

INFOWATCH

InfoWatch Traffic Monitor 6.10

Installation Guide

05/14/2021

© JSC “InfoWatch”

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

http://www.infowatch.com

TABLE OF CONTENTS

1 Introduction 4
1.1 Who Should Read this Guide 4
1.2 Set of Documents 4
1.3 Technical Support 4
2 Getting Ready to Install 5
2.1 System Deployment Schemes and Installation Types 5
2.2 Hardware and Software Requirements 6
3 Installing the System 16
3.1 Installing Traffic Monitor Server and Database 17
3.1.1 General Information on Installation Steps for Server Components 17
3.1.1.1 Start Window 18
3.1.1.2 Selecting the Database 19
3.1.1.3 Selecting the Installation Mode 19
3.1.1.4 Choosing a Time Zone 20
3.1.1.5 Setting Password for System Superuser 21
3.1.1.6 Choosing disk partitioning method 21
3.1.1.7 Network Settings 24
3.1.1.8 Configuring Time Synchronization (NTP-server) 27
3.1.1.9 Localization Setting 28
3.1.1.10 Configuring the Automatic Event Deletion from the Database 30
3.1.1.11 Completing the Installation 32
3.1.2 All-in-one Installation Mode of TM Enterprise and TM Standard 32
3.1.3 Distributed Installation of TM Enterprise 39
3.1.3.1 Installing Database 40
3.1.3.2 Installing Traffic Monitor Server 44
3.2 Installing Crawler Subsystem 46
3.3 Installing InfoWatch Device Monitor 51
3.3.1 InfoWatch Device Monitor Server End Setup 51
3.3.1.1 Database deployment managed by Microsoft SQL Server DBMS 51
3.3.1.2 Database deployment managed by Oracle DBMS 52
3.3.1.3 Database deployment managed by PostgreSQL DBMS 53
3.3.1.4 Server Setup Recommendations 53
3.3.1.5 InfoWatch Device Monitor Server End Installation Procedure 54
3.3.2 InfoWatch Device Monitor Agent Installation 64
3.3.2.1 Standard Agent Installation 66

3.3.2.2 Agent Installation via Software Distribution Tools 66
3.3.3 Deployment Scheme for InfoWatch Device Monitor 70
3.4 Pre-installed Server Parameters 73
4 Updating the System 75
4.1 Updating TM All-in-one Enterprise and Standard 79
4.2 Updating TM in case of distributed installation 92
4.3 Updating Crawler Subsystem 116
4.4 Updating InfoWatch Device Monitor 116
4.4.1 Updating InfoWatch Device Monitor Server End 117
4.4.2 Updating InfoWatch Device Monitor Agent 118
4.5 Merging Configuration Files 119
4.5.1 Merging configuration files in Midnight Commander 119
4.5.2 Merging configuration files by means of vimdiff 121
4.6 Updating PostgreSQL DBMS 122
4.6.1 Prepare for update 122
4.6.2 Update 124
4.6.3 Old DB backup removal 124
4.6.4 Update rollback 125
4.6.5 Error alert 126
5 Uninstalling the System 127
5.1 Deleting the Database Scheme 127
5.2 Deleting Crawler Subsystem 128
5.3 Uninstalling Device Monitor 129
5.3.1 Remove Agent Installed via Software Distribution Tools 130
6 Appendix A. Username and Password Recommendations 131
7 Appendix B. Licenses for Third-Party Technologies 133

1 Introduction

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

1.1 Who Should Read this Guide

This document is intended for InfoWatch company technical support service and support engineers of InfoWatch partner companies.

1.2 Set of Documents

For more information see the following documents:

- «*InfoWatchTraffic Monitor. Installation Guide*».

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

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

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

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

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

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

The document describes the frequently used configuration files.

1.3 Technical Support

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

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

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

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

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

2 Getting Ready to Install

In this chapter, you can find information on;

- System Deployment Schemes and Installation Types;
- Hardware and Software Requirements.

2.1 System Deployment Schemes and Installation Types

InfoWatch Traffic Monitor features depend on the installation mode, the database in use (Oracle / PostgreSQL), and the edition (Standard / Enterprise).

The following typical solutions can be:

- **InfoWatch Traffic Monitor Standard** is a solution for companies using up to 500 workstations. It has a set of restrictions as compared to Enterprise version (see details in the table below). The solution is deployed on a single server.
- **InfoWatch Traffic Monitor Enterprise** is an integrated scalable solution with a flexible configuration of components. The most extensive configuration can include the following components:
  - **Traffic Monitor Server** enables operation of interceptors (IW_SNIFFER, IW_ICAP and IW_SMTPD), the analysis subsystem, and the Policy Applying subsystem. In some cases, several Traffic Monitor servers should be used: this enables more efficient operation of loaded processes. Besides, you should take into account that some processes should run on one server only (see details in "Checking Process Autorun" article of the Administration Guide).
  - **Database** is Oracle or PostgreSQL DBMS server.

    > **Note:**
    >
    > You should not install or run applications (especially server ones) on Traffic Monitor or Database server or use it as a file server.

  - **Device Monitor** is an interception module designed as server part with Management console and Agents deployed to computers and mobile devices of a company. See description of this module in "InfoWatch Device Monitor. User Guide".
  - **Crawler** is an interception module designed as server and scanner services.
  - **Connectors** are a set of interception modules for integration with external systems.
  - **Management console** is a web interface for System managing designed as a set of processes which should run at the only one Traffic Monitor server (see details in "Checking Process Autorun" article of the Administration Guide).

The following table describes the functional difference between System editions depending on the database in use.

Feature	TM Enterprise		TM Standard
	TM Enterprise Oracle	TM Enterprise PostgreSQL	TM Standard PostgreSQL

Storage period of intercepted data	Limited by storage size only	Limited by storage size only
Computers control	Control of using removable devices, communication ports, print control	Optional (the availability of InfoWatch Device Monitor computer control module using depends on data size and required storage period)
Scalability	The solution can be adapted for servicing a large number of employees (tens of thousands) scaling the company growth. Can be used for geographically-distributed company branches connected by any communication channels	Designed for companies with up to 500 employees
Blocking traffic transfer when the violation was found	Yes	Optional (implementation is held by certified engineers only)
Integration scheme	Several options available: "in-line" integration, ICAP support, intercepting the traffic copy (SPAN, port mirroring, etc.)	Operating in traffic copy mode ("in-line" integration is optional)

There are following installation types:

- *All-in-one Standard* – all the System components (together with Oracle Standard or PostgreSQL DBMS) are installed on the same server. This installation type is used if, with respect to the assumed load, the server has resources for DBMS and TM services.
- *All-in-one Enterprise* – all the System components (together with Oracle Enterprise or PostgreSQL DBMS) are installed on the same server. This installation type is used if, with respect to the assumed load, the server has resources for DBMS and TM services.
- *Traffic Monitor Server* + *Database* – Traffic Monitor Server and DBMS (Oracle Enterprise or PostgreSQL) are installed on different computers. This installation type is used if, with respect to the assumed load, DBMS and TM services cannot efficiently operate on the same server.

Warning!

After installation, the Administrator configures the System depending on implementation purposes (see "*InfoWatch Traffic Monitor. Administration Guide*", "Configuring the System after Installation").

2.2 Hardware and Software Requirements

Hardware requirements for Traffic Monitor Server are defined basing on the installation type, the estimated load on the System and parameters of the network, where the System is installed. Therefore, equipment specification is determined individually in each case.

Variants of the System deployment schemes are described in "System Deployment Schemes and Installation Types". According to the article, there can be the following elements to install:

- **Server for "All-in-one" installation** is used for the following editions:
- TM Standard - the Stanadard solution installation. *See the requirement for standalone TM Enterprise server*.
- TM Enterprise - the Enterprise solution is installed in "All-in-one" mode. *See the requirements for standalone TM Enterprise server.*
- **Traffic Monitor Server** – standalone server or cluster of TM Enterprise servers. *See the requirements below.*
- **Database Server** – server for Oracle or PostgreSQL DBMS. You should not install or run applications (especially server ones) on it or use this computer as a file server. *See requirements below.*
- **Crawler Server and Crawler Scanner** – Windows services. *See the requirements below.*
- **Connectors** – their requirements are listed in the documentation supplied with connectors software.
- **Device Monitor Server and Device Monitor Agents** – the module, based on Windows systems and containing the agents on Windows and Linux systems, as well as the mobile devices. See the requirtements below.
- **Management Console** is automatically installed together with Traffic Monitor Server and does not impose any additional hardware or software requirements for the server. To access Management Console, you should use Google Chrome browser of actual version.

The Traffic Monitor Server hardware and software requirements are varied in a great range. So, the minimal configuration supposes following constraints:

- OCR is disabled for all interceptors;
- server does not accept data from Device Monitor and Crawler.

A significant difference in the load on a certain interception channel can also influence the number and role of Traffic Monitor Servers: for example, the efficient traffic processing from Device Monitor you need to dedicate a separate server for **iw_xapi_xapi** process and as per the traffic from Crawler a separate server for **iw_expressd** process should be used.

Estimated minimal software and hardware requirements are listed in the following table. We strongly recommend you to make a detailed configuration computation with the assistance of InfoWatch experts or specialists of partner company from which you have purchased the product.

Disk subsystem	Processor	RAM	Software	Additional requirements
TM Standard server				
RAID-array with fault tolerance: 300 GB	2CPU 6xC, 2,6 GHz	24 GB	OS Red Hat Enterprise Linux 6.8 x64	The server should have a network interface with the assigned IP address. If interceptors are used on the server, requirements imposed by the interceptors should be fulfilled**
TM Enterprise server, less than 10 GB/day				

Disk subsystem	Processor	RAM	Software	Additional requirements
RAID-array with fault tolerance: 600 GB	2CPU 8xC + Hyper-threading (Intel® Xeon® Processor E5-2640 v3 - 2,6 Hz)	24 GB	OS Red Hat Enterprise Linux 6.8 x64	The server should have a network interface with the assigned IP address. If interceptors are used on the server, requirements imposed by the interceptors should be fulfilled**
TM Enterprise server, from 10 GB/day to 50 GB/day				
RAID-array with fault tolerance	2SRVx2CPU 10xC	32-48 GB for each server	OS Red Hat Enterprise Linux 6.8 x64	The server should have a network interface with the assigned IP address. If interceptors are used on the server, requirements imposed by the interceptors should be fulfilled**
TM Enterprise server, more than 50 GB/day				
RAID-array with fault tolerance	Calculated on demand	From 32GB for each server	OS Red Hat Enterprise Linux 6.8 x64	
Oracle DB or PostgreSQL server (Provides storage for traffic of 1-2 thousand users by 3 months; if OCR and Device Monitor are used, then requirements are calculated on demand)				
RAID-array with fault tolerance: 500 GB	2CPU от 6xC, 2,6 GHz	16GB and more depending on data volume, insertion and processing speed	OS Red Hat Enterprise Linux 6.8 x64	
Crawler server and scanner				

Disk subsystem	Processor	RAM	Software	Additional requirements
30 GB of free space - for the server and the scanner: required for temporary storage of files that are copied from checked resources and for installation purposes	From 2 cores	From 2 GB	OS: • [1]Microsoft Windows Vista Service Pack 2; • *Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8; • Microsoft Windows Server 2008 R2 Service Pack 1; • Microsoft Windows Server 2012. Platform: • Microsoft .Net Framework 4.5.1	• **iw_expressd** process autorun should be enabled on the TM server (see details in «*InfoWatch Traffic Monitor. Administration Guide*») • Both Crawler Server and Scanner should be installed on computers located in the same domain which includes all workstations supposed to be scanned. • It is recommended that a computer where Crawler scanner works should be located in the network segment maximum close to segments to be scanned. Otherwise, the network load may increase significantly. • If network segments where InfoWatch Traffic Monitor with Crawler is deployed are divided by firewalls, then for correct operation of Crawler, the 1337 TCP port (Traffic Monitor connects to Crawler server) and 6556 TCP port (Crawler scanner connects to Crawler server) must be opened.
Device Monitor server				

Disk subsystem	Processor	RAM	Software	Additional requirements
Not less than 1 GB free space for installation	From 2 cores	From 2 GB	OS (x86 and x64 platforms are supported): • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016. Platform: • Microsoft .Net Framework 4.5.1. DBMS client: • Oracle Database 11; If you install Device Monitor on x64 server OS, using x64 Oracle Client application is required;	▪ Autostart for **iw_xapi_xapi** process should be enabled on TM server ▪ Local DNS is required to convert domain names into addresses ▪ FIPS mode should be disabled

Disk subsystem	Processor	RAM	Software	Additional requirements
			• Microsoft SQL Server 2005, 2008, 2012, 2014, 2016 (Standard, Enterprise); • PostgreSQL version 9.	
Device Monitor Agent for workstations				

