer and Traffic Monitor server are installed on the same computer).

# 2.2.2. IW ICAP Module

If the IW ICAP module is integrated with the System, HTTP requests are transmitted over a proxy server. An ICAP client is required to send HTTP requests to Traffic Monitor server over ICAP protocol. The System supports ICAP clients integrated with the proxy server.

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

The following proxy servers are supported:

- SQUID no lower than 3.1.7 with ICAP support enabled.
- Cisco IronPort S10.
- Blue Coat SG Series with ICAP license. Some models which are currently produced by Blue Coat Systems are supported. The manufacturer constantly updates the product range. Therefore, prior to using a

specific model of Blue Coat Proxy SG, contact InfoWatch technical support service to check whether or not this model is compatible with the IW ICAP module.

> **Note:**
>
> If interception of HTTPS traffic is required, configure proxy settings to process HTTPS traffic and send it to InfoWatch Traffic Monitor server as HTTP traffic.

See the documentation for the selected proxy server for installation and configuration steps. Recommendations for configuring proxy servers are covered in 3.3.4 on page. 54.

ICAP server is a part of ICAP integration module. The module is installed on the same computer as Traffic Monitor Server (see requirements in i.2.2 on page. 22). There are no special requirements for hardware and software of the module.

# 2.2.3. IW Crawler

Requirements for the using InfoWatch Traffic Monitor server instance:

- minimum 6 Gb RAM
- in `/usr/local/infowatch/tm3/etc/tm.conf` file, `[AUTO_RESTART]` section, autorestart of `iw_expressd` process should be enabled:

```
autorestart = On
```

The computer, to which the **Crawler server** will be installed, should meet the following requirements:

- Processor: at least 2 cores
- RAM: 200 Mb free
- Hard drive: 1 Gb free
- OS:
  - Microsoft Windows XP / Vista / 7 / 8
  - Microsoft Windows Server 2003 / 2008 / 2012
- Microsoft .Net Framework 4.0

The computer, to which the **Crawler scanner** will be installed, should meet the following requirements:

- Processor: at least 2 cores
- RAM: 200 Mb free
- Hard drive: at least 10 Gb free for temporary storing files copied from reviewed resources
- OS:
  - Microsoft Windows XP / Vista / 7 / 8
  - Microsoft Windows Server 2003 / 2008 / 2012
- Microsoft .Net Framework 4.0
- Bandwidth of the network channel between Crawler scanner and Traffic Monitor server should be not less than bandwidth between Crawler scanner and scanned network nodes (workstations and file servers).

> **Warning!**
>
> We recommend to deploy a computer where Crawler scanner works so that it was located in the network segment maximally near to scanned segments. The distance from Crawler scanner to scanned objects can significantly increase network load.

**Warning!**

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.

# 2.2.4. Management Console

### Hardware requirements

| Hardware | Minimum hardware required | Recommended hardware |
|---|---|---|
| Processor | 1.7 GHz Celeron or faster | 3 GHz Pentium IV or faster |
| RAM | 512 Mb | 1 GB |
| Hard drive | 1 GB of free space | 1 GB of free space |

### Software requirements

| Software | Requirements |
|---|---|
| Operating system | Microsoft Windows XP Service Pack 3<br>Microsoft Windows Vista<br>Microsoft Windows 7 |
| .Net Framework platform | Microsoft .Net Framework 4.0 |

# CHAPTER 3. INSTALLING AND CONFIGURING THE SYSTEM

The order of installation the InfoWatch Traffic Monitor System is defined by deployment schema selected considering intercepting traffic type, intercepting mode (filtering the traffic or receiving traffic copy), and by network infrastructure (see i.2.1 on page. 10).

The following sections describe the System installation and configuring:

- *Server Components Installation (i. 3.1 on page 28)*
- *Configuring the Traffic Monitor Server (i. 3.2 on page 37)*
- *Traffic Interceptors Settings (i. 3.3 on page 48)*
- *Configuring the Monitoring Subsystem for Distributed Architecture (i. 3.4 on page 62)*
- *Installing the Management Console (i. 3.5 on page 66)*

## 3.1. Server Components Installation

The installation of InfoWatch Traffic Monitor Server components is carried out by means of the kickstart installer. The kickstart installer is launched automatically from the distributor disk:

1. Select the installation mode:

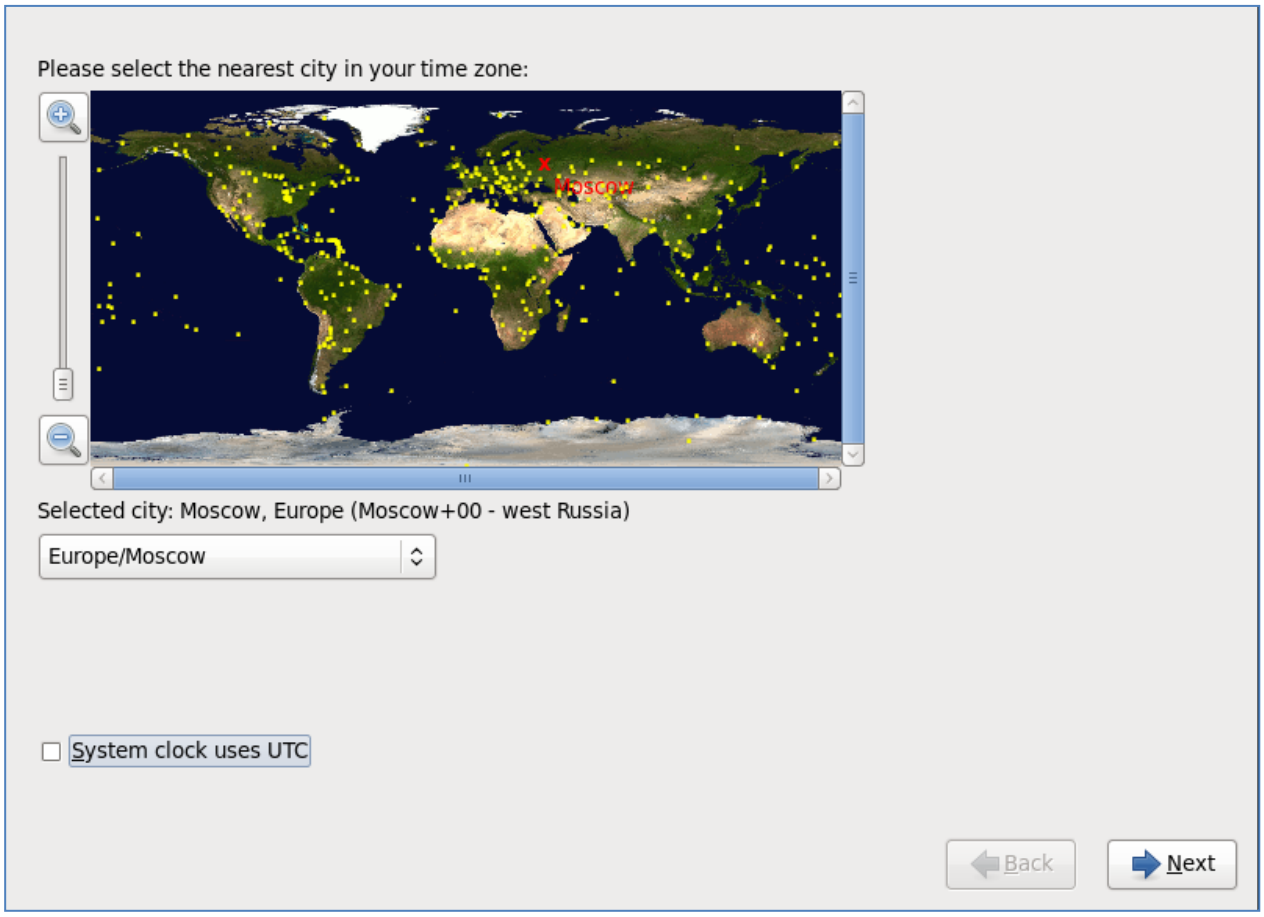



Considering the server´s purpose (Traffic Monitor server; database server, or the installation of both components on a single server) and System editing (full version - Traffic Monitor Enterprise, or the lightweight ver-

sion of Traffic Monitor Standard: for more details on the differences see i.1.2 on page 7), select the applicable setting mode.

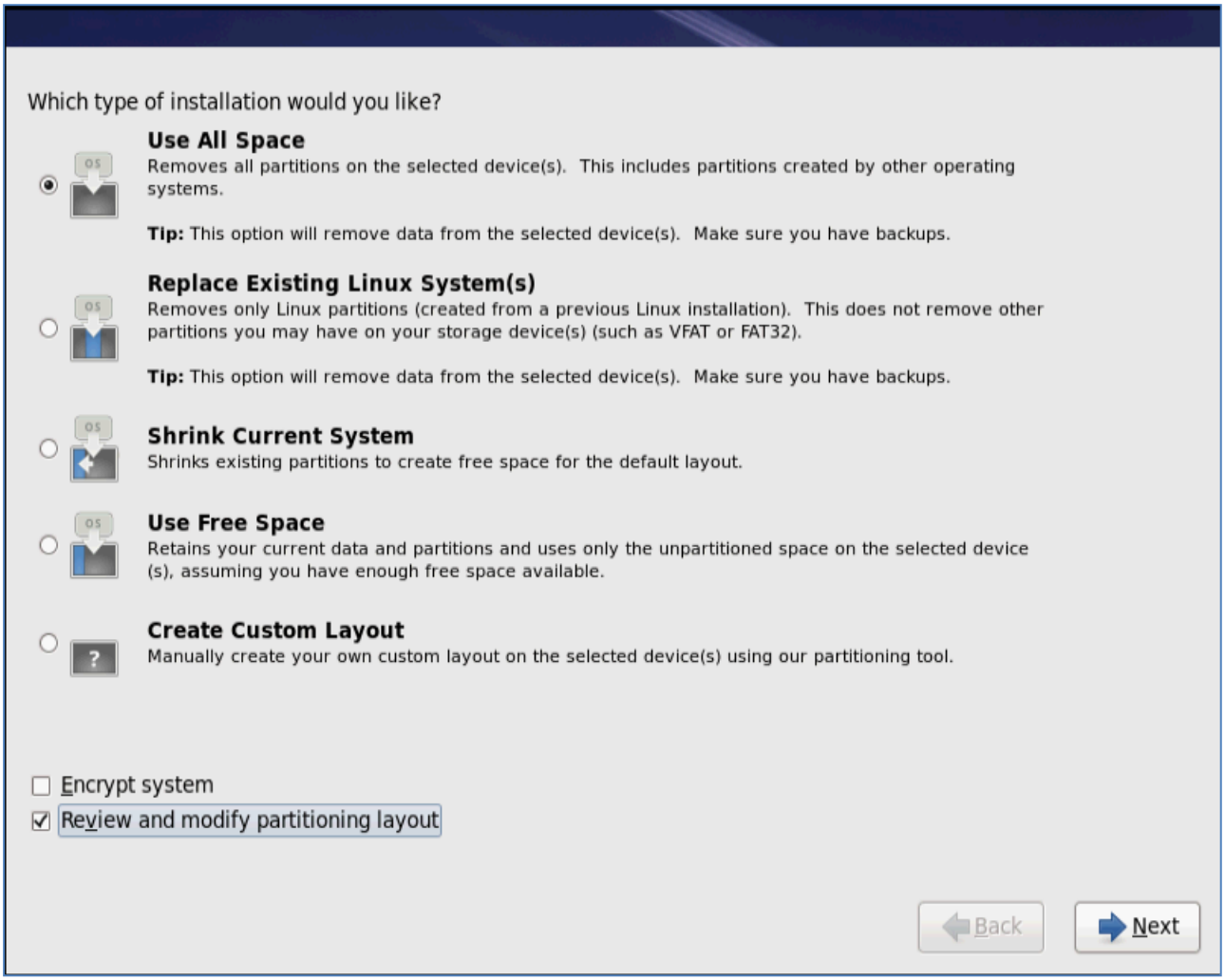
| **Installation mode** | **Kickstart launch key** | **Procedure of installation and configuration components by the installer** |
|---|---|---|
| Installing the Traffic Monitor Server on a separate computer | IWTMX | 1. Installing OS Linux<br>2. Installing RPM packages of IWTM server<br>3. Installing Monitoring subsystem |
| Installing the Oracle DBMS Server with a Traffic Monitor database scheme to a separate computer | IWDBX | 1. Installing OS Linux<br>2. Configuring network interface<br>3. Installing and configuring Oracle DBMS<br>4. Installing IW Traffic Monitor database schema<br>5. Installing Monitoring subsystem |
| "All-in-one" mode: all components are installed to a single server.<br>**Warning!** Not recommended for industrial use in company traffic. To be used for pilot installations. | IWALLX | 1. Installing OS Linux<br>2. Configuring network interface<br>3. Installing and configuring Oracle DBMS<br>4. Installing IW Traffic Monitor database schema<br>5. Installing RPM packages of IWTM server<br>6. Installing Monitoring subsystem |
| Installing InfoWatch Traffic Monitor Standard. | IWTMSX | 1. Installing OS Linux<br>2. Configuring network interface<br>3. Installing and configuring Oracle Standard DBMS<br>4. Installing IW Traffic Monitor database schema<br>5. Installing RPM packages of IWTM server<br>6. Installing Monitoring subsystem |

2. Specify server timezone.




3. Select the procedure of disk space partitioning:

- **Use All Space** - all the partitions of the selected drive will be removed and default layout will be created.
- **Replace Existing Linux System** - Linux partitions will be removed from the selected drive and default layout will be created.
- **Shrink Current System** – existing partitions will be compressed to free the space.
- **Use Free Space** - default layout is created only within the free space of the selected drive.
- **Create Custom Layout** - manual layout of the selected drive (recommended for experienced administrators only).