Disk subsystem	Processor	RAM	Software	Additional requirements
Not less than 320 GB free space for temporary storage of files which are then sent for analysis	From 2 cores	From 2 GB	OS: • [1]Microsoft Windows XP Professional Service Pack 3 with all the updates; • [1]Microsoft Windows Vista Service Pack 2; • [2]Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 and 8.1; • Microsoft Windows 10; • [1]Microsoft Windows Server 2003; • [2]Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2.	Local DNS is required to convert domain names into addresses
Device Monitor Agent for mobile devices				

Disk subsystem	Processor	RAM	Software	Additional requirements

No requirements: the agent is installed on a mobile device with a specific configuration. See the list of supported devices below.	No requirements: the agent is installed on a mobile device with a specific configuration. See the list of supported devices below.	No requirements: the agent is installed on a mobile device with a specific configuration. See the list of supported devices below.	No requirements: the agent is installed on a mobile device with a specific configuration. See the list of supported devices below.	The following device configurations on Android platform are supported:
				• InfoWatch Taigaphone (entrusted firmware)
				• on Android platform:
				  • LG Nexus 5X (Nexus 5X), Android 6.0.1 version (firmware version MTC20K)
				  • Samsung Galaxy A3 2017 (SM-A320F), Android version 6.0.1 (firmware version MMB29K.A320FXXU1AQA1)
				  • Samsung Galaxy A5 (SM-A510F), Android version 6.0.1 (firmware version MMB29K.A510FXXU2BPH6)
				  • Samsung Galaxy J1 (SM-J120F), Android version 5.1.1 (firmware version LMY47X.J120FXXU1AOL2)
				  • Samsung Galaxy S6 (SM-G920F), Android version 6.0.1 (firmware version MMB29K.G920FXXU4DPJN)
				  • Samsung Galaxy Tab A (SM-T355), Android 6.0.1 version (firmware version MMB29M.T355XXU1BQA2)
				  • Samsung Galaxy Tab Active (SM-T365), Android 5.1.1 version (firmware version T365XXU1BOL1)

Device Monitor Management Console				

Disk subsystem	Processor	RAM	Software	Additional requirements
Not less than 35 MB	Same as for used OS	Same as for used OS	OS: • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • [1]Microsoft Windows Vista Service Pack 2; • Microsoft Windows 7 Service Pack 1 • Microsoft Windows 8 and 8.1; • Microsoft Windows 10.	

Note!

[1] - marked OS is not supported starting from version 6.10.21.

[2] - starting from version 6.10.21 the marked OS require the following Microsoft updates: KB4474419, KB4490628 and KB2921916. The System is intended to check the computer for bug fix before starting the installation and/or update. Starting from version 6.10.22 the marked OS do not require KB2921916 Microsoft updates.

Note:

You can install the System to the virtual environment: VMware, MS Hyper-V or other virtualization systems.

Device Monitor agents activity is supported within Citrix 6.0, 7.6, 7.13, 7.14 and 7.15 LTSR virtualisation environment.

*There are no software requirements for the server: the kickstart installer formats the hard drive and installs all required software.

** Traffic Monitor server can use interceptors which impose additional requirements:

- **iw_sniffer** can get a traffic copy from a switch with SPAN / Port Mirroring function (Cisco Catalyst 2960 Series is recommended) with a port configured for TRx mode (BOTH - receiving and sending within the same connection).
- **iw_icap** handles ICAP client built in any proxy server confirming RFC 3507 standard (for example SQUID 3.4.x or higher, Cisco IronPort S10 and Blue Coat SG Series). Please consult with InfoWatch support service before using a certain model to confirm the compatibility with IW ICAP module. The proxy server should contain ICAP license; enabling ICAP support is performed according to support documentation of certain proxy server.

3 Installing the System

This section contains instructions for each type of the System installation.

See information on how to choose the installation type in "System Deployment Schemes and Installation Types".

Details on deployment this schemes in the existing infrastructure are described in «*InfoWatch Traffic Monitor. Administration Guide*».

> **Warning!**
>
> Before the installation, make sure that the environment, where the System will be deployed meets software and hardware requirements (see "Hardware and Software Requirements").

Installation of the server components of the InfoWatch Traffic Monitor system is performed using **kickstart** installer.

Depending on the server purpose, a different set of components is installed:

Server purpose	Kickstart key	Components installed by kickstart
All InfoWatch Traffic Monitor (Enterprise or Standard) components are installed on the same computer	**TME All-in-one (RHEL)** **TMS All-in-one**	• Installing OS Linux • Configuring network interface • Installing and configuring DBMS Oracle (only for **TME All-in-one**) or PostgreSQL • Installing IW Traffic Monitor database schema • Installing RPM packages of IWTM Server • Installing Monitoring subsystem • Installing Management Console
DBMS Server with Traffic Monitor DB schema is installed on a separate computer	**TME DB server (RHEL)** **DB node (Astra Linux)**	• Installing OS Linux • Configuring network interface • Installing and configuring DBMS Oracle or PostgreSQL • Installing IW Traffic Monitor database schema
Traffic Monitor Server on the separate computer	**TME Node server (RHEL)** **TM node (Astra Linux)**	• Installing OS Linux • Configuring network interface • Installing RPM packages of IWTM Server • Installing Monitoring subsystem • Installing Management console

You can find information on the desired installation type in the following articles:

- Installing the System
- General Information on Installation Steps for Server Components
- All-in-one Installation Mode of TM Enterprise and TM Standard
- Distributed Installation of TM Enterprise

    - Installing Database
    - Installing Traffic Monitor Server
- Installing InfoWatch Device Monitor (optionally)
- Installing Crawler Subsystem (optionally)

For information on pre-installed accounts, see "Pre-installed Server Settings".

When installation of the server components is finished, the Management console is available through the browser window by entering the URL:

- of the Traffic Monitor Server – if All-in-one installation mode is used;
- of the primary Traffic Monitor Server (server, where `web-gui` pack is installed) – if the System components are installed on different computers.

Information on allocating of the primary server in a distributed installation mode is provided in the document "*InfoWatch Traffic Monitor. Administration Guide*", "*Additional Settings when Installing with TME DB Server and TME Node Server keys*" article.

3.1 Installing Traffic Monitor Server and Database

You can find information on installing Traffic Monitor on Red Hat Enterprise Linux operating system in the following sections:

- General Information on Installation Steps for Server Components
- All-in-one Installation Mode of TM Enterprise and TM Standard
- Distributed Installation of TM Enterprise

3.1.1 General Information on Installation Steps for Server Components

This section contains a description of installation steps which are common for all types of installing server components of the System:

- Start Window
- Selecting the Database
- Selecting the Installation Mode
- Choosing a Time Zone
- Setting Password for System Superuser
- Choosing a Disk Partitioning Method
- Network Settings
- Configuring Time Synchronization (NTP-server)
- Localization Setting
- Configuring the Automatic Event Deletion from the Database
- Completing the Installation

Start Window



The first screen of the Installation Wizard (**kickstart**) allows you to select one of the following actions:

- **TM Enterprise** – begins InfoWatch Traffic Monitor Enterprise installation
- **TM Standard** – begins InfoWatch Traffic Monitor Standard installation

> **Important!**
>
> **TM Standard** edition is available only in **TMS All-in-one** mode: **TM+DB server - PostgreSQL**. In this mode, "Selecting the Database" and "Selecting the Installation Mode" steps will be omitted.

- **Boot from local drive** – loads from a local computer disk.
- **Rescue installed system** – emergency recovery of InfoWatch Traffic Monitor system. This option should be used by InfoWatch engineers only.
- **Memory test** – hardware test (can take some time). Used a supportive option, once required.

> **Note:**
>
> To review additional loading options press **F1**.
> Due to major complexity, additional options should be used by InfoWatch engineers only.

Selecting the Database



If you have chosen the Enterprise edition, you will be prompted to select the DBMS:

- **DB - Oracle Enterprise**
- **DB - PostgreSQL**

Details on installation type selecting see in "System Deployment Schemes and Installation Types".

Press **Enter**.

Selecting the Installation Mode

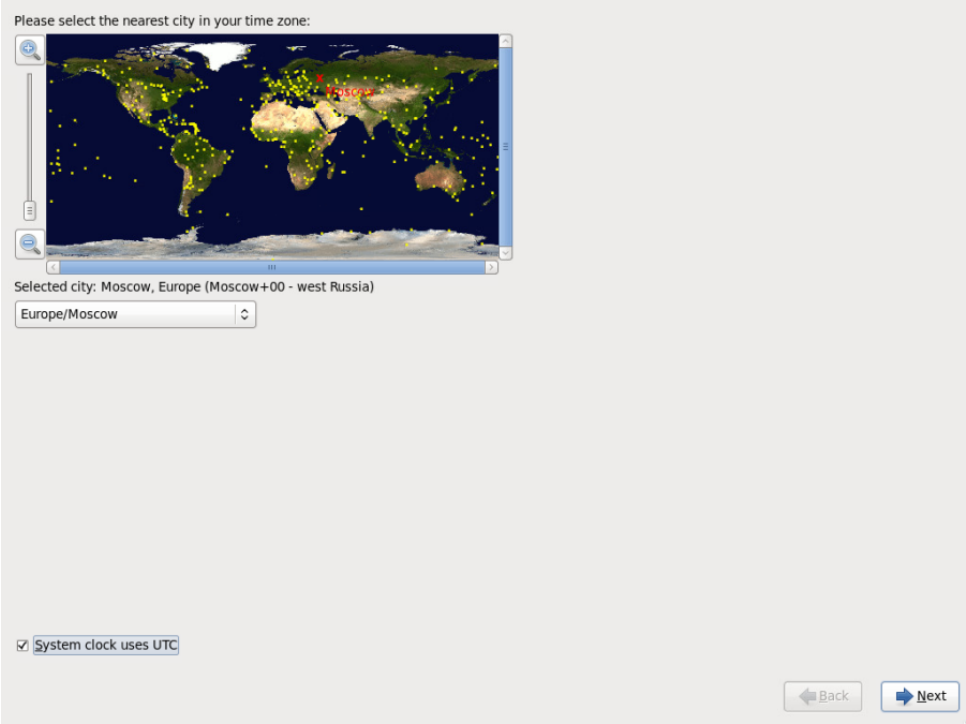


When you have selected the DBMS, you will be prompted to select the installation mode. The set of modes depends on what you selected at the previous steps. The can be the following modes:

- **TME All-in-one: TM+DB server** (**PostgreSQL** or **Oracle**) – all System components (with Oracle DBMS or PostgreSQL) are installed on the same server. This installation type is used if, with respect to the assumed load, the server has resources for DBMS and TM services. See details in "All-in-one Installation Mode of TM Enterprise and TM Standard".
- **TME DB server** (**PostgreSQL** or **Oracle**) – installation of the database together with a selected DBMS on the separate computer. See details in "Installing Database".
- **TME Node server** (**PostgreSQL** or **Oracle**) – installation of the Traffic Monitor Server on a separate computer. See details in "Installing Traffic Monitor Server".

See details on chosing the installation mode in "System Deployment Schemes and Installation Types".

Choosing a Time Zone



Specify settings of the time zone for the server.

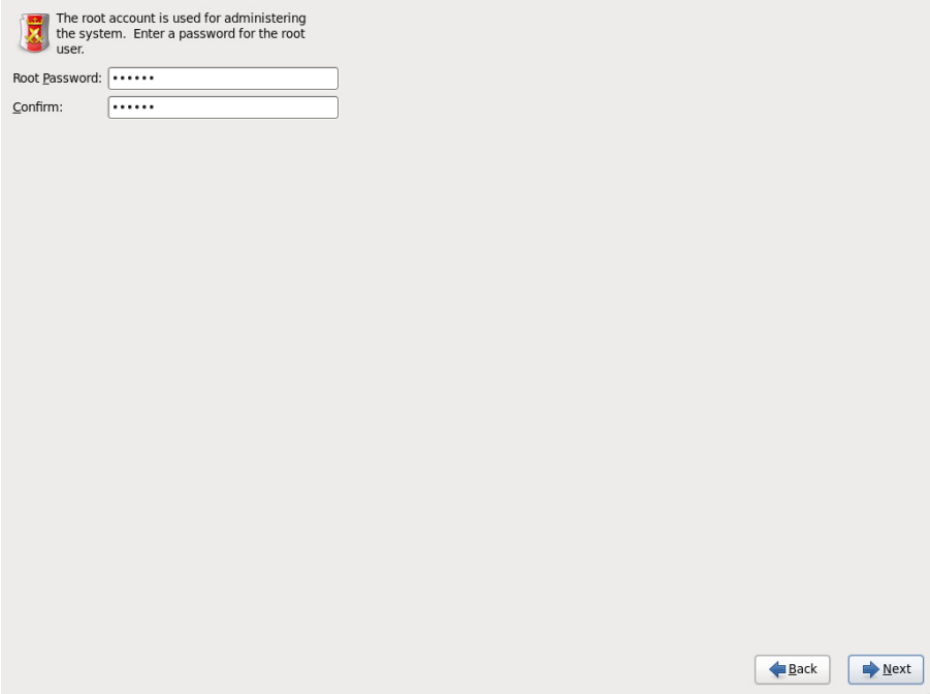
You can find your city:

- In the drop-down list. The cities are sorted based on a part of the world they belong to. For example, Moscow is included into Europe group;
- On the map. For navigation, use a scroll-bar and scale buttons.

Mark the **System clock uses UTC** checkbox if system time is set to Greenwich time (UTC).

Click **Next**.

Setting Password for System Superuser



root user is the System superuser. For the *root* user, a password must be specified.

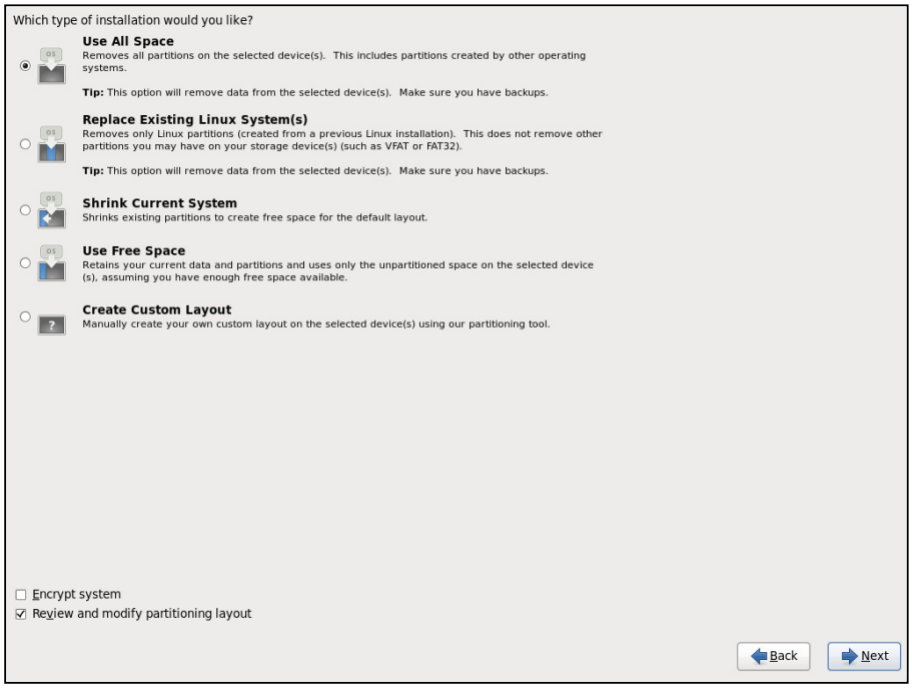
> **Note:**
>
> Recommendations on password creation are available in Appendix A .

In case your password does not match safety requirements, you will see a warning **Weak Password**. Use the following buttons:

- **Use anyway** – if you want to use an entered password despite recommendations;
- **Cancel** – if you want to change the entered password.

Choosing disk partitioning method

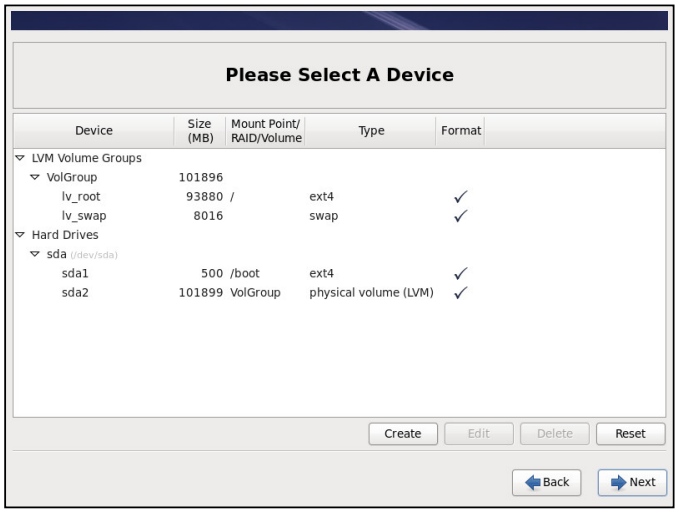
> **Warning!**
>
> When the System is installed, its components are located in the following directories:
>
> - InfoWatch Traffic Monitor – `/opt/iw`;
> - Database – `/u01` and `/u02`.



Now, you need to specify how the installer should split the disk space (for recommendations, see "Recommendations to Partition Server Disk Space during Installation in Different Modes."). On InfoWatch Traffic Monitor server, the disk space is used only by the System, so at this step, select **Use All Space**.

> **Important!**
>
> This will delete all partitions of the device(-s) including partitions that were created by other operating systems. *Make sure that all required data have been backed up!*

To split the disk space or just to make sure that the default settings are correct, select the **Review and modify partitioning layout** option and click **Next**.

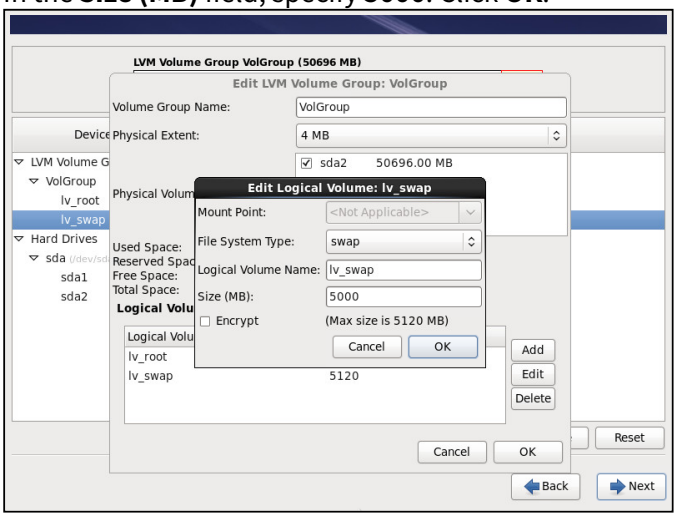


In most cases, you do not need to change the default partition. If the installation is distributed and Oracle DBMS is used, we recommend allocating at least 100 GB of the disk space for the */root* partition.

If you want to make changes, use standard tools for working with disks that are available in the installer.

For example, you need to change the size of *lv_swap* partition to *5000*:

1. In the **Please Select A Device** window, select **lv_swap** partition and click **Edit**.
2. In the **Size (MB)** field, specify **5000**. Click **OK**.

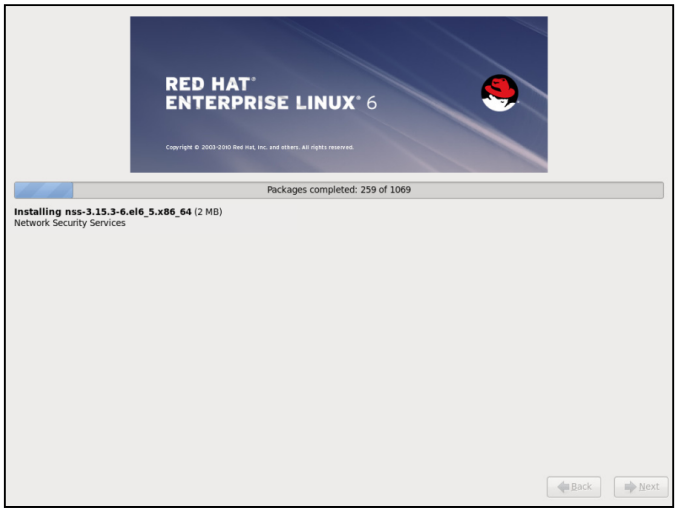


3. In the **Please Select A Device** window, select **lv_root** partition and click **Edit**.
4. In the **Size (MB)** field, specify all remaining disk space (is displayed under the **Max size is**... field) . Click **OK**.
5. Click **Next** in the **Please Select A Device** window.

Once you have configured the partition and clicked **Next**, the process of disk partitioning and then the OS installation will start.

> **Note:**
>
> The screen may display the **Format Warnings** window which informs you that hard disk volumes needed for the installation will be formatted. To continue the installation, click **Format**.

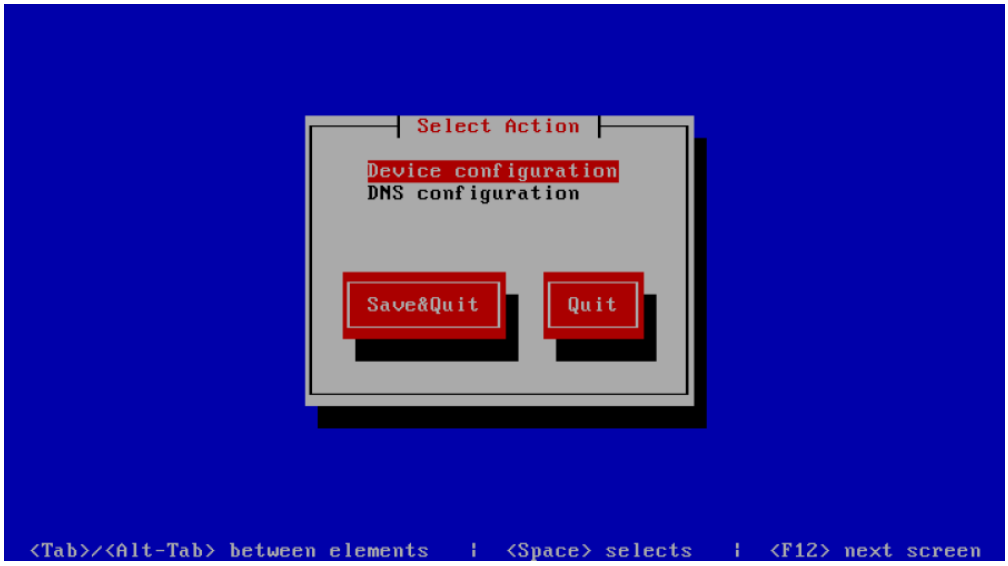
The progress is displayed on the screen:



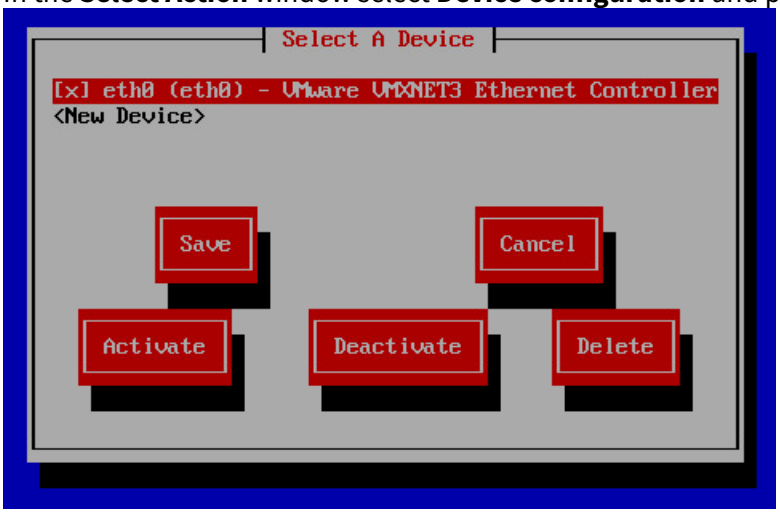
The process can take some time.

When the operating system is installed, the computer will be restarted and you will be prompted to configure the network settings (see "Network Settings").