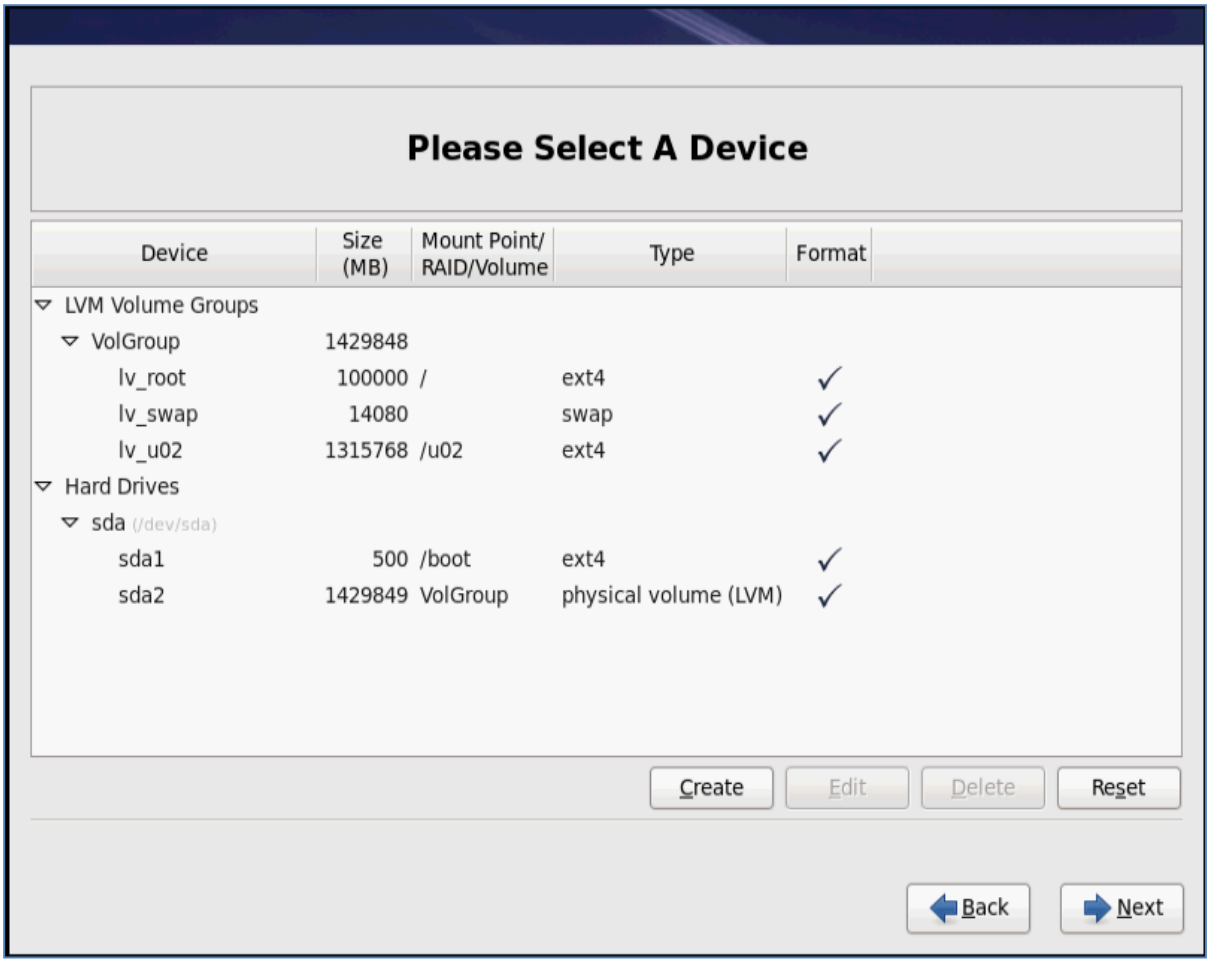



To ensure optimal performance of the server, choose the first option (**Use All Space**), select **Review and modify partitioning layout** and press **Next**.

4. Change the partitions in the following way:

| Installation mode | root | /uo2 | SWAP |
|---|---|---|---|
| IWTMX (only TM server) | at least 200 GB | not needed | leave default size |
| IWDBX (only database server) | at least 100 GB | the rest free space | |
| IWALLX (All-in-One) | at least 100 GB | the rest free space | |
| IWTMSX (TM Standard) | at least 60 GB | 400 GB enough | |

> **Warning!**
>
> For systems that should proceed a significant data volume, you should consider the recommendations for storage array organization: see i.2.2 on page. 22.




To change **root** partition parameters from the default to the recommended ones:

a) Choose **lv_root** partition and click **Edit**.

b) In the **Size** field specify a recommended value (for example, for IWALLX - 10000 Mb).

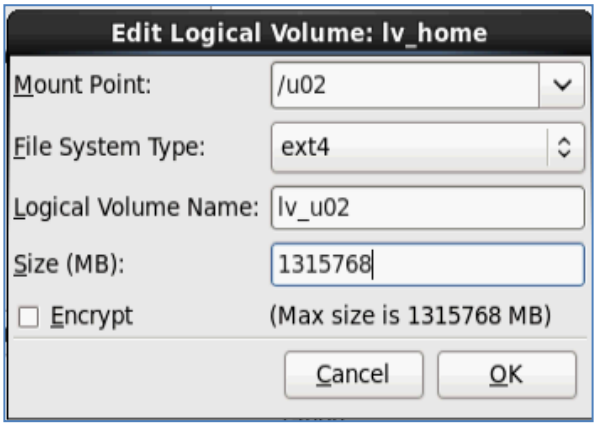
c) Click **OK**.

To set **/u02** partition parameters:

a) Choose **lv_ home** partition and click **Edit**.

b) Specify the following parameters:

- **Mount Point** - **/u02**
- **Logical Volume Name** – **lv_u02**
- If database server in installing, select **ext3** file system type
- **Size** – all available volume (see **Max size**)

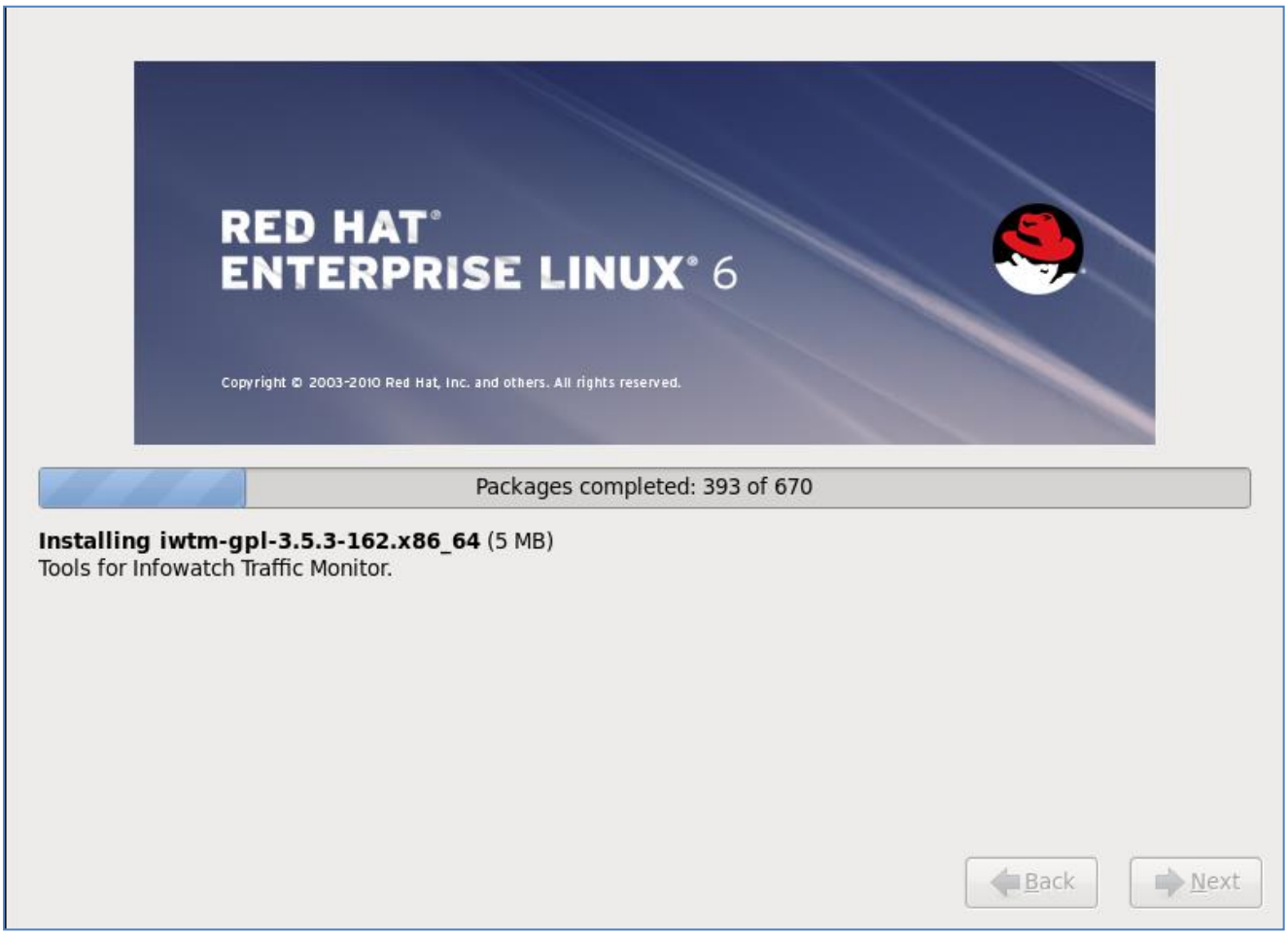



c) Click **OK**.

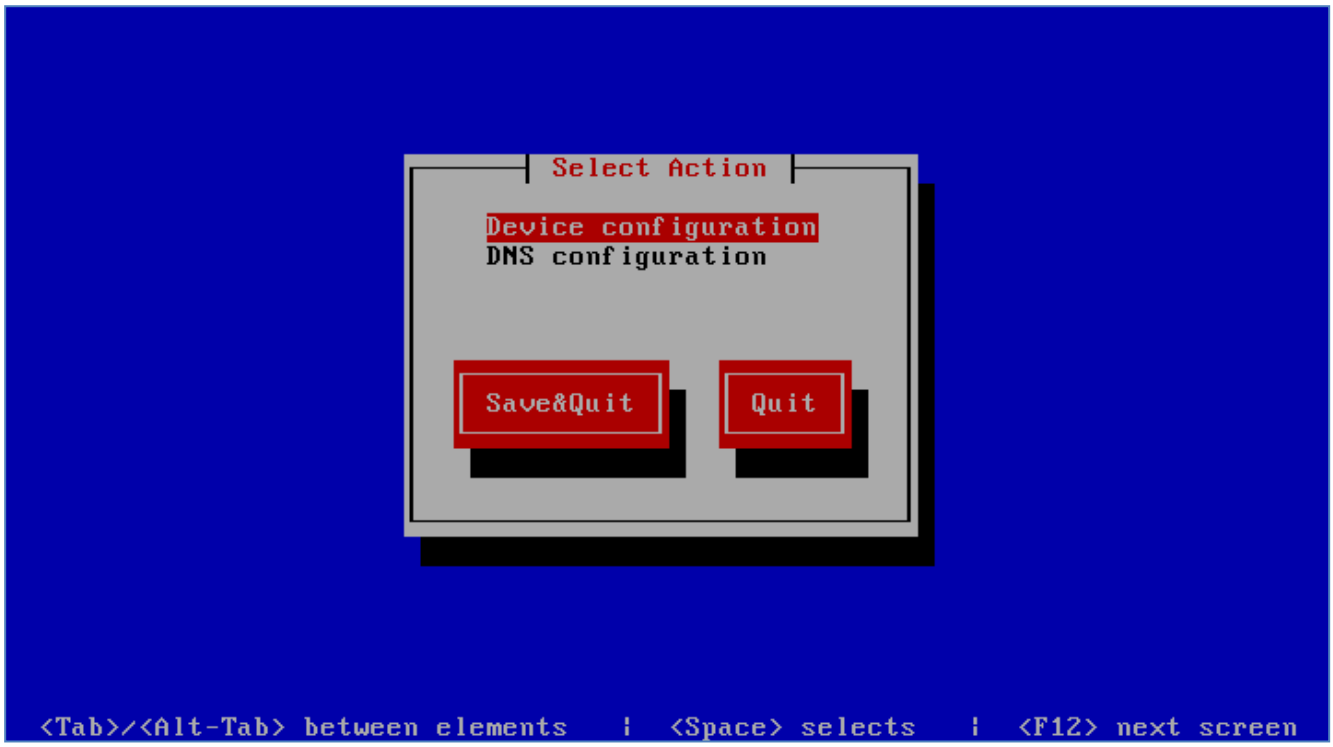
To delete **/u02** partition, choose **lv_ home** and click **Delete**

After specifying all the disk partition parameters, click **Next**.

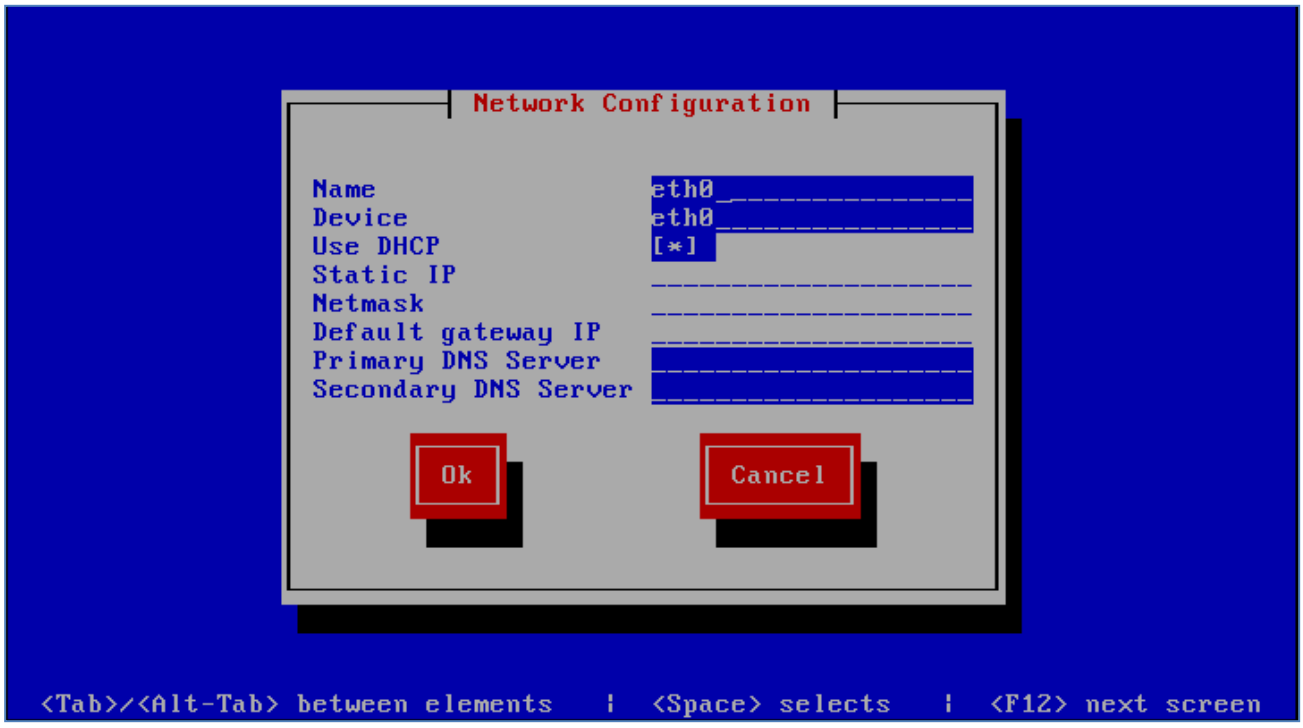
5. First the partitioning process, then operating system installation will begin. The status bar for both procedures will be displayed on the screen.



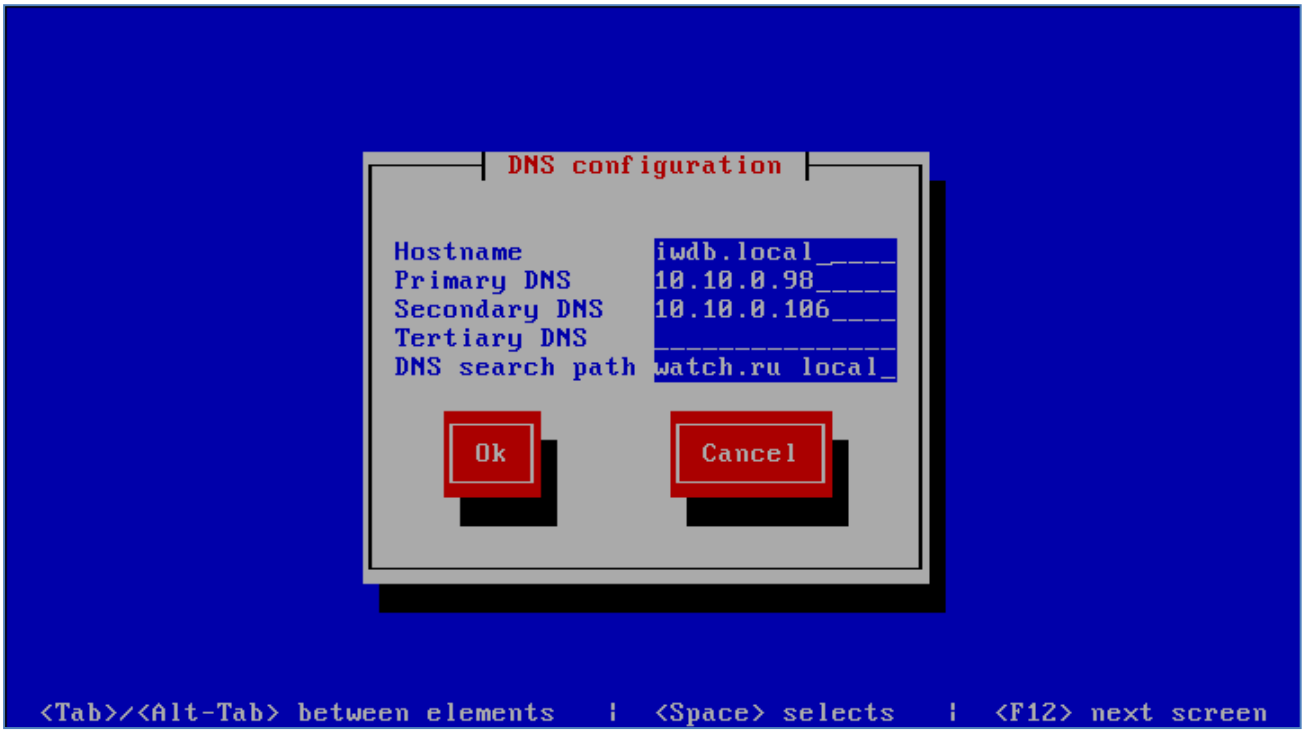

After a reboot at the end of the installation of the operating system, you will be prompted to configure the network settings.




6. To configure the network card parameters:
   a. Select **Device configuration**.
   b. Select the network interface **eth0**.
   c. Make shure **Use DHCP** parameter is selected. Change other parameters if needed, then click **OK**.
   d. Press **Save** to save the applied settings.




7. To setup the DNS configuration, click **DNS configuration** and specify the required parameters of the server´s network configuration. Then click **OK**.




8. Verify the selected network settings. If the configuration is wrong, enter **N** and select the correct parameters (see steps 6 and 7). If the configuration is correct, enter **Y** to confirm.

```
eth0: NIC Link is Up 10000 Mbps
 done.
                                                          [  OK  ]
/etc/hosts:
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
10.60.21.30      iwdb.local iwdb

DNS configuration (/etc/resolv.conf):
; generated by /sbin/dhclient-script
search infowatch.ru local
nameserver 10.10.0.98
nameserver 10.10.0.106

IP configuration (ip addr show):
1: lo:
    inet 127.0.0.1/8 scope host lo
2: eth0:
    inet 10.60.21.30/16 brd 10.60.255.255 scope global eth0

IP ROUTE configuration (ip route show):
169.254.0.0/16 dev eth0  scope link  metric 1002
10.60.0.0/16 dev eth0  proto kernel  scope link  src 10.60.21.30
default via 10.60.0.1 dev eth0
HOSTNAME: iwdb.local
Are the network settings correct (Y/n)? _
```

9. If the stand-alone Traffic Monitor server is installing (**IWTMX** option), specify database server IP address (**Enter IWDB IP adress**). Then `$ORACLE_HOME/network/admin/tnsnames.ora` file will be customized to work with specified address.

10. Prior to database scheme installation (if **IWDBX**, **IWALLX** or **IWTMSX** mode is selected) you will be prompted to configure scheme language (**Language for IWDB Scheme**). This will be a language of preset entities such as Classifier, Reports, Queries and “Default” script. To choose English select **en**.

The following accounts are created:

| Account | Name | Password |
|---|---|---|
| Linux Superuser´s account (root) | root | xxXX1234 |
| Oracle Administrator | sys | xxXX1234 |
| | system | xxXX1234 |
| Oracle: Database Scheme Owner | iwtm | xxXX1234 |
| Oracle: a Linux user of DBMS, whose account will be used to load intercepted objects into the database | iwtm_linux | xxXX1234 |
| Management Console: User Administrator | administrator | xxXX1234 |
| Management Console: Security Officer | officer | xxXX1234 |
| Linux user for launching Oracle server procedures | oracle | xxXX1234 |
| Linux user for launching Traffic Monitor server procedures | iwtm | No password |
| Oracle DBMS client installation´s owner group including `iwtm` and `oracle` users | oinstall | - |

> **Warning!**
>
> Please change the password for `root` and `oracle` account immediately after installation is completed.

Server will receive the hostname as follows:

```
iwdb-xxxxxxxxxxxxxxx.local
```

where:

- xxxxxxxxxxxxxxx is a Serial Number of a server
- instead of **iwdb** (installation type – database) can be **iwtm** (Traffic Monitor server), **iwall** (all-in-one) or **iwts** (Traffic Monitor Standard).

To complete server configuration you should do the following:

- Specify time synchronization server (see i. 3.3 on page 3.3 or i. 3.2.4.1 at page 40)
- Configure sending notifications from Monitoring subsystem (see i. 3.2.4.2 at page 41 (for «all-in-one» architecture) or i. 3.4 on page 62, step 2 (for distributed architecture) )
- If needed, install commercial InfoWatch Traffic Monitor license. Just after installation there is a trial license valid within 30 days from the date of installation. Detailed information on licenses see in i. 3.2.5.3 on page 43.
- Make sure that monitoring indicators have  **Normal** state. Detailed information on Monitoring subsystem see in «*InfoWatch Traffic Monitor. Administration Guide*» document.
- Configure Traffic Monitor server as described in i. 3.2 on page 37
- Configure interceptors (see i. 3.3 on page 3.3) required to operate the system in accordance with the selected deployment scheme (see i. 2.1 on page. 10).

# 3.2. Configuring the Traffic Monitor Server

Configuring the Traffic Monitor server installed by means of kickstart installation program, can consist of the following procedures:

- *Checking Processes Autorun (i. 3.2.1 on page 37)*
- *Configuring Time Synchronization Server (i. 3.2.2 on page 38)*
- *Traffic Monitor Cluster with a Single Analysis Subsystem (i. 3.2.3 on page 39)*
- *Server Configuring with Web-Console for "All-in-one" Architecture (i. 3.2.4 on page 40)*
- *Traffic Monitor Server Configuring for Distributed Architecture (i. 3.2.5 on page 42)*
- *Installing and Configuring the Remote Database Management Module (i. 3.2.6 on page 44)*

## 3.2.1. Checking Processes Autorun

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

| Process name | Cases when the process autorun is required | Autorun is enabled by default |
|---|---|---|
| iw_smtpd | Intercepting SMTP traffic in the mail relay mode | Yes |
| iw_messed | Intercepting SMTP traffic in any mode (relay or Sniffer) | Yes |
| iw_deliverd | Only if the system performs delivery of blocked SMTP traffic (*Normal* transport mode) | No |
| iw_sniffer | On a computer where Sniffer is installed | Yes |
| iw_proxy SMTP<br>iw_proxy HTTP<br>iw_proxy ICQ | Intercepting a copy of SMTP, HTTP, or ICQ traffic with Sniffer Enable autorun only for required interceptors | Enabled for the HTTP and ICQ interceptors |
| iw_icap | Intercepting and processing HTTP traffic, delivered to the Traffic Monitor server through the ICAP protocol.<br>This process runs if the IW ICAP module is installed | Yes |
| iw_expressd | Receiving objects intercepted by the InfoWatch Device Monitor system.<br>Receiving objects intercepted by the DeviceLock system. | Yes |
| iw_qmover_server | In the headquarter office. If objects from a branch office will be received.<br>The process appears if the server part of the remote database management module is installed. | Yes |
| iw_qmover_client | In a branch office. If objects are transferred to the headquarters´ Traffic Monitor server to be loaded into the database.<br>The process appears if the client part of the remote database management module is installed. | Yes |

| Process name | Cases when the process autorun is required | Autorun is enabled by default |
|---|---|---|
| iw_dbloader<br>iw_updater<br>iw_warpd | Autorun must be enabled regardless of the implementation scheme | Yes |
| iw_adlibitum | Only on a single instance of the Traffic Monitor server | Yes |

**Warning!**

Disable autorun of unlicensed processes, responsible for intercepting traffic (**iw_smtpd**, **iw_proxy**, **iw_expressd**, **iw_icap**). It reduces the number of records in the log.

**To enable/disable process autorun:**

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

   ```
   service iw-trafmon stop
   ```

2. In `[AUTO_RESTART]` section of `/usr/local/infowatch/tm3/etc/tm.conf` file complete the settings:

To enable the autorun of a process, set this value in the process section: `autorestart = On`

Example (enabling `iw_sniffer`):

```
iw_sniffer:
autorestart = On
```

To disable the autorun of a process, set this value in the process section: `autorestart = Off`

3. Start Traffic Monitor Server processes:

   ```
   service iw-trafmon start
   ```

# 3.2.2. Configuring Time Synchronization Server

For correct server operation you should configure date, time and time synchronization (NTPD).

1. Change system date and time to the necessary ones by running 'date' command with options. For example, for date 11 Sep 2012 13:30:

   ```
   date 09111330
   ```

2. Check current time at the server using 'date' command:

   ```
   date
   ```

   The result should be as following:

   ```
   Tue Sep 11 13:31:13 MSK 2012
   ```

3. Synchronize hardware and system clocks by copying the system time for configuring hardware clocks using the following command:

   ```
   hwclock --systohc
   ```

4. To check that system and hardware time set properly run 'hwclock' and 'date' commands as one string using ';' as a delimiter:

   ```
   hwclock ; date
   ```

   The time should be almost the same.

5. Stop ntpd service:

   ```
   service ntpd stop
   ```

> **Note:**
>
> As a source of NTP time you can use Active Directory server's IP address. It usually spreads time to the network using NTP.
>
> Or you can use IP of gateway, but make sure that it supports NTP.
>
> To check whether server support NPT or not, use '**ntpdate -q <IP>**' command (replace IP with checked server address). The output should be as follows:
>
> ```
> root@atl-iw:~# ntpdate -q 10.10.0.98
> server 10.10.0.98, stratum 3, offset 9.196765, delay 0.04437
> 11 Sep 13:09:02 ntpdate[13819]: step time server 10.10.0.98 offset 9.196765 sec
> ```

6. Set synchronization by specifying NTP server in /etc/ntp.conf. Add to this file entry (replace IP with actual NTP server address):

   ```
   server 10.10.0.98
   ```

7. Run ntpd service:

   ```
   service ntpd start
   ```

8. Check ntpd service state:

   ```
   service ntpd status
   ```

9. Enable automatic time synchronization:

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

For correct Monitoring subsystem operation you NTP server IP should be specified in `/etc/nagios/iwmon/iwmon-services-ntp.conf`: see also i. 3.2.4.1 at page 40 (for «all-in-one» architecture) or i. 3.4.2 on page 62, step 2 (for distributed architecture).

# 3.2.3. Traffic Monitor Cluster with a Single Analysis Subsystem

> **Warning!**
>
> The information in this section can only be applied a Digital Fingerprints Detection module is used.

The Analysis subsystem performs an analysis of intercepted object text using the following methods:

- **Linguistic Analysis**. Determining the subject and content of a text based on the terms (words and phrases) found in this text. The search for the terms is performed using the classification. The classification includes the organization-specific terminology. All terms are divided into categories (each term can be correlated with one or more categories). Thus, the presence of a term belonging to a category allows the relating a text to this category.
- **Detecting Text Objects**. Search for text objects matching the specified templates (like searching for credit card numbers in the intercepted objects).
- **Detecting Digital Fingerprints**. Search for fragments of a text matching the predefined template documents (orders, financial reports, contracts, etc.).

If you use Digital Fingerprints Detection module, only one Analysis subsystem may function within the System.

If the System contains several instances of the Traffic Monitor Server, you must configure the text data to be delivered for content analysis from all server instances to a common Analysis subsystem.

**To configure sharing a single Analysis subsystem by multiple Traffic Monitor server instances:**

1. Stop the Analysis subsystem on all instances of Traffic Monitor server:

   ```
   service iw-caserv stop
   ```

2. On the computer where Analysis subsystem will run, in `/usr/local/infowatch/tm3/etc/tm.conf` file, `[CAS]` section, specify `0.0.0.0` instead of current server address.

   ```
   ListenAddr=0.0.0.0
   ```

3. On other instances of Traffic Monitor server, in `/usr/local/infowatch/tm3/etc/tm.conf` file, in the `[FILTER]` section, specify address and port of the computer where Analysis subsystem is running.
4. Launch this subsystem on the computer where Analysis subsystem will run.

```
service iw-caserv start
```

# 3.2.4. Server Configuring with Web-Console 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.

After IWTM server was installed, the system administrator should perform the following settings with web-console:

- Specify time synchronization server (see i. 3.2.4.1 at page 40)
- Configure sending notifications from the Monitoring subsystem (see i. 3.2.4.2 at page 41)
- If needed, install commercial InfoWatch Traffic Monitor license. Just after installation there is a trial license valid within 30 days from the date the Traffic Monitor Server is installed. Detailed information on licenses see in i. 3.2.4.3 at page 41.
- Make sure that monitoring indicators have  **Normal** state. Detailed information on Monitoring subsystem see in «*InfoWatch Traffic Monitor. Administration Guide*» document.

**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**.

## 3.2.4.1. Configuring Addresses of Time Synchronization Server

General server parameters of InfoWatch Traffic Monitor servers are set during in (see i. 3.1 at page 28, steps 6 and 7). 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**.

## 3.2.4.2. Configuring Notifications from Monitoring Subsystem

The Monitoring subsystem provides sending e-mail notifications in cases when current indicator value threshold.

**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.

## 3.2.4.3. Installing the License

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. 3.2.4.2 at page 41

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 (see Chapter 5 at page 78).
- If you change configuration of the traffic transfer according to the new deployment scheme (see i.2.1 on page 10) 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.

**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**.

**To install Traffic Monitor license:**

1. Place the license key (**iw_license.dat** file) received after request 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.