Network Settings

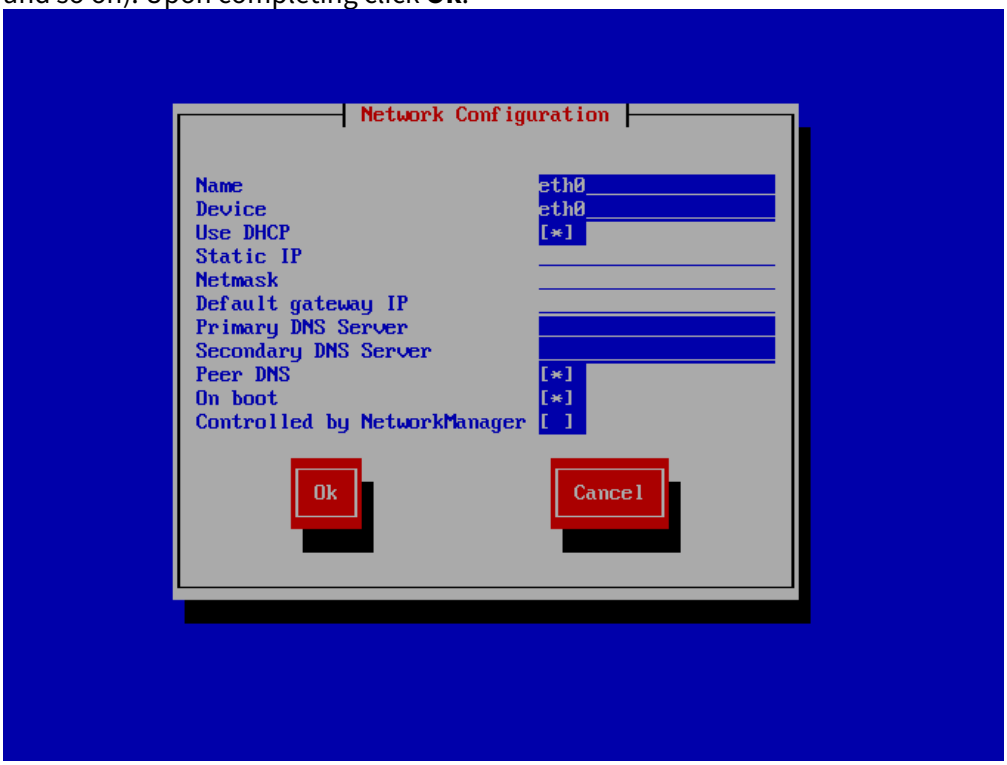


1. To set up parameters of a network card:
   a. In the **Select Action** window select **Device configuration** and press **Enter**.



   b. In the **Select A Device**window select network interface **eth0** and press **Enter**.
   c. if you want the System to use network settings from DHCP server, set the cursor in the **Use DHCP** field and click space. Otherwise enter network settings manually (static IP address

and so on). Upon completing click **Ok**.

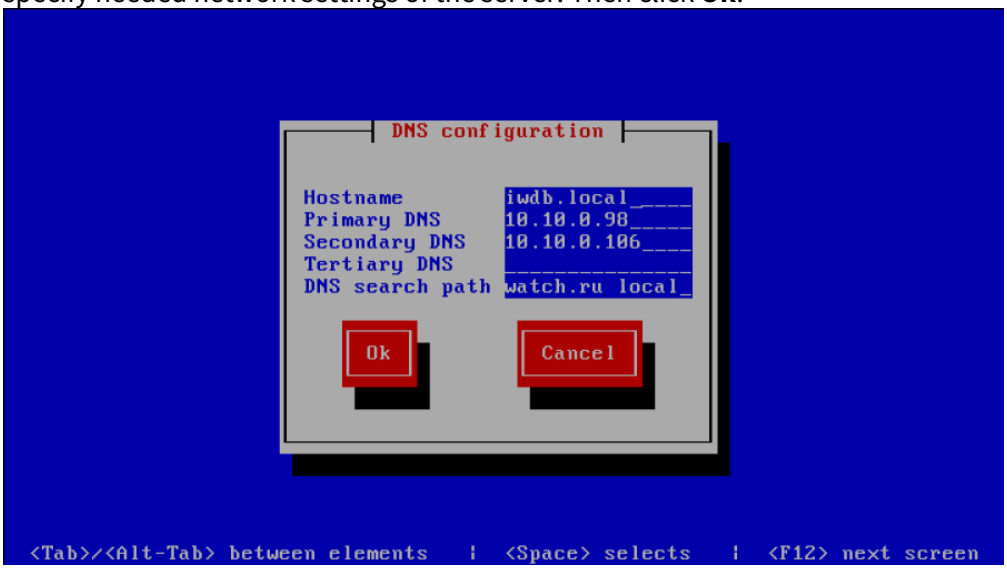


> **Warning!**
>
> Do not use **Controlled by NetworkManager** option.

> **Warning!**
>
> When using **Use DHCP** setting, the System will use only data gained from specified DHCP servers. Data entered to the **DNS configuration** window (see further) will be ignored. If you change `/etc/resolv.conf` file manually, iths data will be replaced by gained from DHCP server after the next server reboot.

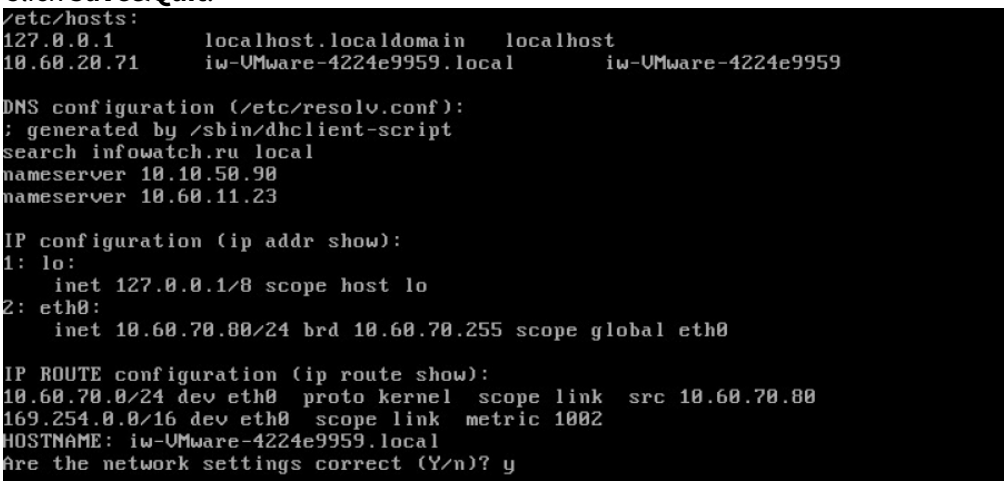
d. Click **Save** to save settings.

2. To configure DNS configuration in the **Select Action** window select **DNS configuration** and specify needed network settings of the server. Then click **Ok**.



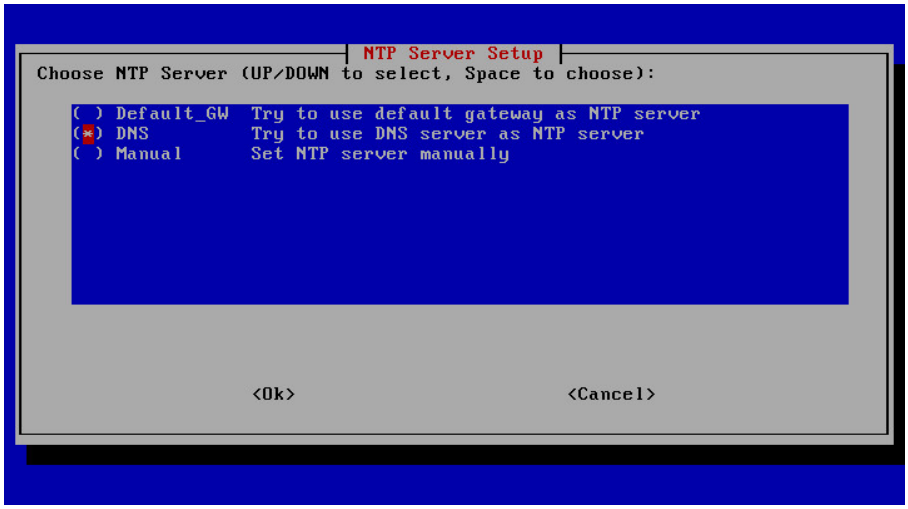
> **Warning!**
>
> If you select **Use DHCP** in the **Network Configuration** window then instaed of parameters you specified the ones received fron DHCP will be used.

3. Click **Save&Quit**.



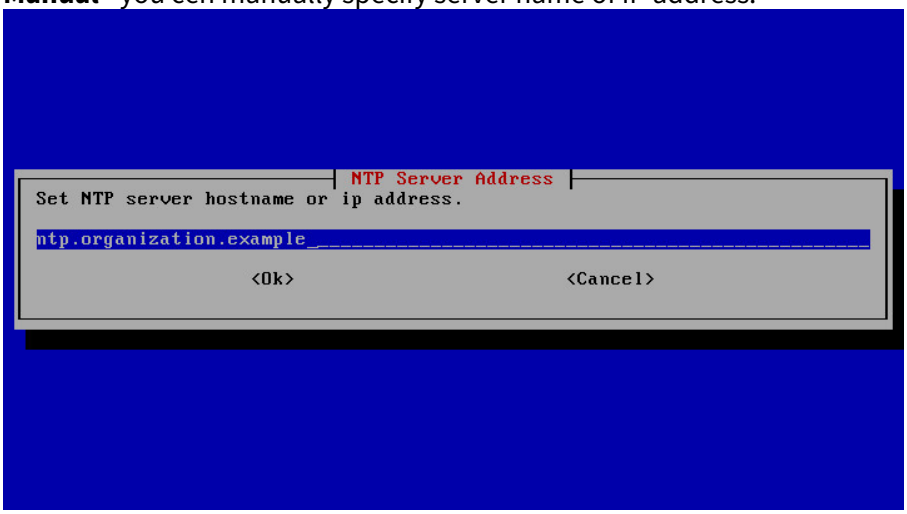
4. Examine the network settings you specified. If settings are wrong, enter **N** and specify the correct ones (see previous steps) If settings are correct, enter **Y** to confirm and press **Enter**.

Configuring Time Synchronization (NTP-server)



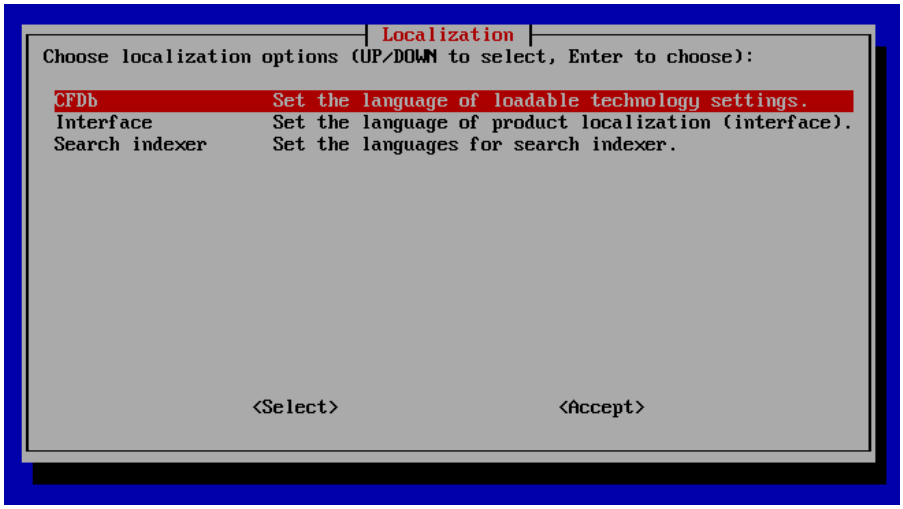
You can select one of three server setup options for time synchronization (NTP-server). Set asterisk symbol (*) in the required field and press space then click **OK**.

- **Default_GW** - default gateway
- **DNS** - domain controller: usually used in organizations as a time server
- **Manual** - you cen manually specify server name of IP address.



If NTP server cannot be specified for some reasons, click **Cancel** and set this parameter later; details on configuring the NTP server see in «*InfoWatch Traffic Monitor. Administration Guide*».

Localization Setting



To specify System localization parameters:

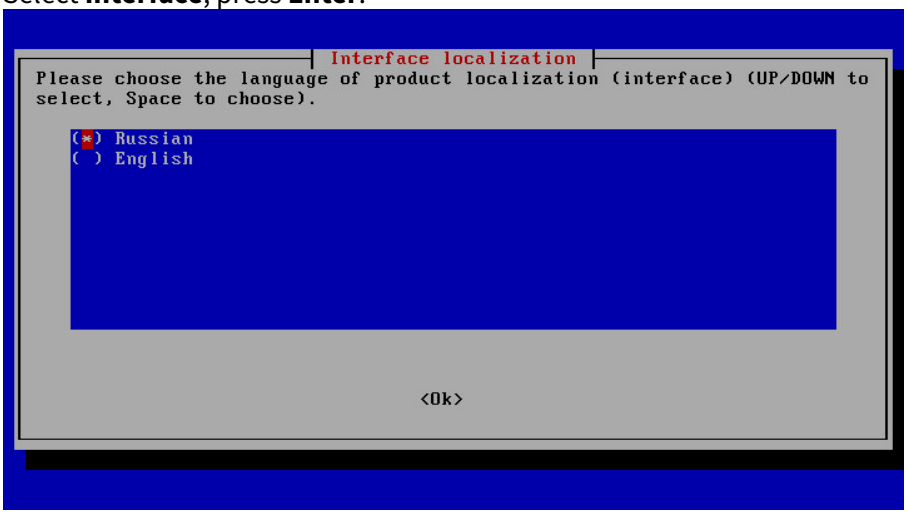
1. Specify language settings for such preinstalled units as categories and terms, списки, preinstalled filters and default policies:
   a. Select **CFDb** and press **Enter**.