# 3.2.5. Traffic Monitor Server Configuring 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 administrator should make the following server configurations at the Traffic Monitor server:

- *Configuring Date and Time Synchronization (п. 3.2.5.1 on page 42)*
- *Configuring Connection to the Oracle DBMS Server (i. 3.2.5.2 on page 43)*
- *Installing the License (i. 3.2.5.3 on page 43)*

The Monitoring subsystem is configured at the database server as described in i. 3.4 on page 62.

## 3.2.5.1. Configuring Date and Time Synchronization

1. Set the system time using **date** command. For example, to set 11 September 2013 13:30 run the command with following parameters:

   ```
   date 09111330
   ```

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

   ```
   hwclock --systohc
   ```

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

   ```
   hwclock ; date
   ```

   The time should be almost the same.

4. Stop ntpd service:

   ```
   service ntpd stop
   ```

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

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

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

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

   ```
   server 10.10.0.98
   ```

7. Run ntpd service:

   ```
   service ntpd start
   ```

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

   ```
   service ntpd status
   ```

9. Enable authomatic time synchronization:

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

10. If you use Monitoring subsystem of Traffic Monitor, please edit **/etc/nagios/iwmon/iwmon-services-ntp.conf** file and specify IP-address of NTP server (see i. 3.4.1 at page 62).

## 3.2.5.2. Configuring Connection to the Oracle DBMS Server

If Oracle DBMS server is installer apart of Traffic Monitor server (first the server with **IWDBX** option was installed, then – with **IWTMX** option), then to provide connection to the Oracle DBMS server, uncomment and configure the connection settings in the file `$ORACLE_HOME/network/admin/tnsnames.ora` on the Traffic Monitor server, for example:

```
IWTM =
 (DESCRIPTION =
 (ADDRESS_LIST =
 (ADDRESS = (PROTOCOL = TCP)(HOST = iwtm)(PORT = 1521))
 )
 (CONNECT_DATA =
 (SERVER = DEDICATED)
 (SERVICE_NAME = iwtm)
 )
 )
```

where `HOST` is the network name of the Oracle DBMS server, and `SERVICE_NAME = iwtm` is the setting to define database instance service name.

> **Warning!**
>
> `tnsnames.ora` file is formatting-sensitive. Therefore if you want to copy given example it your file, please note that resulting line arrangement should correspond to example pattern.

## 3.2.5.3. Installing the License

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.

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 (see Chapter 5 at page 78).
- If you change configuration of the traffic transfer according to the new deployment scheme (see i.2.1 on page 10) 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 the System has a cluster of Traffic Monitor servers, then you need an individual licence key for every Traffic Monitor instance. For example, if the System has three Traffic Monitor server instances, then there should be three `iw_customer.dat` file generated (one file per instance). An individual `iw_license.dat` file will be sent for every `iw_customer.dat` file.

  > **Warning!**
  >
  > If the instance of Traffic Monitor server will be used as Sniffer only (see i. 2.1.3 on page 13, Variants 2 – 4), no license is required

- 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.

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

1. Run the **iw_lickey** utility located in the `/usr/local/infowatch/tm3/bin` directory. The utility will create the `iw_customer.dat` file in the `/usr/local/infowatch/tm3/bin` directory.
2. Email the `iw_customer.dat` file to the email address of InfoWatch's sales representative. After receiving `iw_customer.dat` file, manager will email you the `iw_license.dat` file.
3. Save `iw_license.dat` file, that you received from InfoWatch representative, to `/usr/local/infowatch/tm3/etc` directory. If the directory already contains the `iw_license.dat` file, replace this file with the new one.

   > **Warning!**
   >
   > The license key file must be located on the same computer where `iw_customer.dat` file was generated.

   If you use the license for intercepting HTTP traffic transmitted over ICAP protocol, set the owner of Traffic Monitor Server (default owner is **iwtm**) as the owner of the `iw_license.dat` file:

   ```
   chown iwtm:oinstall iw_license.dat
   ```

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

4. To apply a new license restart Traffic Monitor Server processes:

   ```
   service iw-trafmon restart
   ```

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

# 3.2.6. Installing and Configuring the Remote Database Management Module

If the system deployment scheme (i. 2.1 on page. 10) is chosen so that objects captured in the branch shall be transmitted to a remote database in headquarters through a slow channel, the remote database interaction module must be installed with the following configuration:

- in the branch, install the client part of the module on a computer with the Traffic Monitor server: see i. 3.2.6.1 on page 44.
- in headquarters, install the server part of the module on a computer with the Traffic Monitor server: i. 3.2.6.2 on page 46).

## 3.2.6.1. Installing the Client of the Remote Database Management Module (a Branch Office)

### Step 1. Install and configure general settings

1. Install the `iwtm_qmover-x.x.x-x.x86_64.rpm` (where `x.x.x-x` is the version of InfoWatch Traffic Monitor) on the computer where Traffic Monitor Server is installed. To do this, run the following command (as the `root` user):

   ```
   rpm -i /opt/distr/infowatch/traffic-monitor-3.5.3-265/Linux/ iwtm_qmover-3.5.3-265.x86_64.rpm
   ```

   The package will be installed to this directory:

   ```
   /usr/local/infowatch/tm3
   ```

2. Create a backup for `qmover.conf` file using the following command:

```
cp /usr/local/infowatch/tm3/etc/qmover.conf /usr/local/infowatch/tm3/etc/qmover.conf.bak
```

3. Run the qmover-setup.sh script:

```
/usr/local/infowatch/tm3/qmover-setup.sh
```

4. Configure the settings of the client:

`Select remote queue setup type?`

Select `client`.

`Enter TM EE qmover server's IP address.`

The IP address of the server (in the headquarter office) to which the client will send intercepted objects. The default value is `127.0.0.1`.

`Enter TM EE qmover server's port number.`

The server port, to which the intercepted objects will be delivered. Default value is 16888.

5. Restart Traffic Monitor:

```
service iw-trafmon restart
```

## Step 2. Configure the process autorun

Enable autorun for the `iw_qmover_client` process. Disable autorun for `iw_dbloader`, `iw_deliverd` and `iw_adlibitum` processes.

**To enable/disable the autorun of a process:**

1. For correct modification of settings stop Traffic Monitor server processes:

```
service iw-trafmon stop
```

2. In `/usr/local/infowatch/tm3/etc/tm.conf` file, the `[AUTO_RESTART]` section, apply the following settings:

To enable the autorun of a process, set this value in the section of the process: `autorestart = On`

Example (enabling `iw_qmover_client`):

```
iw_qmover_client:
autorestart = On
```

To disable the autorun of a process, set this value in the section of the process: `autorestart = Off`

3. Run Traffic Monitor Server processes:

```
service iw-trafmon start
```

## Step 3. Change the bandwidth of the data transmission channel

By default, the bandwidth is 128 Kbit/s. You can configure the bandwidth to be changed automatically at different time periods. To do it, use the `iw_qmover_channel_width_setter` utility.

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

**To set bandwidth limitations,**

on the client side (a branch office) configure crond to run the `iw_qmover_channel_width_setter` utility at the specified intervals.

The utility is run with the mandatory parameters:

```
iw_qmover_channel_width_setter <bandwidth>
```

where `bandwidth` is the bandwidth (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%.

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

| Interval | Bandwidth | |
|---|---|---|
| | Percent of the channel width | Equivalent in Kbit/s |
| 9 AM to 6 PM | 50% | 128 |
| 6 PM to 9AM | 100% | 256 |

Add these commands to etc/crontab:

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

# 3.2.6.2. Installing the Server of the Remote Database Management Module (the Headquarter Office)

## Step 1. Install and configure

1. Install the `iwtm_qmover-x.x.x-x.x86_64.rpm` package (where `x.x.x-x` is the version of InfoWatch Traffic Monitor) on the computer where Traffic Monitor Server is installed. To do this, run the following command (as the `root` user):

   ```
   rpm -i /opt/distr/infowatch/traffic-monitor-3.5.3-265/Linux/ iwtm_qmover-3.5.3-265.x86_64.rpm
   ```

   The package will be installed to this directory:

   ```
   /usr/local/infowatch/tm3
   ```

2. Create a backup for `qmover.conf` file using the following command:

   ```
   cp /usr/local/infowatch/tm3/etc/qmover.conf /usr/local/infowatch/tm3/etc/qmover.conf.bak
   ```

3. Run the `qmover-setup.sh` script:

   ```
   /usr/local/infowatch/tm3/qmover-setup.sh
   ```

4. Specify the server settings:

```
Select remote queue setup type?
```

Select `server`.

```
Enter TM EE qmover server's port number.
```

Specify the port on which the server listens to the objects received from the clients (from the branch offices). Default is `16888`.

```
Enter number of clients.
```

Specify the number of clients which will send objects to the server.

```
Please enter IP address of client N.
```

Specify the IP address of Client N. Default value is `127.0.0.1`. A separate query is displayed for each client.

The `/usr/local/infowatch/tm3/etc/qmover.conf` configuration file is created.

**Warning!**

When branch offices parameters are changed (offices quantyty or IP addresses):

- restore `qmover.conf` backup file and then run `qmover-setup.sh` script and specify new settings; restoring is performed with the following command:
  `cp /usr/local/infowatch/tm3/etc/qmover.conf.bak /usr/local/infowatch/tm3/etc/qmover.conf`
  or
- manually edit `qmover.conf` file.

## Step 2. Configure the process autorun

Enable autorun for `iw_qmover_server` process:

1. Stop Traffic Monitor server processes:

   ```
   service iw-trafmon stop
   ```

2. In `/usr/local/infowatch/tm3/etc/tm.conf` file, the `[AUTO_RESTART]` section, set the following values in `iw_qmover_server` block: `autorestart = On`:

3. Run Traffic Monitor server processes:

   ```
   service iw-trafmon start
   ```

## Step 3. Create different queues for clients

Objects received from all clients (the branch offices) are sent by default to a `/usr/local/infowatch/tm3/queue/db` common queue. Objects intercepted in the local network of the headquarter office (i.e. in the network where the database is located) are sent to the same queue.

It is advised to create a single queue for each client to increase the reliability of receiving objects. The queues are configured on the server in headquarters office.

**To create a separate queue to receive objects from the client,**

1. Open the `/usr/local/infowatch/tm3/etc/qmover.conf` file.
2. In `[client_N]` section (N is the ordinal number of the client) change the value of `QueuePath` setting by specifying full path to the directory where the queue will be located. The queue will be created in the specified directory when the server connects to the client for the first time.

   Repeat this until queues for each client are specified.

   > **Warning!**
   >
   > The queues from all clients must be placed on the same volume of the hard drive.

3. For the queue of each client, specify the parameters for moving the objects to the general queue. Run the iw_qtool utility with these parameters:

   ```
   iw_qtool move <source_queue> <receiving_queue>
   ```

   Where:

`source_queue` is the full path to the directory where the queue of Client N is located (the value must meet `QueuePath` value in `[client_N]` section).

`receiving_queue` is the full path to a common queue of the server (`queue/db` is used by default).

   Example:

   ```
   iw_qtool move /u01/client_1 /usr/local/infowatch/tm3/queue/db
   ```

4. In crond, configure the autorun of the iw_qtool utility with the required frequency.

# 3.3. Traffic Interceptors Settings

This section contains procedures and examples for configuring interceptors when using different System deployment schemas:

| Deployment schema | Interceptor settings | Link |
|---|---|---|
| Receiving Copies of SMTP Traffic from a Mail Server (i. 2.1.1 on page 10) | Configuring Blind Carbon Copies Forwarding | i.3.3.1 on page 48 |
| SMTP traffic interception via Postfix (i. 2.1.2 on page 12) Also recommended when the System receives a copy of SMTP traffic (i. 2.1.1 on page 10). | Integration of Traffic Monitor Server with Postfix | i.3.3.2 on page 49 |
| Intercepting a Traffic Copy through the Sniffer (i. 2.1.3 on page 13) | Configuring Sniffer | i.3.3.3 on page 51 |
| | Configuring cluster parameters for Traffic Monitor servers | |
| Intercepting HTTP-traffic transmitted over ICAP, with a proxy server (i. 2.1.4 on page 17) | Installing and configuring the IW ICAP Module | i.3.3.3 on page 51 |
| Revision of files from the corporate network (i. 2.1.7 on page 22) | Installing and configuring the Crawler | i.3.3.5 on page 57 |

## 3.3.1. Configuring Blind Carbon Copies Forwarding

> **Warning!**
>
> This section contains instructions for forwarding blind carbon copies of SMTP messages (BCC) to Traffic Monitor server (see i. 2.1.1 on page 10) based on Microsoft Exchange Server 2007 and 2010 pattern. If other mail server types are used the configuration procedure may be different.

For sending blind copies of SMTP messages you need to create and configure connector on Exchange Management Console that will forward mail to Traffic Monitor server. For this purpose, take the following steps.

### Step 1. Creating SMTP connector to forward mail to Traffic Monitor server

1. Select **Organization Configuration** node **–> Hub Transport** and click **New Send Connector**.
2. In connector creation wizard window that appears enter the name for connector being created and select **Custom** from drop-down menu. Click **Next**.
3. In **Address space** step create new address space for traffic forwarding. Then click the **Add** button. In the dialog box that appears, specify address space settings and click **OK**. Click **Next**.
4. In **Network Settings** step select **Route mail through the following smart hosts** and click **Add**. In the dialog box that appears, specify IP address of TM server to forward mail to, and click **OK**. Click **Next**.
5. In **Configure smart host authentication settings** step select **None**. By default Postfix requires no authorization on TM server. Click **Next**.
6. In **Source Server** step select the server where this connector will run. Click **Next**.
7. In **New Connector** step make sure that connector settings are correctly configured and click **New**. Wait for process to complete and click **Finish**.

   Connector creation wizard dialogue will close.

### Step 2. Creating a contact where the copies of messages will be forwarded

1. Select **Recipient Configuration** node **–> Mail Contact** and select **New Mail Contact**.
2. In contact creation wizard dialogue that appears select **Mail Contact** and click **Next**.
3. In **Configure smart host authentication settings** step enter general contact information. In **External e-mail address** line click **Edit**. In **SMTP Address** dialogue that appears specify email address to forward copies of messages to.

   > **Warning!**
   >
   > Contact mail address domain should match with connector domain.

4. In **New Mail Contact** step make sure that connector settings are correctly configured and click **New**. Wait for process to complete and click **Finish**.

   Contact creation wizard dialogue will close.

### Step 3. Creating transport rule for messages copying

1. Select **Organization Configuration** node **–> Hub Transport** and click **New Transport Rule**.
2. In transport rule creation wizard dialogue that appears enter the name for the rule being created and check **Enable Rule** field. Click **Next**.
3. In **Conditions** step check **from users inside or outside the organization** condition. Select **Inside** as condition settings. Click **Next**.
4. In **Actions** step check **Blind carbon copy (Bcc) the message to address** action. Click hyperlink with **address** settings select previously created contact in **Select Recipient** window that appears. Then click **OK**. In transport rule creation wizard dialogue click **Next**.
5. Where necessary you may configure exceptions for the rule in **Exceptions** step. For example, to avoid copying mail from individual users, you may check **except when the message is from people** exception and select users in exception settings. Click **Next**.
6. In **Create Rule** step make sure that rule settings are correctly configured, and click **New**. Wait for process to complete and click **Finish**.

## 3.3.2. Integration of Traffic Monitor Server with Postfix

The necessity for Postfix integration is determined based on System deployment schema and on the fact if the TM sever and database are installed on the same computer or not:

| **Deployment schema** | | **Postfix integration** |
|---|---|---|
| The System intercepts and delivers SMTP traffic via integration with Postfix (see i. 2.1.2 on page 12) | TM server is installed apart from the database (kickstart key IWTMX) | Mandatory |
| | All components are installed on the same computer (kickstart key IWALLX or IWTMSX) | Set by default |
| SMTP traffic is delivered by the corporate mail system. The System receives only a copy of SMTP traffic (see i. 2.1.1 on page 10) | TM server is installed apart from the database (kickstart key IWTMX) | Recommended |
| | All components are installed on the same computer (kickstart key IWALLX or IWTMSX) | Set by default |
| System received SMTP traffic copy via Sniffer (see i. 2.1.3 on page 13). | | Not required |
| Intercepting SMTP traffic is not required (for example, Traffic Monitor Server will be used as Sniffer only) | | Not required |

Postfix mail server receives incoming SMTP messages via port **25**. Then incoming SMTP messages are passed to **iw_smtps** process to port **2025**. Then received SMTP messages are analyzed by Traffic Monitor.

Upon completion of the analysis **iw_messed** process forwards mails, whose delivery is allowed, to Port **2020** of Postfix mail server (see Figure 16). The Postfix mail server either directly delivers the e-mails to recipients or forwards them to the next mail relay server.

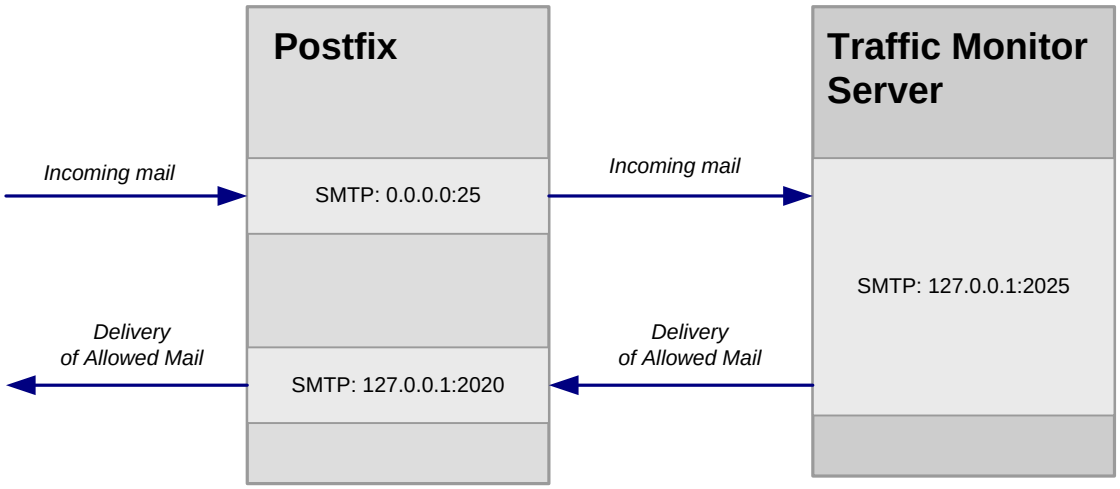



Figure 16 Integration with Postfix

**Warning!**

In the deployment scheme using Traffic Monitor server as a relay-server, other mail servers (Microsoft Exchange etc.) running in enterprise mail system must be set for sending outbound messages to Postfix server.

For correct interaction of InfoWatch Traffic Monitor system with Postfix mail server edit `main.cf` and `master.cf` configuration files:

1. Login the system as root:

```
su – root
```

2. Edit `/etc/postfix/main.cf` configuration file.
3. Check the `mynetworks` parameter correctly denotes subnetwork where Exchange servers are located.
4. If the InfoWatch Traffic Monitor should take part in delivery of SMTP-traffic (blocking mode):
   - specify `relayhost` parameter. Set its value as IP-address of corporate mail server which should receive SMTP letters after analysis in the Traffic Monitor.
   - add the following strings in the end of the file:

```
27.0.0.1:2020   inet  n   -      n    -   21   smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000
-o myhostname=<$hostname>
```

5. Edit `/etc/postfix/master.cf` configuration file.
6. To provide mail transferring to TM add the following string:

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

> **Important!**
>
> The mail transferring is provided by default in type of installation using the kickstart installer.

7. Check the syntax in configuration files:

```
service postfix check
```

8. Restart Postfix:

```
service postfix restart
```

> **Important!**
>
> If you plan to use the Postfix server on the remote computer:
>
> Specify the IP address and port of the computer from which it is necessary to accept messages instead of `127.0.0.1:2020`;
>
> Adjust the `inet_interfaces` parameters according to the recommendations specified on the Postfix web-site:
>
> http://www.postfix.org/start.html

# 3.3.3. Configuring Sniffer

Sniffer is automatically installed when Traffic Monitor is installed. However in some deployment schemas (see i. 2.1.3 on p. 13, variants 2 – 4) the stand-alone installation of Traffic Monitor server working as Sniffer is needed. Hardware and software requirements to computer for Sniffer are listed in i. 2.2.3 on page 23.

This section covers:

- Configuring Traffic Monitor Server as Sniffer (i. 3.3.3.1 on page 51).
- Configuring Traffic Monitor Server to Receive Copy of Traffic from Sniffer (i. 3.3.3.2 on page 52).
- Creating Traffic Monitor Cluster (i. 3.3.3.3 on page 53).

## 3.3.3.1. Configuring Traffic Monitor Server as Sniffer

On the computer, where the Sniffer is installed, configure these settings:

1. Stop Traffic Monitor server processes:

```
service iw-trafmon stop
```

2. In `/usr/local/infowatch/tm3/etc/tm.conf` configuration file, `[AUTO_RESTART]` section, configure the following settings:
   - Variant 1. Traffic will be intercepted and analyzed on different computers. This instance of Traffic Monitor Server will function as Sniffer only (intercept traffic):
     a. Enable the autorun for the iw_sniffer process:

```
iw_sniffer:
  autorestart = On
```

     b. Disable autorun for other processes: `autorestart = Off`.
   - Variant 2. A copy of traffic is intercepted and analyzed on the same computer. Traffic Monitor Server will receive a copy of traffic from CISCO switch (Sniffer feature), analyze received data and load them to the database (Traffic Monitor Server features):
     a. Enable the autorun for `iw_sniffer`. `iw_dbloader`, `iw_updater`, `iw_warpd` and `iw_adlibitum` processes. Also, enable the autorun for needed interceptors: `iw_proxy ICQ`, `iw_proxy HTTP`, `iw_proxy SMTP`:

```
autorestart = On
```

b. Disable autorun for other processes: `autorestart = Off`.

3. In `/usr/local/infowatch/tm3/etc/tm.conf` configuration file, `[SNIFFER]` section, configure intercepting settings:
   - `Host`. IP-address of the host waiting for the proxy connection.
   - `Port`. Port of the host waiting for the proxy connection
4. Run Traffic Monitor server processes:

```
service iw-trafmon start
```

## 3.3.3.2. Configuring Traffic Monitor Server to Receive Copy of Traffic from Sniffer

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

In `/usr/local/infowatch/tm3/etc/tm.conf` configuration file, configure the following settings:

- In `[PROXY_SMTP]`, `[PROXY_HTTP]`, `[PROXY_ICQ]` sections, specify the settings for enabled interceptors: `SnifferHost` (Sniffer IP address) and `SnifferPort` (port used by Sniffer to receive incoming messages)
- in `[SMTP]`, `[HTTP]`, `[ICQ]` sections, specify the following settings:

| Setting | Comments |
|---|---|
| `Interface` | The network interface used to transfer data from the switch. These variants are allowed:<br>• each interceptor is assigned a separate network interface;<br>• all interceptors are assigned one network interface; |
| `OpenTimeout` | Time to keep connection alive (in seconds) if no packages are transmitted. The recommended value is 600. |
| `LiveTimeout` | Timeout (in seconds) when the status of connection must change to *ESTABLISHED*. If the status is not changed, connection will be automatically terminated. The recommended value is 86400. |
| `CloseTimeout` | Time to keep the connection alive (in seconds) when the status is changed to *TIME_WAIT.* The recommended 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 recommended value is 16777216. |

- In `[PROXY_HTTP]` section, set `SkipNegotiate` setting to Off.
- To intercept ICQ traffic transferred through a proxy (over HTTP) set `IcqFilter` to `On` in `[PROXY_HTTP]` section.

# 3.3.3.3. Creating Traffic Monitor Cluster

When a copy of traffic is intercepted via Sniffer, you can build Traffic Monitor server clusters to improve System performance.

> **Warning!**
>
> One cluster can contain up to 2 instances of Traffic Monitor Server. It is not advised to use more than 3 clusters.
>
> When you use a cluster, the speed of network connection between Sniffer and Traffic Monitor Server must be twice as fast as the speed of delivery of traffic to Sniffer.

**To build a cluster of Traffic Monitor servers configure cluster settings in `/usr/local/infowatch/tm3/etc/tm.conf` configuration file in each instance of Traffic Monitor Server that is included in cluster.**

1. In `[PROXY_SMTP]`, `[PROXY_HTTP]`, `[PROXY_ICQ]` sections, specify `ClusterID` value for each enabled interceptor.
2. In `[PROXY_SMTP]`, `[PROXY_HTTP]`, `[PROXY_ICQ]` sections, specify balancing type (`Balancer` settings) value for each enabled interceptor. Available values:

`Connection`. An instance of Traffic Monitor Server with iw_proxy is selected for each new TCP connection. Thus all instances of Traffic Monitor server are used by turn.

`SrcIp`. Traffic is distributed between multiple instances of Traffic Monitor server with iw_proxy according to IP address of the client. This means that all data received from the same IP address of the client will be delivered to the same instance of Traffic Monitor server.

> `SrcIp` option must be specified for the `PROXY_HTTP` interceptor, if you need to intercept ICQ messages transmitted through the proxy-server (over HTTP). In all other cases it is advised to use `Connection` option.

**Example. Creating a cluster containing 2 instances of Traffic Monitor server**

The System intercepts a copy of SMTP and HTTP traffic through the Sniffer.

To increase performance while analyzing traffic, a cluster consisting of 2 instances of the Traffic Monitor server is created (see Figure 17).

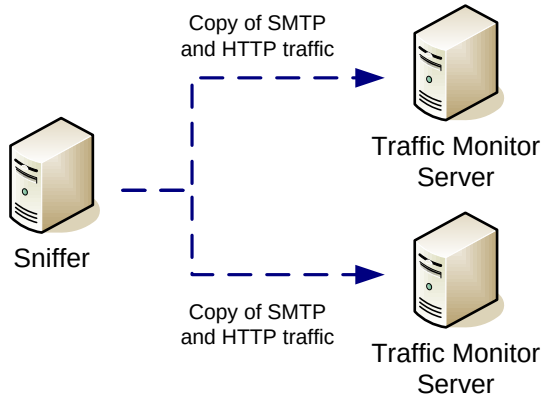



Figure 17. Creating a cluster containing 2 instances of Traffic Monitor server

To build a cluster, configure these settings in `/usr/local/infowatch/tm3/etc/tm.conf` file for each instance of Traffic Monitor Server.

- The [SMTP] Section:

  ```
  Balancer = Connection
  ```

- [HTTP] **Section:**

  ```
  Balancer = Connection
  ```

- [PROXY_SMTP] Section:

  ```
  SnifferClusterID = smtp
  ```

- [PROXY_HTTP] **Section:**

```
SnifferClusterID = http
```

# 3.3.4. Installing and configuring the IW ICAP Module

At the installation of the Traffic Monitor server the IW ICAP module is installed automatically (**IWTMX**, **IWALLX** or **IWTMSX** options). The autostart of `iw_icap` process is enabled by default on the TM server.

If you need to enable the IW ICAP module manually, do the following steps:

## Step 1. Getting ready to Install

Make sure that you have all of the Linux packages that are required to install the IW ICAP module. This can be done by running the following command:

```
rpm –qpR /path_to_the_package_iwtm/iwtm_icap-x.x.x-x.i686.rpm
```

where: x.x.x-x is the InfoWatch Traffic Monitor version number.

## Step 2. Install the IW ICAP module

Install the `iwtm_icap-x.x.x-x.i686.rpm` package (where `x.x.x-x` is the version of InfoWatch Traffic Monitor) on the computer where Traffic Monitor Server is already installed. To do this, run the following command (as the `root` user):

```
rpm –i /path_to_the_package_iwtm/iwtm_icap-x.x.x-x.i686.rpm
```

Example:

```
rpm -i /u01/iwtm_icap-3.5.0-59.i686.rpm
```

The package will be installed to this directory:

```
/usr/local/infowatch/tm3
```

## Step 3. Configuring autorun

Enable autorun for `iw_icap` process:

1. For correct modification of settings stop Traffic Monitor server processes:

   ```
   service iw-trafmon stop
   ```

2. In `/usr/local/infowatch/tm3/etc/tm.conf` file, `[AUTO_RESTART]` section, `iw_icap_server` block specify: `autorestart = On`:
3. Start Traffic Monitor Server processes:

   ```
   service iw-trafmon start
   ```

## Step 4. Configure the proxy server

Configure the settings for intercepting HTTP requests on the proxy server.

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

Examples of settings configuring for various environment are introduced in the following sections:

- Configuring proxy for Integration with Active Directory (i.3.3.4.1 on page 55).
- Recommendations for Configuring ICAP for Blue Coat SG Series (i.3.3.4.2 on page 56).
- Recommendations on SQUID Configuring (i.3.3.4.3 on page 57).

# 3.3.4.1. Configuring proxy for Integration with Active Directory

Below is the example of configuring proxy for its Integration with Active Directory (based on example of SQUID 3.1.7 on a Computer with CentOS 5.5 / RHEL 5.5)

> **Note:**
>
> The procedure of configuring settings, which is described below, may vary depending on the version and model of the proxy server. For the relevant information on configuring the settings, see the documentation for your proxy server.

1. Make sure that the following packages are installed:

squid3

samba

samba-common

kerberos

2. Configure samba configuration file (`/etc/samba/smb.conf`):

```
[global]
        workgroup = EXAMPLE
        server string = Samba server %v
        netbios name = machine

        security = ADS
        realm = EXAMPLE.COM
        password server = 192.168.1.1
        encrypt passwords = Yes
        preferred master = No
        domain master = No
```

Where:

- `EXAMPLE` is the name of workgroup, the ICAP server belongs to;
- `EXAMPLE.COM` is the DNS name of the ICAP server.