   There are three languages available::
   - *Russian* – to install the Classifier in Russian;
   - *English* – to install the Classifier in English;
   - *Malaysian* – to install the classifier in Malaysian.

   To select the language set the cursor on the needed field and click space keyboard key until an asterisk (*) appeared. You can select one, two or three languages.
   b. Press **OK**.
2. Specify language for Management Console:

a. Select **Interface**, press **Enter**.

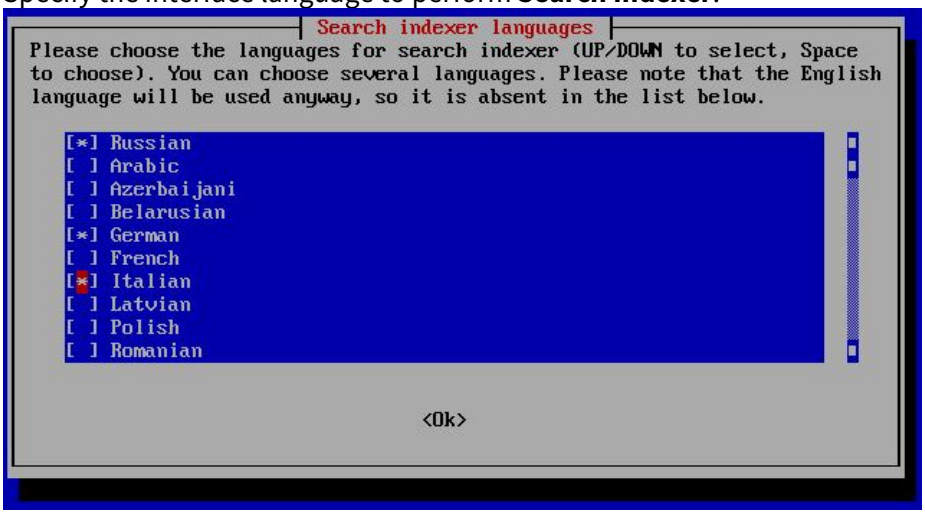


There are two languages available:

- *Russian* – to install interface in Russian;
- *English* – to install interface in English.

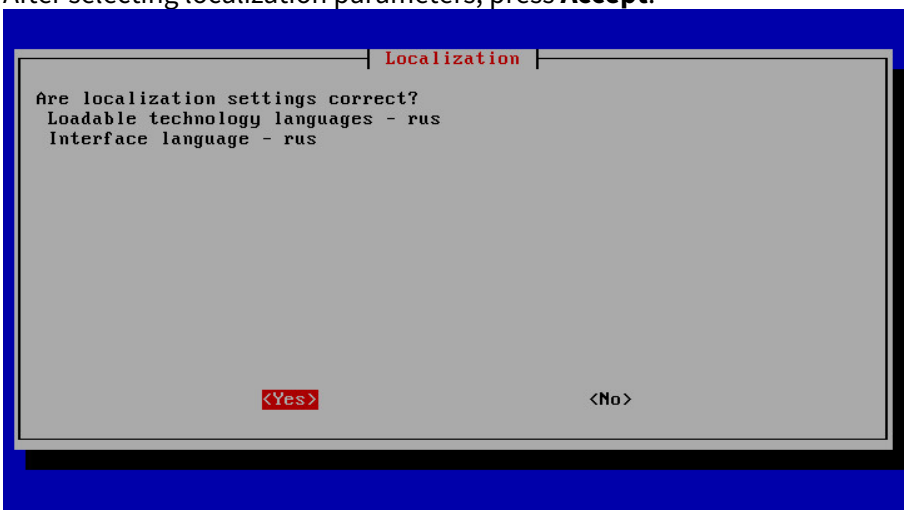
b. select required interface language and press **OK**.

3. Specify the interface language to perform **Search Indexer**.



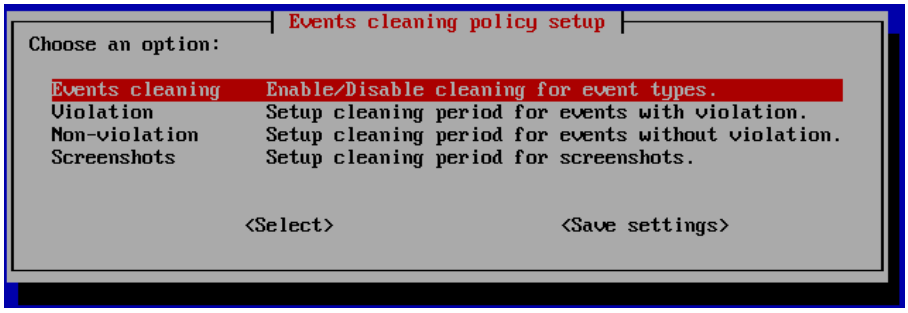
To select the language set the cursor on the needed field and click space keyboard key until an asterisk (*) appeared. You can select one or more languages.

4. After selecting localization parameters, press **Accept**.



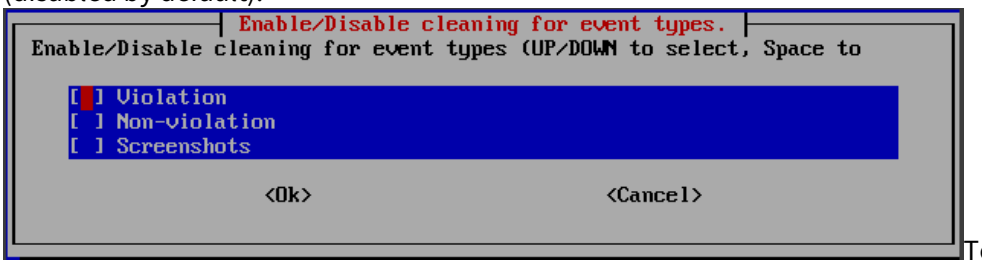
5. In the window that opens, make sure that selected languages for pre-installed entities, interface, and indexing are specified correctly, then press **Yes**.

Configuring the Automatic Event Deletion from the Database



Configure settings of automatic deletion of events from the DB. To do this select one of three options then click **Select**:

- **Events cleaning** – configures enabling and disabling of the automatic deletion of two event types (disabled by default).

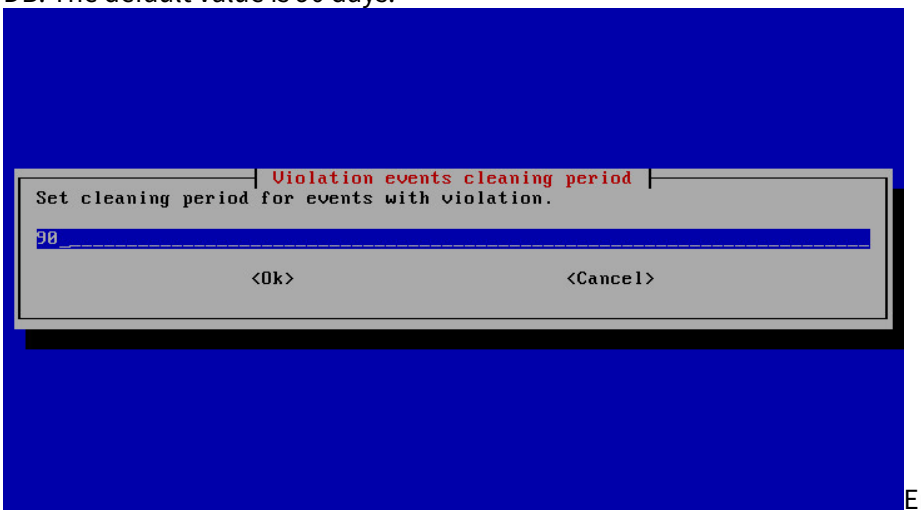


To select the option set the cursor on the needed field and click space keyboard key until an asterisk (*) appeared:
  - **Violation** – enables automatic deletion of events which violate the security policy (see details on policies in "*InfoWatch Traffic Monitor. User Guide*")
  - **Non-violation** – enables automatic deletion of events which do not violate the security policy of the company
  - **Screenshots** –enables automatic deletion of screenshots received from Device Monitor Agents.

    If necessary, you can select several items.

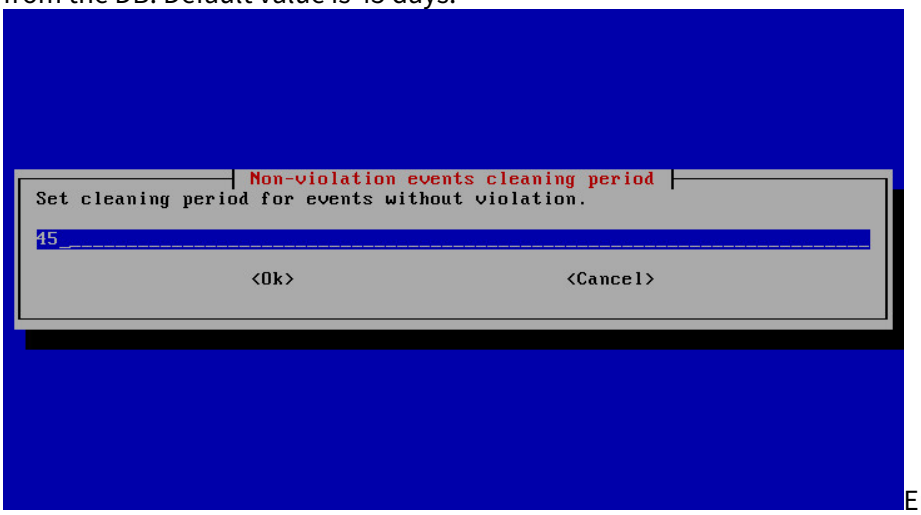
    Click **Ok**.

- **Violation** – sets a number of days after which the event with a violation will be deleted from the DB. The default value is 90 days.



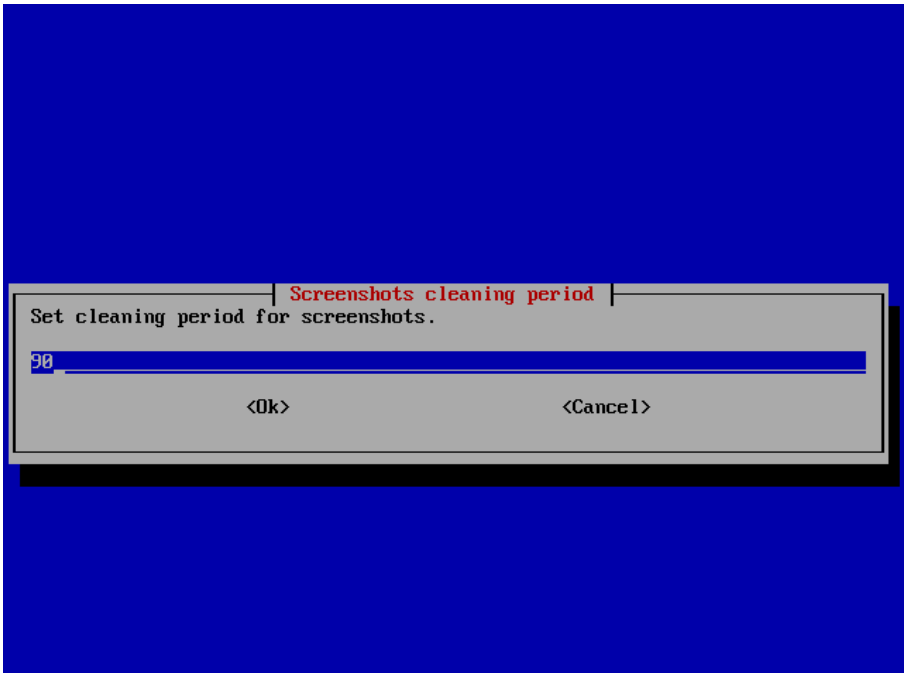
Enter the period of deletion, in days. Click **Ok**.

- **Non-violation** – sets a number of days after which the event without violations will be deleted from the DB. Default value is 45 days.



Enter the period of deletion, in days. Click **Ok**.