3. Configure kerberos configuration file (`/etc/krb5.conf`):

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = EXAMPLE.COM
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 EXAMPLE.COM = {
  kdc = dc.example.com:88
  admin_server = dc.example.com:749
  default_domain = example.com
 }

[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM

[appdefaults]
 pam = {
   debug = false
```

```
    ticket_lifetime = 36000
    renew_lifetime = 36000
    forwardable = true
    krb4_convert = false
  }
```

4. Configure `/etc/nsswitch.conf` configuration file:

```
passwd: files winbind
group:  files winbind
shadow: files
```

5. In `/etc/hosts` file, specify entries for FQDN ICAP server. That is,

```
squid.example.com
```

6. Check `smb.conf` file for errors:

```
testparm
```

If no errors are detected, restart samba:

```
/etc/init.d/smb restart
```

7. Include the computer into a domain

```
net ads join –U username
```

where `username` is the name of user with privileges to include this computer into domain.

8. Start `winbind`:

```
winbindd
/etc/init.d/smb restart
```

9. Check operations of `winbind`:

To obtain a list of domain users, execute the following command:

```
wbinfo –u
```

To obtain a list of domain groups, execute the following command:

```
wbinfo –g
```

10. Edit `/etc/squid/squid.conf` configuration file by adding the following strings:

```
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp
auth_param ntlm children 5
auth_param ntlm keep_alive on
acl ntlm_users proxy_auth REQUIRED
http_access allow ntlm_users
/etc/init.d/squid restart
```

## 3.3.4.2. Recommendations for Configuring ICAP for Blue Coat SG Series

You need to enable using ICAP in `Request Mode` on proxy and configure the settings for interacting with Traffic Monitor Server. The parameters are set through the Web interface under an administrator account.

**Notes:**

The procedure of configuring settings, which is described below, may vary depending on the version and model of the proxy server. For the relevant information on configuring the settings, see the documentation for your proxy server.

If you need to intercept HTTPS traffic, configure Blue Coat to process HTTPS traffic as HTTP traffic. For more information, see the documentation for your proxy server.

1. Go to the **Configuration** tab.
2. Go to the **External Services ► ICAP** section. Create the **tm** service. Configure the settings of the service:

**Service URL**: `icap://<TM_server_IP>/reqmod`

Example: `icap://10.60.0.20/reqmod`.

**Maximum number of connections**: `10`

**Connection timeout**: `70`

Check **This service supports plain ICAP connection**. In Plain ICAP port field, specify 1344.

> **Warning!**
>
> The value of **Plain ICAP port** field must match the value of `ListenPort` setting in `/usr/local/infowatch/tm3/etc/icap.conf` file, `[ICAP]` section. If another value was set for `ListenPort` setting, you need to adjust it.

On **ICAP v1.0 Options** panel, configure the following settings:

- **Method supported**: select **request modification**
- **Send**: Check **Authenticated User, Client address** and **Server address** boxes.

3. Go to the **Health Checks ► General** section. Make sure that verification of server status is enabled — **Health Checks** tab displays the addresses:

   `icap.tm`

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

## 3.3.4.3. Recommendations on SQUID Configuring

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

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

**An example of ICAP configuring for SQUID 3.1.7**

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

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

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

# 3.3.5. Installing and Configuring the Crawler

The Crawler interceptor 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.

For both Crawler components (server and scanner) installation the same distributive is used.

> **Warning!**
>
> One DB Traffic Monitor can be used by **only one** Crawler server instance. One Crawler server can support **only one** Crawler scanner instance.

Hardware and software requirements to computers where to the Crawler will be installed see in i. 2.2.3 at page 26.

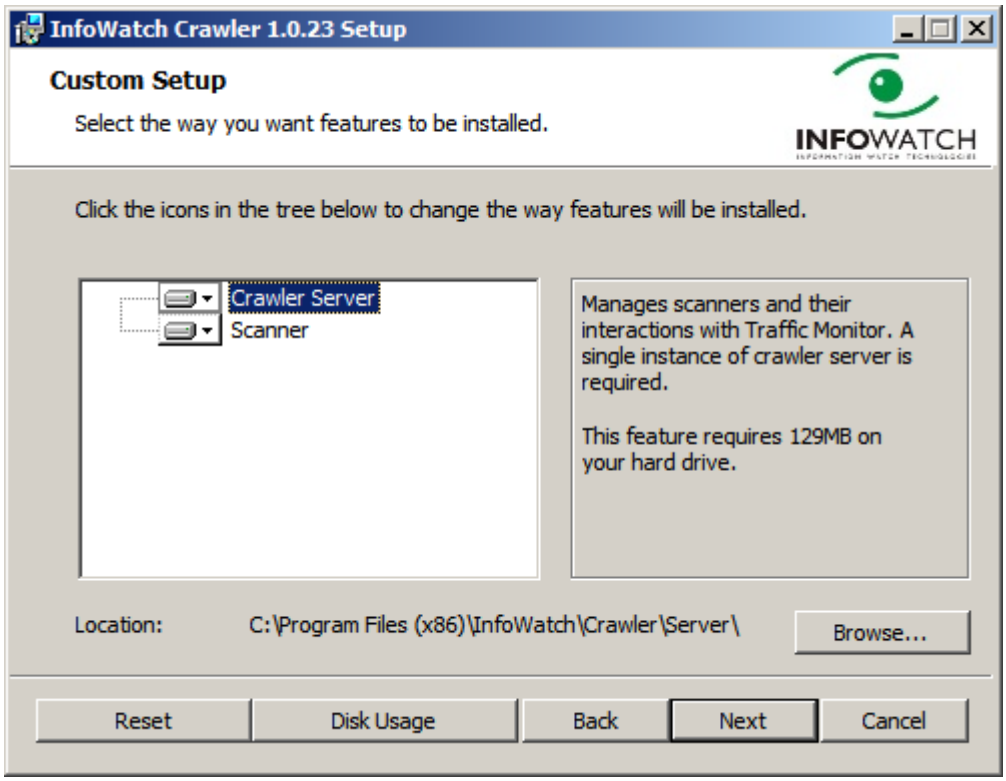
See the detailed information on Crawler installation and configuration in the following sections:

- *Installing Crawler Server and Scanner (i. 3.3.5.1 at page 58)*
- *Configuring Network Access Rules (i. 3.3.5.2 at page 61)*

# 3.3.5.1. Installing Crawler Server and Scanner

**To install the Crawler:**

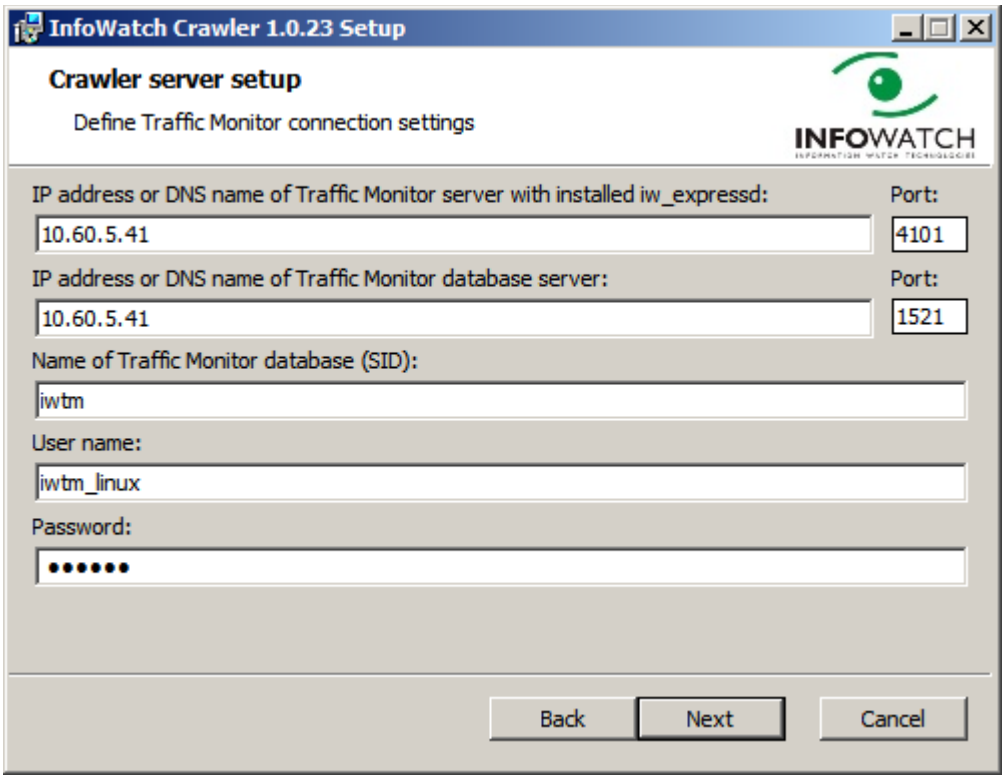
1. Run `Crawler_vx.x.x.xxx.msi` installation package, where `x.x.x.xxx` is a version number.
2. In the InfoWatch Crawler welcome window click **Next**.
3. At the **Custom Setup** screen select which Crawler components should be installed and where to:
   - **Crawler Server** – installing the `InfoWatch.Crawler.Server` service managing scanning tasks and provides communication with the server, database and Traffic Monitor Management Console.
   - **Scanner** – installing the `InfoWatch.Crawler.Scaner` service scanning network folders and file storages according to settings configured by user.




If you don't need any component, select it and click ✕ **Entire feature will be unavailable** in the drop-down menu.

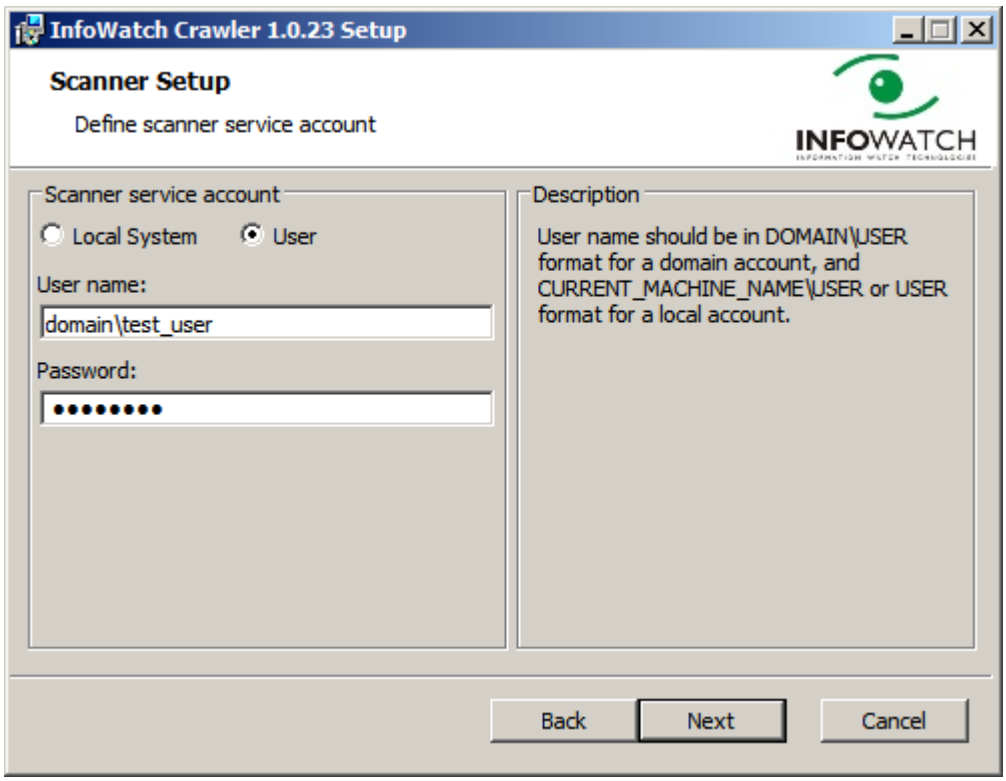
Specify path to directories where to components will be installed and click **Next**.

4. If at **Custom Setup** step you chose **Server** component installation, and then specify parameters of connecting the `InfoWatch.Crawler.Server` service with Traffic Monitor server.

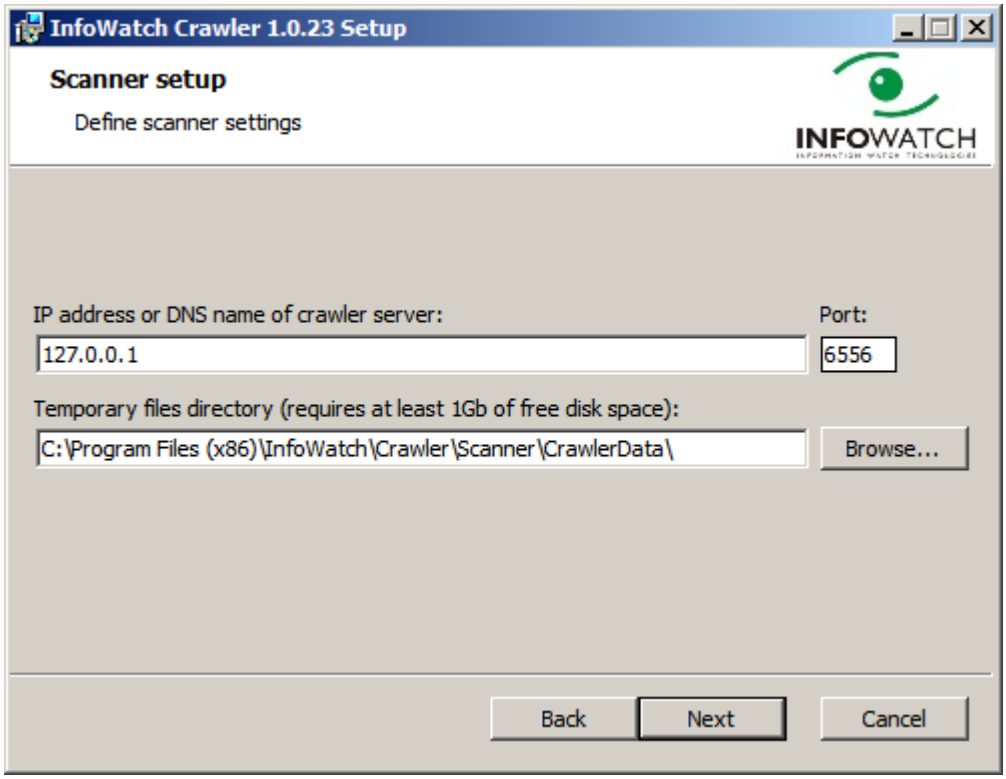



> **Warning!**
>
> **User name** should be the same as a name of Oracle account used for managing the Linux part of IWTM (`iw_adlibitum`, `iw_dbloader`, `iw_updater`). If you installed the system from the kickstart with default options, this is **iwtm_linux**.

5. If at **Custom Setup** step you chose **Scanner** component installation, then specify a name of account used for `InfoWatch.Crawler.Scaner` service running. You can select standard Local System account (recommended option) or enter parameters of an account having a rights for running services in the background (this option is configured in **Control Panel –> Administrative Tools –> Local Security Policy –> local policies –> User Rights Assignment –> log on as a service**).




6. If at **Custom Setup** step you chose **Scanner** component installation, then specify:
   - IP address or DNS name of the computer where the **Server** component is installed;
   - Crawler server's port number;
   - link to the directory to where the scanner will temporary save files copied from reviewed resources.



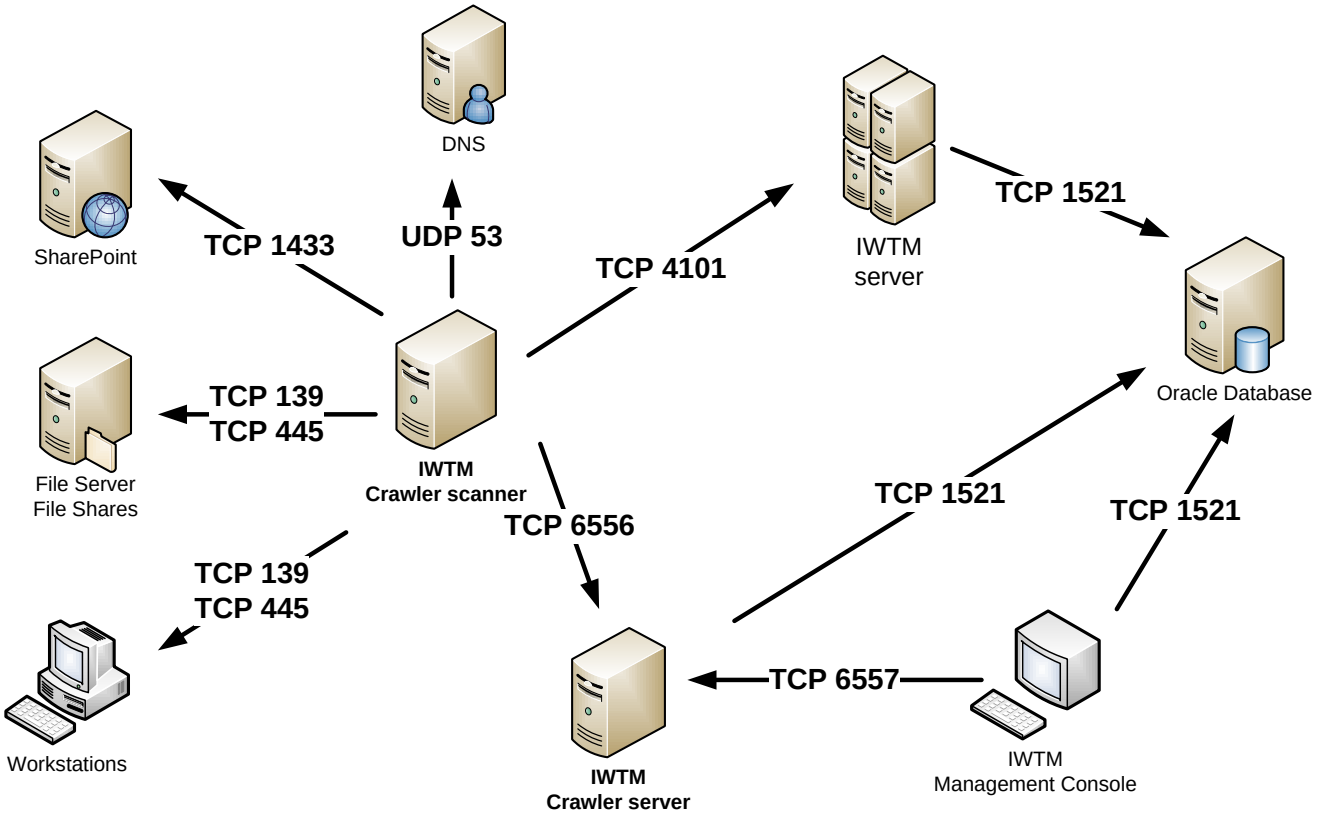

Click **Next**.

Click **Install** to start Crawler installation. Follow the instructions to complete installation.

# 3.3.5.2. 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<br>TCP 445 | |
| Crawler scanner – IWTM server | TCP 4101 | Configured in the IWTM server configuration file `tm.conf`, `[EXPRESSD]` section, `ListenPort` setting |
| 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.

# 3.4. Configuring the Monitoring Subsystem for Distributed Architecture

The InfoWatch Traffic Monitor Monitoring subsystem was developed basing on the Nagios supplement, which provides remote monitoring of hosts and network services.

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 all general settings of Monitoring subsystem are set. You can just configure notifications sending with the web-interface (see i. 3.2.4.2 at page 41).

If InfoWatch Traffic Monitor system is deployed in such a way that database server (**IWDBX** kickstart option) is installed apart of Traffic Monitor servers (**IWTMX** kickstart option), then Monitoring subsystem will operate at the database server. To provide the diagnostics of all servers of the Traffic Monitor solution please perform following additional settings:

- *Configuring Time Synchronization Server Address (i. 3.4.1 on page 62)*
- *Configuring Connection with Servers (i. 3.4.2 on page 62)*
- *Configuring Activation Thresholds for Load Indicator (i. 3.4.3 on page 64)*
- *Configuring Services Autorun (i. 3.4.4 on page 65)*
- *Configuring Notification Engine (i. 3.4.5 on page 65)*

## 3.4.1. Configuring Time Synchronization Server Address

For properly time synchronization you should specify IP address of the NTP server 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. Edit `iwmon-services-ntp.cfg` file
2. In the value of `check command` parameter replace default IP address by the actual IP address of the NTP server (time synchronization server).

## 3.4.2. Configuring Connection with Servers

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` extention 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 – server 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 where all System server components are installed on a single host

**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
    }
```

### Launching installation software

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 keep 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 server specified in step 2.

# 3.4.3. Configuring Activation Thresholds 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.

# 3.4.4. Configuring Services Autorun

Launch nagios and apache services for web interface:

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

Configure apache and nagios services autorun:

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

# 3.4.5. Configuring Notification Engine

The Monitoring subsystem provides sending email notifications in cases when the current value of the indicator exceeds the threshold value.

For more information see:

- *Configuring Notifications of Threshold Exceeding for Indicators (i. 3.4.5.1 at page 65)*
- *Configuring Sending Notification Mails via Postfix (i. 3.4.5.2 at page 66)*

## 3.4.5.1. Configuring Notifications of Threshold Exceeding for Indicators

**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. Please specify each address 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` is 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

### 3.4.5.2. Configuring Sending Notification Mails via Postfix

If the installation of the System enables:

- sending SMTP-messages via Postfix (see ii. 2.1.2 on page 12)

  and

- installation of Monitoring subsystem to the same server where Postfix is installed,

for sending e-mail notifications notification in cases when current indicator value succeeds the threshold value, you should:

1. Add the following strings to `/etc/postfix/transport` file:

   ```
   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 to the `/etc/postfix/main.cf` file:

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

4. Restart Postfix:

   ```
   service postfix restart
   ```

# 3.5. Installing the Management Console

The Installation file of Traffic Monitor Menagement Console (`setup.exe`) is located in the `Setup.Gui.Ru` directory in the System distributive kit.

You also can download the installation file from the Traffic Monitor server using the web console. To enter the web console, type the IP address of the Traffic Monitor server in an address line of any internet-browser. To load a distribution kit of Management Console, press **Download Management Console** int the **General** section of the web console.

Press **.NET Framework** in the **General** section of web console to download the .Net Framework platform, which is necassery to the correct work of Menagement Console.

### Step 1. Run the Installation Wizard

On System installation CD, open `Setup.Gui.En` folder. There, find and run `setup.exe` file.

After that **"InfoWatch Traffic Monitor Management Console"** installation wizard welcome screen displays. Press **Next** button.

### Step 2. Accepting the license agreement

Read the license agreement. If you accept the terms of this License Agreement check **I Agree** box and press **Next** button.

### Step 3. Select the Installation directory

Path to the directory where Management Console will be installed is assigned in the **Folder** field.

Select an option for creating Management Console shortcut:

- **everyone**. The shortcut will be created for each user who is registered on this computer.
- **just me.** The shortcut will be created for the user who installed the console.

Press **Next** button.

### Step 4. Complete the installation

After proceeding to **Confirm Installation** screen, click **Next** to start installation.

To complete installation of Management Console follow installation wizard instructions.

### Step 5. Advanced settings for sending reports

Users analyzing objects in Management Console can send reports containing comments for objects. To support this feature on all computers where Management Console is installed, that will be used to send reports, change operating system settings on these computers. To do it, open **Control Panel (Start ► Settings ► Control Panel)**. Select the **Regional and Language Options** component. In the dialog window than opens, go to **Advanced** tab and select your language for non-Unicode programs.

### Step 6. Configuring support for national charsets & time standards

To support national charsets and time standards open system registry and set the `NLS_LANG` environment variable to appropriate value.

Registry key path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\KEY_OraClient11g_home#\NLS_LANG
```

where "`#`" denotes a digit. The value of "`#`" in `KEY_OraClient11g_home#` should match the value of the same character for `OraHome_#` directory.

**Warning!**

If registry key is unavailable in the indicated path, the Oracle DBMS server settings will be used for national charsets and time standards (for example, while selecting days of week).

# 3.6. Configuring the Settings for Analyzing and Monitoring Objects

**Warning!**

The Management Console is initially launched using the user administrator account or security officer account. These accounts are created along with database scheme (see the last table in i. 3.1 on page 28).

User administrator only has privileges to create accounts and roles for other users.

Configuration setting may be performed using preset security officer account (see the last table in i. 3.1 on page 28) or other user account, having sufficient permissions (for more details see «*InfoWatch Traffic Monitor. User Guide"* documents).

After installation ended, start Management Console, connect to Traffic Monitor database and configure analysis and objects processing settings:

1. To support the analysis of intercepted text object, configure the following settings:
   - Load or generate classification for enabling linguistic analysis.
   - Configure list of text objects for enabling text objects detection.

- Generate and compile reference document database for enabling Digital Fingerprints Detection.

2. Where necessary apply synchronization with Active Directory.
3. Configure advanced settings (color sets, lists and responsibility zones), required for correct operations of object processing script.
4. Configure and enable objects processing script.

> **Warning!**
>
> If the system should block intercepted objects, i.e.:
>
> - when SMTP traffic is intercepted by Traffic Monitor server connected in-line (i. 2.1.2 on page 12),
> - when HTTP traffic is intercepted by proxy server with ICAP (i. 2.1.4 on page 17)
>
> then for *Smtp* or *Http* monitor respectively there should be specified the trainsport mode (instead of default *Copy)*:
>
> - *Normal* – if the system should block an object depending on the verdict. Then for `Monitor.Smtp` or `Monitor.Http` respectively you should specify `root.processing.transport_mode = TransportMode.Normal`
> - *Transparent* – if an object should be always delivered to the recipient regardless of verdict. Then for `Monitor.Smtp` or `Monitor.Http` respectively you should specify `root.processing.transport_mode = TransportMode.Transparent`

5. Send setup configuration to hosts.

For more detailed information on configuring the above settings, see *"InfoWatch Traffic Monitor. User Guide"* document.

To make sure the allied settings are correct, you may run one of preset queries and view intercepted objects.

# CHAPTER 4. UPDATING THE SYSTEM

The standard InfoWatch Traffic Monitor updating procedure uses **kickstart** installation program and provides the complete re-installing not only system components but the whole operating system of the server. Therefore you should give a special consideration to saving all changes made in the System during its exploitation: all the differences between your system and the default configuration. This can include database content, configuration files and object processing scripts.

This chapter includes:


- The order of updating (see i 4.1 on page 69)
- Creating database backup (see i 4.2 on page 71)
- Restoring database from the backup (see i 4.3 on page 75)
- Updating a database schema (see i 4.2 on page 75)
- Modifying files of a new version (see i 4.2 on page 77)


## 4.1. The Order of Updating

While you update the Traffic Monitor server, you should disable interception of all the traffic. Therefore we recommend that you should perform update when the traffic and the size of the file queue are minimal.

To update the System, perform the following steps:

1. Stop the `iw-trafmon` and `iw-caserv` processes. On computers where Crawler is installed, stop `InfoWatch.Crawler.Server` and `InfoWatch.Crawler.Scanner` services.
2. Create a backup copy of the **database.conf** file, which is located in the `/opt/distr/infowatch/csw-auto-install/csw-4.1.NNN` directory, where `NNN` is the number of the installed version.
3. Save configuration files.

   If you have customized object processing scripts, the sample document database or configuration files, then you should save them to an external storage before updating the System. Default locations for the main files are as follows:

   - object processing scripts: `/usr/local/infowatch/tm3/etc/scripts`
   - sample document database: `/usr/local/infowatch/tm3/cas/ca_db`
   - configuration file `/usr/local/infowatch/tm3/etc/tm.conf`
   - web-resources lists: `etc/scripts/user_resources.list`

   Please save them to a storage located outside the servers being updated.
4. Install a new version of the server side.

> **Warning!**
>
> Before installing server components make sure that server software and hardware match the recommended one (see i. 2.2 on page 22).

To update the server side, connect a local repository with new packages and do the following steps:

a) If the disk is inserted into the drive, mound it with the following command:
```
# mount /dev/cdrom /mnt/dvd/ -o loop
```
If the disk image is in the local directory (for example, `/opt/distr/infowatch/iwks-4.1.XXX-TME.iso`), use the following command: `# mount /opt/distr/infowatch/iwks-4.1.XXX-TME.iso /mnt/dvd -o loop`, where `XXX` is the number of a new version.

b) Edit the **/etc/yum.repos.d/rhel-dvd.repo** file the following way:
```
[rhel-dvd]
```

```
name=Kickstart_whole_system_rhel6
baseurl=file:///mnt/dvd/
enabled=1
gpgcheck=0

[rhel-dvd-iwtm]
name=IWTM_4.1.XXX_RPMs
baseurl=file:///mnt/dvd/infowatch/traffic-monitor-4.1.XXX/Linux
enabled=1
gpgcheck=0, где XXX – номер новой версии
```

c) Update packages using commands:
```
# yum remove iwtm-*
# yum install iwtm-*
```
d) If some errors occurred during the update, run the following command:
```
# yum remove iwtm-*
# yum install iwtm-*
```

5. Update the database schema.
   a) Copy a file with the schema from the `/mnt/dvd/infowatch/traffic-monitor-4.1.XXX/Linux/csw-4.1.XXX.tar.gz` (where XXX is the number of a new version) directory to the DB server and unpack with the following command:
   `tar xvfz csw-4.1.XXX.tar.gz,` where `XXX` is the number of the new version
   b) Make sure that the file **database.conf** contains correct data (you can copy connection parameters from the **database.conf** file of the previous installation)
   c) Run the command:
   `alter system set filesystemio_options=setall scope=spfile;`
   d) Restart the database:
   ```
   dbshut $ORACLE HOME
   service oracle restart
   dbstart $ORACLE HOME
   ```
   e) Run the database update script with the following command: ./`update.sh`.
6. Align files of the new version with the files that were saved at step 3.
7. On the database server, in the **/etc/cron.hourly/addm.cron** file, change the line:
   `find /home/oracle/addm/logs/ -maxdepth 1 -type f -name "*.txt" -name "*.html" -mtime 60 –delete`
   with the line
   `find /home/oracle/addm/logs/ -maxdepth 1 -type f \( -name '*.txt' -or -name '*.html' \) -mtime +60 -delete`
   Or you can change the whole **/etc/cron.hourly/addm.cron** file with the **/mnt/dvd/infowatch/extras** file.
8. Start the `iw-trafmon` and `iw-caserv` processes. On computers where Crawler is installed, start the `InfoWatch.Crawler.Server` and `InfoWatch.Crawler.Scanner` services.
9. Delete the installed Management Console and install a new version. You can find *.msi installation files with required interface languages in the `/mnt/dvd/infowatch/traffic-monitor-4.1.XXX/tm-management-console-windows/` directory.