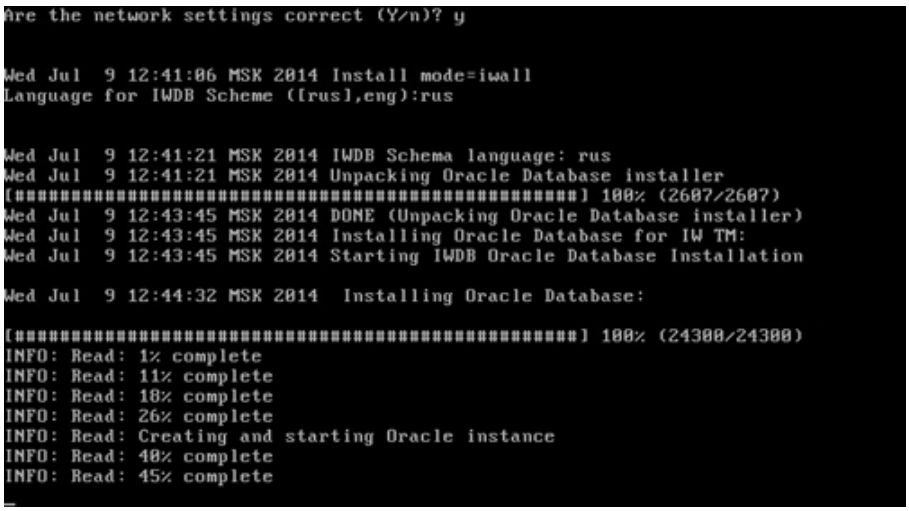
- **Screenshots** – sets a number of days after which screenshots, received from DM Agent will be deleted.



Enter the period of deletion, in days. Click **Ok**.
When all settings are finished, click **Save settings**.

Completing the Installation

Upon the settings are configured, the DBMS and DB schema begins. The progress will be displayed on the screen:



During the installation, the System creates accounts listed in "Pre-installed Server Settings".

The server hostname will have the following format:
`iwtm-xxxxxxxxxxxxxxx.local`
where xxxxxxxxxxxxxxx is the Serial Number of a server.

See details on further System configuration in «*InfoWatch Traffic Monitor. Administration Guide*».

3.1.2 All-in-one Installation Mode of TM Enterprise and TM Standard

All-in-one installation mode allows you to install all components of the System on the same computer.

> **Important!**
>
> This chapter contains instructions without detailed description of installation screens. For additional information, see «General Information on Installation Steps».

To install the Traffic Monitor Enterprise or Traffic Monitor Standard in All-in-one mode, take the following steps:

1. Connect the distribution disk: the installation program (kickstart) will run automatically.
2. In the Welcome window, select:
   - **TM Enterprise** – to install Enterprise edition
   - **TM Standard** – to install Standard edition.

   > **Important!**
   >
   > When you install **TM Standard** edition, you can select only PostgreSQL database.

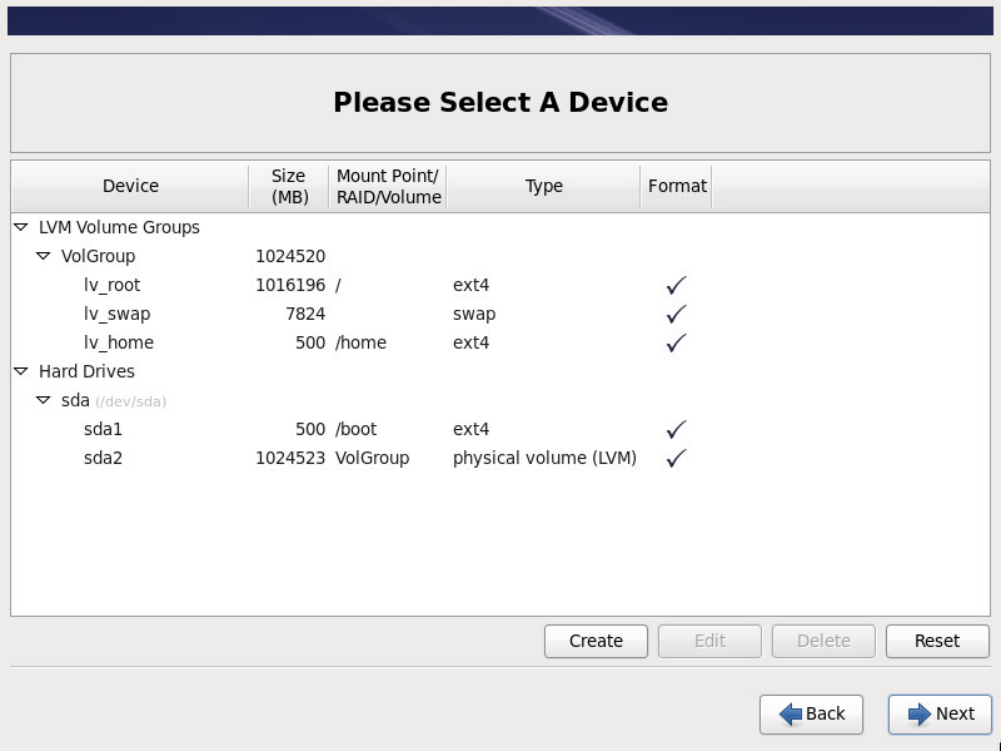
   Press **Enter**.
3. In the window of the Database selection, please select the required DBMS (the option is available for **TM Enterprise** only):
   - **Oracle Enterprise**
   - **PostgreSQL**

   Press **Enter**.
4. In the window of installation mode selection, choose **TME All-in-one** or **TMS All-in-one** and press **Enter**.

   > **Important!**
   >
   > When the installation mode is selected, the following warning message may appear: «*The storage device below may contain data*». To clean the disk and start the installation, click **Yes, discard any data** and leave the field **Apply my choice to all devices with undetected partitions of file systems** unchanged.

5. Specify time zone settings for the server (if the system time is set by Greenwich (UTC), select the field **System clock uses UTC**) and click **Next**.
6. Specify a password for *root* superuser and click **Next**. Recommendations on password creation are available in Appendix A.
7. Specify the mode of disk space partitioning (see detailed description in "Choosing a Disk Partitioning Method"):
   a. Select **Use All Space**.
   b. Select the checkbox **Review and modify partitioning layout**.
   c. Click **Next**.
   d. In **Please Select A Device** select **lv_home** partition and click **Edit**.
   e. In **Size (MB)** field specify **5000**. Click **OK**.
   f. In **Please Select A Device** window select **lv_root** partition and click **Edit**.

g. In **Size (MB)** field specify all remain free space (displayed under the field - **Max size is...**). Click **OK**.



h. Click **Next**.

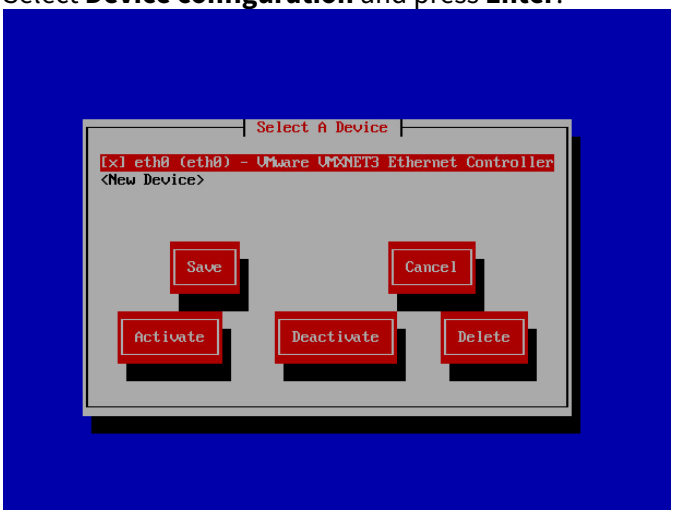
> **Note:**
>
> The **Format > Warnings** window can be displayed which informs you that hard disk partitions, which will be used for installation, need formatting. To continue the installation, click **Format**.

The disk partitioning and operating system installation will start. Progress will be displayed on the screen.
The process may take some time.

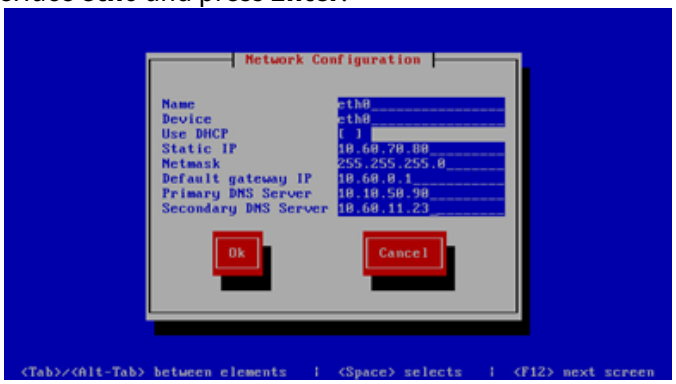
When installation of the operating system is completed, the system will be restarted and you will be prompted to configure network parameters:

8. To configure parameters of a network card:

a. Select **Device configuration** and press **Enter**.



b. Select network interface **eth0** and press **Enter**.

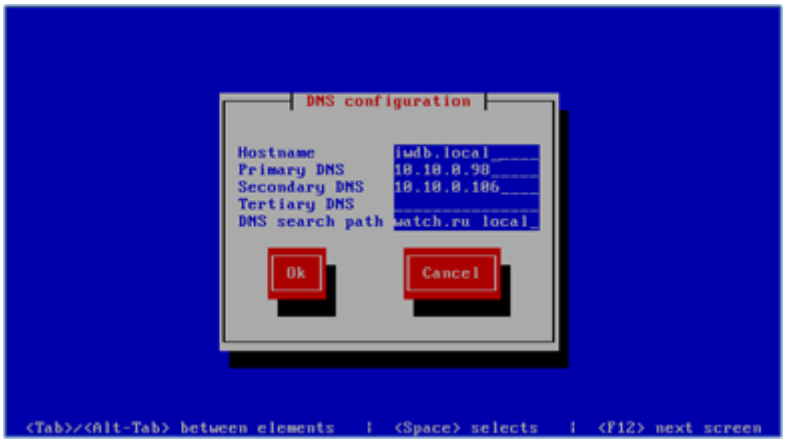


> **Important!**
>
> Do not enable the **Controlled by Network Manager** option.

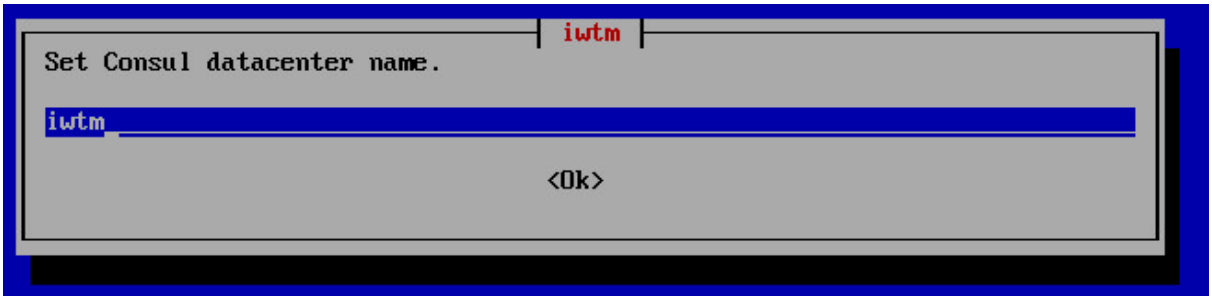
> **Important!**
>
> While configuring **eth0**, make sure that the **On boot** option is enabled.

c. If you want network settings of DHCP server to be used in the System, move the cursor to the **Use DHCP** field and press Space. Otherwise, specify network settings for the server manually (static IP-address of the computer, etc.). When all settings are specified, click **OK**.
d. Click **Save** to save the settings.

9. To configure DNS, select **DNS configuration** and specify required server network parameters. Then click **OK**.



10. Click **Save&Quit**.
11. Check specified network settings. If they are incorrect, type **N** and specify correct parameters (see previous steps). If the settings are correct, type **Y** to confirm and press **Enter**.
12. Enter the name of Consul datacenter and click **OK**.



13. Specify the server address for time synchronization (NTP-server). To do this, set asterisk (*) in the required field by pressing Space, then click **OK**.

> **Note:**
>
> If NTP server cannot be specified for some reasons, click **Cancel** and set this parameter later (details on configuring the NTP server see in "*InfoWatch Traffic Monitor. Administration Guide*»).

14. Set localization settings:
    a. Set the language of pre-installed settings:
        i. Select **CFDB** and press **Enter**.
        ii. Specify the desired language.
        If you select **Don't preinstall loadable technology settings** option, the standard System configuration is not installed.
        iii. Click **OK**.
        The selected language will be used when creating terms and categories, filters and default policies.

    b. Set interface language:
        i. Select **Interface**and press **Enter**.
        ii. Specify the desired language.
        The Management console will be installed in selected language.
        iii. Click **OK**.

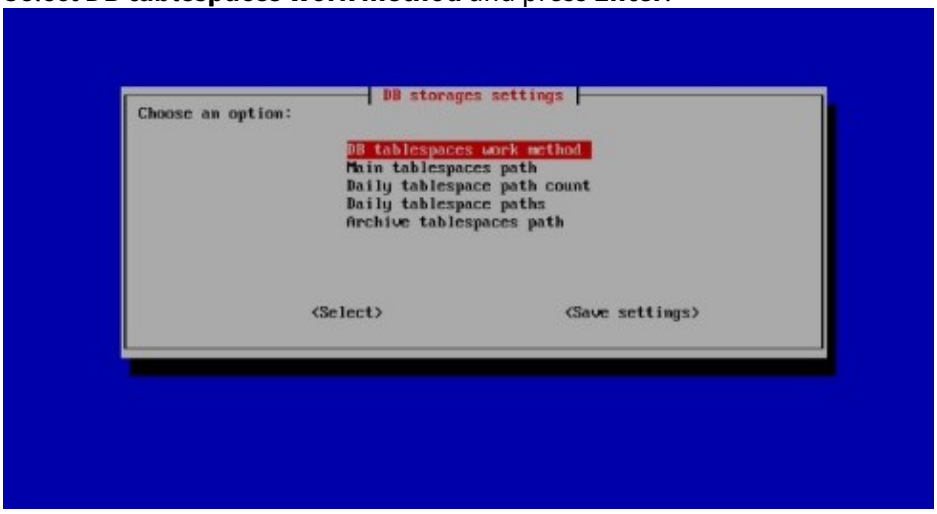
c. Set the language of the search indexer:
    i. Select **Search indexer** and press **Enter**.
    ii. Select one or more languages.
    iii. Click **OK**.

d. Click **Accept**.

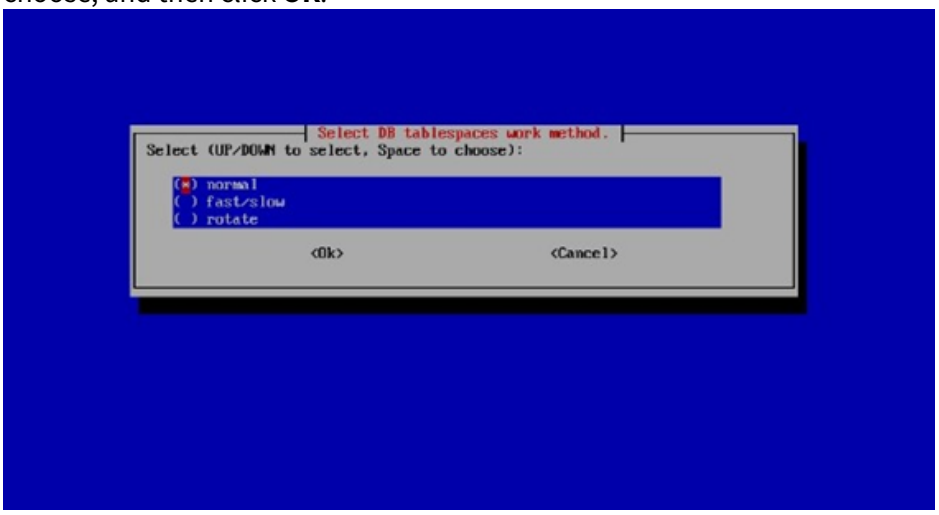
e. In the opened window, make sure the selected languages for pre-installed settings and interface are specified correctly, then click **Yes**.

15. Set parameters of DB data storage:

a. Select **DB tablespaces work method** and press **Enter**.



b. Specify tablespace storage method, setting the asterisk sign (*) opposite to mode you choose, and then click **OK**.



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

> **Note:**
>
> The peculiarities of data storage methods (**normal**, **fast/slow** and **rotate**) are described in knowledge base article "Tablespaces data storage settings. Data storage partition".

c. Select **Main tablespaces path** and specify the path to main tablespaces data storage disk (by default, the path specified for Oracle database is **/u02/oradata** and for PostgreSQL database it is **/u02/pgdata**).
d. Press **Enter**.
e. Select **Daily tablespace path count** and specify the number of daily tablespaces paths (number from 1 to 10, by default, it is number 1).
f. Press **Enter**.
g. Select **Daily tablespace paths** and specify the path to daily tablespace data storage disk (by default, the path specified for Oracle database is **/u02/oradata1** and for PostgreSQL database it is **/u02/pgdata1**).
h. Press **Enter**.
i. Select **Number of days to store in fast tablespaces for fast/slow method** and specify the period to store files in fast tablespaces in the **fast/slow** mode (number from 1 to 1000, by default, it is 7 days). Files kept for more than 10 days are to be automatically relocated on slow disks (for **fast/slow** method only).
j. Press **Enter**.
k. Select **Fast daily tablespaces path for fast/slow method** and specify the fast daily tablespaces path in the **fast/slow** mode (by default, the path specified is **/u03/pgdata** - for **fast/slow** method only**)**.
l. Press **Enter**.
m. Select **Archive tablespaces path** and specify the archive tablespaces path (by default, the path specified is **/u02/arch)**.
n. Press **Enter**.
o. Press **Save settings** to keep the settings chosen.
p. In the opened window make sure the selected settings are specified correctly, then click **Yes**.

16. Set parameters of events automatic deletion from the database (by default, the automatic event deletion is disabled).
    a. Choose **Events cleaning** and click **Select**:
        i. Place the cursor to the required field and press the space button until the field displays an asterisk (*):
            - **Violation** – enable automatic deletion of events that are considered violations (for more details on violations, see «*InfoWatch Traffic Monitor. User Guide*»);
            - **Non-violation** – enable automatic deletion of events that are not considered violations;
            - **Screenshots** – enable automatic deletion of screenshots received from Device Monitor Agents.

            You can select several options if needed.
        ii. Click **Ok**.

b. If automatic deletion of events with violations is enabled, specify the period after which the events are deleted:
   i. Choose **Violation** and click **Select**:
   ii. In the window that opens, specify the number of days after which the event will be automatically deleted (by default, 90 days).
   iii. Click **Ok**.

c. If automatic deletion of events without violations is enabled, specify the period after which the events are deleted:
   i. Choose **Non-violation** and click **Select**:
   ii. In the window that opens, specify the number of days after which the event will be automatically deleted (by default, 45 days).
   iii. Click **Ok**.

d. If automatic deletion of screenshots received from Device Monitor Agents is enabled, specify the period after which the screenshots are deleted:
   i. Choose **Screenshots** and click **Select**:
   ii. In the window that opens, specify the number of days after which the screenshot will be automatically deleted (by default, 90 days).
   iii. Click **Ok**.

e. When all settings are configured, click **Save settings**.
f. In the window that opens, make sure that all settings are specified correctly, then click **Yes**.

The installation of the DBMS and DB schema will start. The progress will be displayed on a screen.

The process may take some time.

During the installation, the System creates accounts listed in "Pre-installed Server Settings".

The server hostname will have the following format:
`iwtm-xxxxxxxxxxxxxxx.local`
where xxxxxxxxxxxxxxx is the Serial Number of a server.

Web Console is installed in an automatic mode using **kickstart** program. When the server components are installed, you can work in the Management console in a browser: for this, enter the URL of the Traffic Monitor Server.

The further System configuration is described in the document «*InfoWatch Traffic Monitor. Administration Guide*»

3.1.3 Distributed Installation of TM Enterprise

The Enterprise edition of the Traffic Monitor system allows you to deploy the System so that Traffic Monitor Server and DBMS (Oracle Enterprise or PostgreSQL) are installed on the different computers. Such installation is used if Traffic Monitor Server services and DBMS cannot efficiently operate on the same computer with respect to the supposed load.

Servers are installed in the following order:

1. Installing Database (TM DB Server)
2. Installing Traffic Monitor Server (TME Node Server).

> **Warning!**
>
> Installation in a different order (Traffic Monitor Server is installed before the Database) is not supported and results in errors during the installation.

You can install several Traffic Monitor Servers. In this case, you should logically divide them into a primary one and secondary one(s). All processes, which run in a single copy, run on the primary server.

Installing Database

> **Warning!**
>
> This chapter contains instructions without detailed description of installation screens. For additional information, see "General Information on Installation Steps".

> **Warning!**
>
> Each server should have unique and correct FQDN.

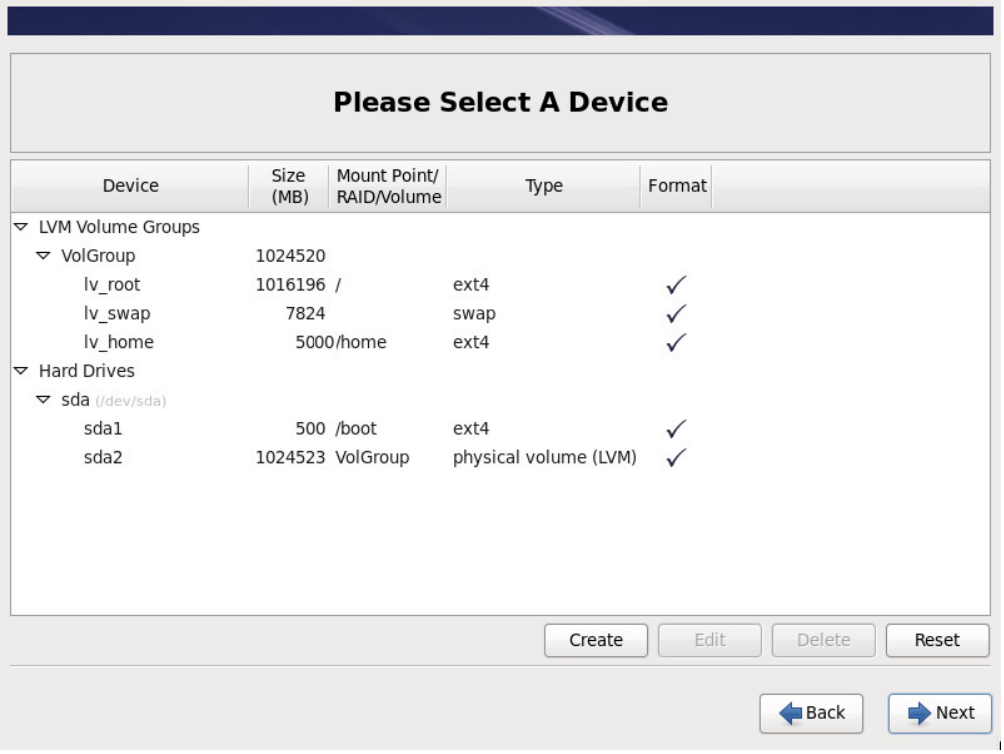
To install a database, perform the following steps:

1. In the Welcome window, select **TM Enterprise** and press **Enter**.
2. In the database selection window specify which DBMS should be installed:
   a. Oracle Standard;
   b. PostgreSQL.

   Click **Enter**.
3. In the window of selecting the installation mode, choose **TME DB server** and press **Enter**.

   > **Warning!**
   >
   > When the installation mode is selected, the following warning message may appear: "*The storage device below may contain any data*". To clean a disk and start the installation, click **Yes, discard any data** and left the **Apply my choice to all devices with undetected partitions of file systems** field unchanged.

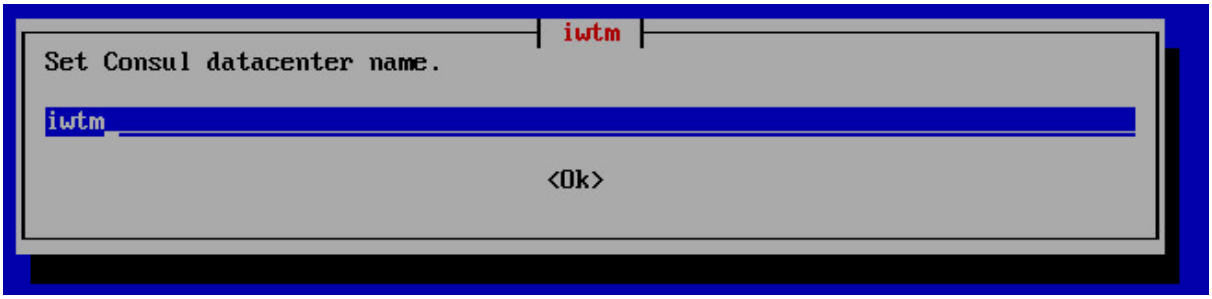
4. Specify time zone settings for a server (if the system time is set by Greenwich (UTC), place a check mark to a field **System clock uses UTC**) and click **Next**.
5. Specify a password for *root* superuser and click **Next**. Recommendations on password creation are available in Appendix A
6. Specify the mode of disk space partitioning (detailed description see in "Choosing disk partitioning method"):
   a. Select **Use All Space**
   b. Select the checkbox **Review and modify partitioning layout**
   c. Click **Next**
   d. In the **Please Select A Device** window, select **lv_home** partition and click **Edit**.
   e. In the **Size (MB)** field, specify **5000**. Click **OK**.
   f. In the **Please Select A Device** window, select **lv_root** partition and click **Edit**.
   g. In the **Size (MB)** field, specify **all remain free space** (displayed under the field - **Max size is...**). Click **OK**.



h. Click **Next**.