> **Warning!**
>
> The old version of the Management Console should not be used for working with an updated database.

10. In case of distributed installation, the server side is updated on all computer while the database is update only on the computers where it is installed. Once the server side is updated on the computer where the database is installed, you should restart the computer and then update the database.

When the System is being updated, it does not receive objects. When the System is updated, it starts running in the standard mode.

# 4.2. Creating Database Backup

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

- *Defining the Size of Backup (i. 4.2.1 on page 71);*
- *Checking the Backup Storage (i. 4.2.2 on page 71);*
- *Creating Backup Directories (i. 4.2.3 on page 72);*
- *Creating Recovery Aid Files (i. 4.2.4 on page 72);*
- *Collecting a List of Files to Backup (i. 4.2.5 on page 73);*
- *Stopping IWTM System (i. 4.2.6 on page 74);*
- *Stopping Oracle Database (i. 4.2.7 on page 74);*
- *Copying Database Files to the Backup Storage (i. 4.2.8 on page 74).*

## 4.2.1. Defining the Size of Backup

**To define backup size:**

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

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

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

   Wait for **Connected** message.
3. 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);
   ```
4. Note the resulted databaser size.
5. Exit Oracle SQL*Plus:

   ```
   SQL> exit
   ```

## 4.2.2. 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.

# 4.2.3. 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
   ```

# 4.2.4. 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
   ```

# 4.2.5. 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
```

# 4.2.6. 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
```

# 4.2.7. 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
```

# 4.2.8. 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. 4.2.5 on page 73).

   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.

# 4.3. Restoring the Database from the Backup

The following procedure lets you to restore the database from the backup to the database server installed using kickstart installation program.

1. Stop Traffic Monitor processes:

```
OS:root> service iw-trafmon stop
```

```
OS:root> service iw-caserv stop
```

2. Stop database:

```
OS:root> su - oracle
OS:oracle> dbshut $ORACLE_HOME
OS:oracle> su –
```

3. Start Midnight Commander:

```
OS:root> mc
```

4. Delete the content of **/u02/oradata/** directory
5. Delete the content of **/u01/app/oracle/oradata/iwtm/** directory
6. Using WinScp copy the content of database backup from **/opt/IWTM_Backup_Files/IWTM/** directory to **/u02/oradata/** directory
7. Using WinScp copy the content of database backup from **/opt/IWTM_Backup_Files/Oradata/** directory to **/u01/app/oracle/oradata/iwtm/** directory
8. Rename **control01.ctl** located in **/opt/IWTM_Backup_Files/Oradata/** directory, as **control02.ctl** and copy it to **/u01/app/oracle/flash_recovery_area/iwtm/** directory:

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

9. Run database:

```
OS:oracle> dbstart $ORACLE_HOME
```

10. Check the database is succesfully started:

```
OS:oracle >cat  /u01/app/oracle/product/db_1/startup.log
```

The log should be as follows:

```
ORACLE instance started.
Total System Global Area 1970864128 bytes
Fixed Size                  2214656 bytes
Variable Size            1124074752 bytes
Database Buffers          788529152 bytes
Redo Buffers               56045568 bytes
Database mounted.
Database opened.
```

11. Check error log:

```
OS:oracle >tailf /var/log/alert_iwtm.log
```

# 4.4. Updating a Database Schema

1. Logon to the database as schema owner:

```
OS:oracle > sqlplus iwtm@iwtmOracle DBMS server is running
```

(using **wsqlplus** command instead of sqlplus is convenient)

2. Check there is no job running:

```
SQL:IWTM>SELECT job_name FROM user_scheduler_running_jobs;
```

If some jobs are running, wait the ending or eliminate the causes of their long-time execution

3. Check the planned jobs:

```
SQL:IWTM>select * from user_scheduler_jobs u where u.enabled = 'TRUE';
```

Suppose your query results the following list:

```
IWADDPARTS
IWTM_CHECK_MAIN_TS_OVERFLOW
IWTM_DELETE_OLD_LOGS
```

```
IWTM_POST_IDENTIFICATION
IWTM_SHRINK_TABLESPACES
IWTM_SYNC_INDEXES
```

If your list differs, please modify corresponding queries.

4. Disable jobs to prevent their running during update:

```
SQL:IWTM>
BEGIN
dbms_scheduler.disable('IWADDPARTS', true);
dbms_scheduler.disable('IWTM_CHECK_MAIN_TS_OVERFLOW',true);
dbms_scheduler.disable('IWTM_DELETE_OLD_LOGS',true);
dbms_scheduler.disable('IWTM_POST_IDENTIFICATION',true);
dbms_scheduler.disable('IWTM_SHRINK_TABLESPACES',true);
dbms_scheduler.disable('IWTM_SYNC_INDEXES',true);
COMMIT;
END;
/
```

5. Exit SQLPLUS

```
SQL:IWTM>exit
```

Log off if you are connected to the Oracle database through SQLDeveloper (or analogue).

6. Go to the directory containing database update script.

```
OS:root >cd /opt/distr/infowatch/csw-auto-install/csw-3.5.x.xxx/
```

where `3.5.x.xxx` is Traffic Monitor version.

7. Run database update script:

```
OS:root >./update.sh
```

8. Check database schema version:

```
SQL:IWTM> SELECT vers.get_schema_version FROM dual;
```

9. Check the status of planned jobs:

```
SQL:IWTM> select * from user_scheduler_jobs u where u.enabled = 'TRUE';
```

If some jobs are absent, enable them:

```
SQL:IWTM>
BEGIN
dbms_scheduler.enable('IWADDPARTS');
dbms_scheduler.enable('IWTM_CHECK_MAIN_TS_OVERFLOW');
dbms_scheduler.enable('IWTM_DELETE_OLD_LOGS');
dbms_scheduler.enable('IWTM_POST_IDENTIFICATION');
dbms_scheduler.enable('IWTM_SHRINK_TABLESPACES');
dbms_scheduler.enable('IWTM_SYNC_INDEXES');
COMMIT;
END;
/
```

10. Run TM services:

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

# 4.5. Modifying Files of New Version

**Warning!**

Changes in new version should be very significant (for example, configuration files structure or syntax was changed) then using the old files can damage System functionality.

So if you want to change default settings to ones you used before, please perform editing carefully taking into account changes described in Release Notes.

After System update, in the Management Console the **Scripts** section (**Navigation pane > Configuration**) will display both the old object processing scripts and the new one – **Default script of version [version_number]** where **[version_number]** is updated InfoWatch Traffic Monitor version.

Functions used in the script are different in InfoWatch Traffic Monitor of 4.1 version and previous ones (details on script functions see in «*InfoWatch Traffic Monitor. User Guide*»). That's because it we recommend you to modify a new **Default script of version [version_number]** alike an old script with respect to function changes.

**To transfer settings of the old script to the new one:**

1. Copy required sections of old script.
2. Paste copied sections to the text of a new script taking into account function changes.
3. Save **Default script of version [version_number]**.
4. Activate **Default script of version [version_number]**.

# CHAPTER 5. UNINSTALLING THE SYSTEM

Uninstalling of the InfoWatch Traffic Monitor system should be performed in the following order (all available components are listed; some of them can absent in specified configurations):

- *Database Scheme (i.5.1 on page 78).*
- *Remote Database Management Module (i.5.2 on page 79) – both client and server part.*
- *IW ICAP Module (i.5.3 on page 79).*
- *InfoWatch DeviceLock Adapter module – if used. Recommendations see in «InfoWatch DeviceLock Adapter. Installation and configuration guide» document.*
- *Traffic Monitor Server (i.5.4 on page 79).*
- *Sniffer – if installed apart (i.5.5 on page 80).*
- *Management Console (i.5.6 on page 80).*

## 5.1. Database Scheme

> **Warning!**
>
> Do not uninstall the database scheme from which daily tablespaces were detached for archival purposes. Otherwise you will not be able to recover data from these tablespaces.

### Step 7. Verification of Oracle DBMS server

Make sure that:

- Version of database scheme installed matches version of software package used for its removal.
- The Oracle DBMS server is running;
- Login and password for account with SYSDBA permissions (`sysdba` and `sysdba_password` setting values) are correctly specified in `database.conf` file.

### Step 8. Stopping Traffic Monitor

Before uninstalling you need to:

- Stop all Traffic Monitor Server processes:

  ```
  service iw-trafmon stop
  ```

- Close all instances of Management Console;
- Stop all connections to deleted database scheme from other programs.

### Step 9. Launch of scheme deletion

Run the following command:

```
sh uninstall.cmd
```

# 5.2. Remote Database Management Module

**To uninstall the remote database management module:**

1. On the computers where client and server parts of module are installed, run the following command:

   ```
   rpm -e iwtm_qmover
   ```

   If configuration file (`qmover.conf`) was changed during operations, it will be saved to the computer as `qmover.conf.rpmsave` after uninstalling the module.

2. On the client side (the interceptor of objects), from cron, delete all settings which change the bandwidth of the data transmission channel (for settings example see i. 3.2.6.1 on page 44, Step 2).

# 5.3. IW ICAP Module

If interception of HTTP requests over the ICAP protocol is no longer required you may disable IW_ICAP module.

**To disable the IW_ICAP module:**

1. Stop Traffic Monitor server processes:

   ```
   service iw-trafmon stop
   ```

2. Disable autorun of iw_icap process in `/usr/local/infowatch/tm3/etc/tm.conf` file, `[AUTO_RESTART]` section:

   ```
   iw_icap:
   autorestart = Off
   ```

3. Start Traffic Monitor server processes:

   ```
   service iw-trafmon start
   ```

4. Check the status of Traffic Monitor processes:

   ```
   service iw-trafmon status
   ```

5. Restore the original proxy settings (example of changing the settings see in i. 3.3.4 on page 54, Step 2).

If required, you can delete the rpm package of iwtm_icap.

**To delete the rpm package of the IW ICAP module:**

run the command:

```
rpm -e iwtm_icap
```

If configuration file (`qmover.conf`) was changed during operations, it will be saved to the computer as `qmover.conf.rpmsave` after uninstalling the module.

# 5.4. Traffic Monitor Server

Before uninstalling server part of Traffic Monitor you must uninstall:

- Remote database management module (both client and server part of the module: i.5.2 on page 79) – if Traffic Monitor server was used to load objects to remote database.
- IW ICAP module (i.5.3 on page 79) - if HTTP traffic was intercepted through integration with ICAP server.
- InfoWatch DeviceLock Adapter module – of it was installed as part of Traffic Monitor package to receive objects from DeviceLock. See recommendations for uninstalling in *"InfoWatch DeviceLock Adapter. Installation and Configuration Guide".*

**To uninstall Traffic Monitor server:**

1. Run the following commands:

   ```
   rpm -e iwtm_gpl_components
   rpm -e `rpm -qa | grep iwtm`
   ```

2. Reconfigure traffic interception components configured on Traffic Monitor.

| The traffic interception schema in InfoWatch Traffic Monitor | Required steps after InfoWatch Traffic Monitor is uninstalled |
|---|---|
| Intercepting a Copy of SMTP Traffic (Using a Mail Relay Server) | Make sure that the parameters of Postfix are restored (i.e. the values of the parameters are identical to the values when the System has not been installed yet). Changing Postfix parameters is covered in i.3.3.2 on page 49. |
| SMTP traffic is intercepted and filtered by the System (integration with Postfix) | Make sure that the parameters of Postfix are restored (i.e. the values of the parameters are identical to the values when the System has not been installed yet). Procedure to change Postfix settings is covered in i.3.3.2 on page 49.<br>Configure SMTP emails to be delivered by the corporate mail server and by-pass InfoWatch Traffic Monitor. |

After uninstalling, these elements remain on the computer:

- Modified configuration files (`tm.conf, detector.conf, qmover.conf, icap.conf`).

  `The .rpmsave` suffix is added to modified files (for example, `tm.conf.rpmsave`). The unchanged files will be deleted.
- Object queue.
- Classification
- The license file.
- The account of the user who owns InfoWatch Traffic Monitor and the group in which this user was included.

# 5.5. Sniffer

If the Sniffer and other Traffic Monitor Server components are installed on the same computer, Sniffer will be uninstalled together with Traffic Monitor (see i. 5.4 on page 79). A special uninstallation procedure is not required in this case.

**To uninstall Sniffer installed separately from other Traffic Monitor components:**

run the command:

```
rpm -e `rpm -qa | grep iwtm`
```

After uninstalling, these elements remain on the computer:

- `tm.conf` configuration file, if it was modified during operations. The file will be saved as `tm.conf.rpmsave`. The unchanged files will be deleted.
- The account of the user who owns InfoWatch Traffic Monitor and the group in which this user was included.

# 5.6. Management Console

**To delete the Management Console:**

1. Open **Add or Remove programs** component. To do this, from **Start** menu select **Settings ► Control Panel**. In the Control Panel window, double click the **Add or Remove Programs** component.
2. In the **Add or Remove Programs** window, select **InfoWatch Traffic Monitor Management Console** and click **Remove**.
3. Follow Wizard recommendations.

# Appendix 1. TROUBLESHOOTING

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

Invalid `ORACLE_HOME` environment variable in the `iw-trafmon autorun` script.

**Decision**

Open **autorun** script for 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.

**Solution**

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).

**The account of the Linux user is blocked.**

The incorrect password of the Linux user was specified when installing the Traffic Monitor Server.

**Solution**

Complete these steps to unlock the account of the Linux user:

1. To stop all Traffic Monitor processed run the following command:

   ```
   service iw-trafmon stop
   ```

2. In `/usr/local/infowatch/tm3/etc/tm.conf` file, specify the login and password for Linux user (`[ORACLE]` section, `Username` and `Password` settings correspondingly).

3. Unlock the user account of the Linux user by running the SQL *Plus command:

   ```
   ALTER USER user_name_of_the_Linux_user ACCOUNT UNLOCK
   ```

4. To start all Traffic Monitor processes run the following command:

   ```
   service iw-trafmon start
   ```

# Appendix 2. THIRD-PARTY LICENSES

System contains third-party components distributed under MIT License (http://www.opensource.org/licenses/mit-license.html):

- Lua – http://www.lua.org/license.html
- LuaBind – http://www.rasterbar.com/products/luabind.html
- libxml2 – http://www.xmlsoft.org/

The system also contains software

- Distributed under BSD license (http://www.opensource.org/licenses/bsd-license.php):
  - Stringencoders – http://code.google.com/p/stringencoders/
- Distributed under GNU GENERAL PUBLIC LICENSE license (http://www.gnu.org/licenses/gpl-2.0.html):
  - Pdftotext http://www.foolabs.com/xpdf/
  - Tnef http://sourceforge.net/projects/tnef/
  - Unzip http://www.info-zip.org/UnZip.html
  - libcole.so arturo@directmail.org; andy.scriven@research.natpower.co.uk
  - libhtmltree.so pauljlucas@mac.com

# GLOSSARY

**Active Directory**

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

**Administrator**

Preset role and management console account that has privileges for managing other accounts and their rights. See 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

**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**

Preset 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; doesn’t support detecting text objects and digital prints or working with responsibility zones. See also: Copy Mode, Responsibility Zone

**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.