The disk partitioning and installation of the operating system will start. Progress will be displayed on a screen.
The process may take some time.
When installation of the operating system is completed, the system will be restarted and you will be prompted to configure network parameters.

7. Configure parameters of a network card and DNS as described in "Network Settings". Click **Save&Quit**.
8. Check specified network settings. If they are incorrect, type **N** and specify correct parameters (see previous steps). If the settings are correct, type **Y** to confirm and press **Enter**.
9. Enter the name of Consul datacenter and click **OK**.



10. Specify server address for time synchronization (NTP-server). To do this, set asterisk (*) in the required field by pressing **Space**, then click **OK**.
11. Set localization settings:
    a. Set the language of pre-installed settings:
        i. Select **CFDB** and press **Enter**.
        ii. Specify the desired language and click **OK**.

    The selected language will be used when creating terms and categories, filters and default policies.

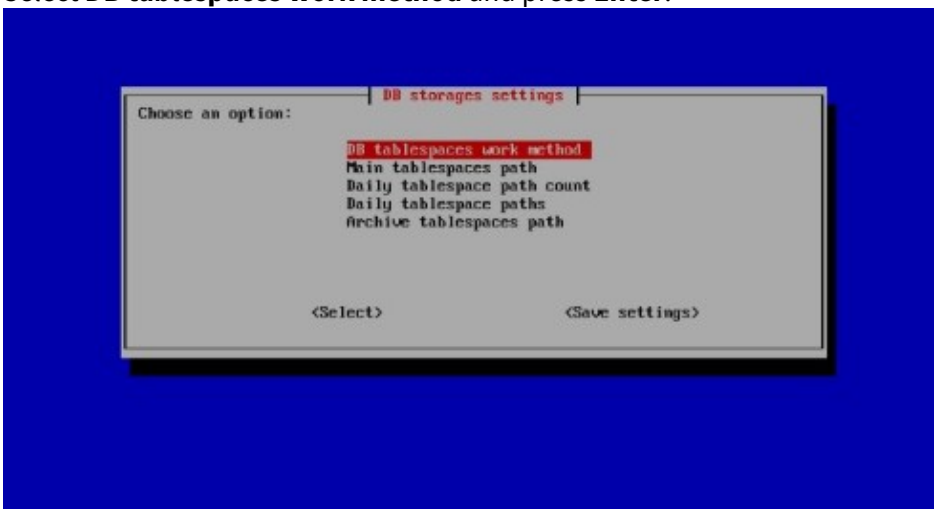
b. Set interface language:
    i. Select **Interface** and press **Enter**.
    ii. Specify the desired language and click **OK**.
    The Management console will be installed in selected language.

c. Set the language for Search indexer:
    i. Select **Search indexer** and press **Enter**.
    ii. Specify one or several languages.
    iii. Press **OK**.

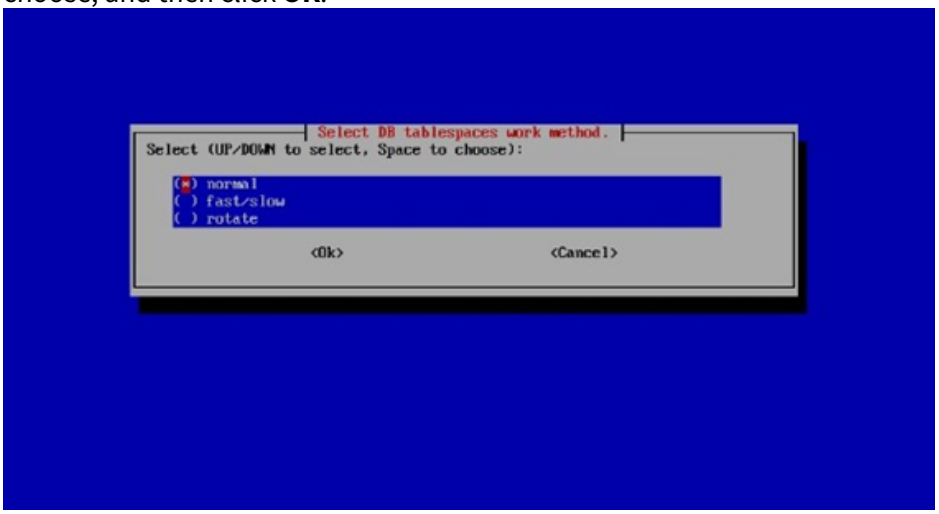
d. Click **Accept**.

e. In the opened window make sure the selected languages for pre-installed settings and interface are specified correctly, then click **Yes**.

12. Set parameters of DB data storage:
    a. Select **DB tablespaces work method** and press **Enter**.



    b. Specify tablespace storage method, setting the asterisk sign (*) opposite to mode you choose, and then click **OK**.



- **Normal** – data transfer method, when the switching to the following partition (when it is specified) happens after the previous one is overflow.
- **Fast/slow** – data transfer method, dividing pools into fast and slow one. Recent data are to be kept in fast pool and to be relocated to the slow ones in a number of days specified (slow pool operates in normal mode).

- **Rotate** – data transfer method, when the switching to the following partition happens every day once the previous one is overflow.

> **Note:**
>
> The peculiarities of data storage methods (**normal**, **fast/slow** and **rotate**) are described in knowledge base article "Tablespaces data storage settings. Data storage partition".

c. Select **Main tablespaces path** and specify the path to main tablespaces data storage disk (by default, the path specified for Oracle database is **/u02/oradata** and for PostgreSQL database it is **/u02/pgdata**).
d. Press **Enter**.
e. Select **Daily tablespace path count** and specify the number of daily tablespaces paths (number from 1 to 10, by default, it is number 1).
f. Press **Enter**.
g. Select **Daily tablespace paths** and specify the path to daily tablespace data storage disk (by default, the path specified for Oracle database is **/u02/oradata1** and for PostgreSQL database it is **/u02/pgdata1**).
h. Press **Enter**.
i. Select **Number of days to store in fast tablespaces for fast/slow method** and specify the period to store files in fast tablespaces in the **fast/slow** mode (number from 1 to 1000, by default, it is 7 days). Files kept for more than 10 days are to be automatically relocated on slow disks (for **fast/slow** method only).
j. Press **Enter**.
k. Select **Fast daily tablespaces path for fast/slow method** and specify the fast daily tablespaces path in the **fast/slow** mode (by default, the path specified is **/u03/pgdata** - for **fast/slow** method only**)**.
l. Press **Enter**.
m. Select **Archive tablespaces path** and specify the archive tablespaces path (by default, the path specified is **/u02/arch)**.
n. Press **Enter**.
o. Press **Save settings** to keep the settings chosen.
p. In the opened window make sure the selected settings are specified correctly, then click **Yes**.

13. Set parameters of automatic events deletion from DB.
Select one from three options, then click **Select**:
    - **Events cleaning** – sets enabling and disabling the automatic deletion of two event types (disabled by default).
      To select the option set the cursor on the needed field and click space keyboard key until an asterisk (*) appeared:
        - **Violation** – enables automatic deletion of events which violate the security policy (see details on policies in "InfoWatch Traffic Monitor. User Guide")
        - **Non-violation** – enables automatic deletion of events which do not violate the security policy of the company.
          You can select both items to delete both violating and not violating events.

      Click **Ok**.

- **Violation** – sets a number of days after which event with violations will be deleted from the DB (default: 90 days).
  Enter the period of deletion, in days. Click **Ok**.
- **Non-violation** – sets a number of days after which event without violations will be deleted from the DB (default: 45 days).
  Enter the period of deletion, in days. Click **Ok**.
- **Screenshots** – sets a number of days after which screenshots, recieved from DM Client will be deleted from the DB (default: 90 days).

14. When all settings are set, click **Save settings**.

The installation of the DBMS and a DB scheme will start. The progress of both processes will be displayed on a screen. The process may take some time.

During the installation, the System creates accounts listed in "Pre-installed Server Settings".

The server hostname will have the following format:
`iwtm-xxxxxxxxxxxxxxx.local`
where xxxxxxxxxxxxxxx is the Serial Number of a server.

Web-console installation is performed in an automatic mode. After the completion of the server-end installation the Management console is available through a browser: enter the URL of the Traffic Monitor Server.

The procedure of the further System configuration is described in the document "InfoWatch Traffic Monitor. Administration Guide".

Installing Traffic Monitor Server

Warning!

This chapter contains instructions without detailed description of installation screens. For additional information, see «General Information on Installation Steps».

Warning!

Each server should have unique and correct FQDN.

To install Traffic Monitor Server perform the following steps:

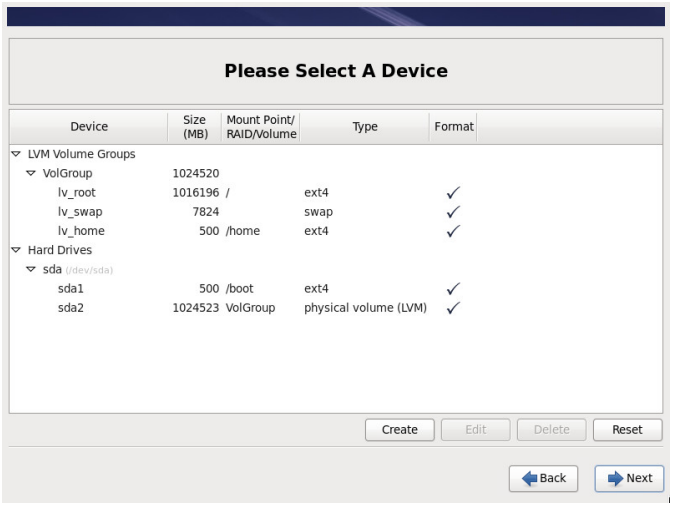
1. Connect the distribution disk: the installation program (kickstart) will run automatically.
2. In the Welcome window, select **TM Enterprise**. Then press **Enter**.
3. In the window of the Database selection, select the required DBMS:
   - **Oracle**
   - **PostgreSQL**

   Then press **Enter**.
4. In the window of installation mode selection, choose **TME Node server** and press **Enter**.

Warning!

When the installation mode is selected, the following warning message may appear: «*The storage device below may contain any data*». To clean the disk and start the installation, chick **Yes, discard any data** and leave the field **Apply my choice to all devices with undetected partitions of file systems** unchanged.

5. Specify time zone settings for a server (if the system time is set by Greenwich (UTC), select the option **System clock uses UTC**) and click **Next**.
6. Specify a password for *root* superuser and click **Next**. Recommendations on password creation are available in Appendix A.
7. Specify the mode of disk space partitioning (detailed description see in "Choosing disk partitioning method"):
   a. Select **Use All Space**.
   b. Select the **Review and modify partitioning layout** checkbox.
   c. Click **Next**.
   d. In **Please Select A Device** window select **lv_home** partition and click **Edit**.
   e. In **Size (MB)** field specify **5000**. Click **OK**.
   f. In **Please Select A Device** window select **lv_root** partition and click **Edit**.
   g. In **Size (MB)** field specify all remain free space (displayed under the field - **Max size is...**). Click **OK**.



   h. Click **Next**.

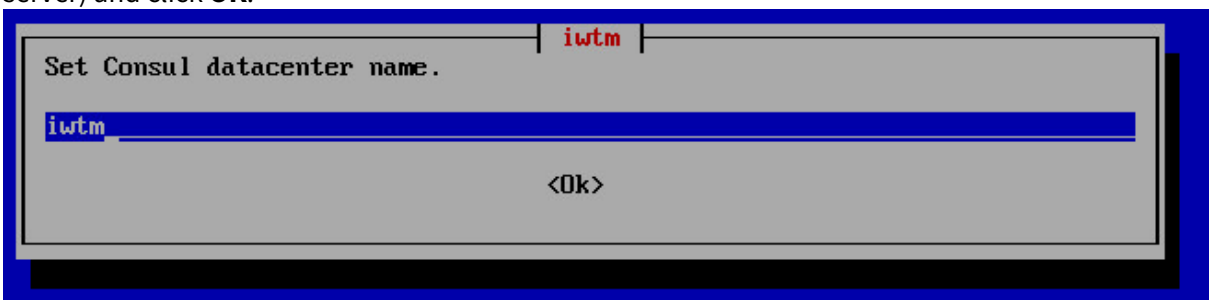
Note:

The **Format > Warnings** window can be displayed which informs you that hard disk partitions, which will be used for installation, need formatting. To continue the installation, click **Format** .

8. The disk partitioning and operating system installation will start. Progress will be displayed on a screen.
   The process may take some time.

When installation of the operating system is completed, the system will be restarted and you will be prompted to configure network parameters.

9. Configure parameters of a network card and DNS as described in "Network Settings". Click **Save&Quit**.
10. Check specified network settings. If they are incorrect, type **N** and specify correct parameters (see previous steps). If the settings are correct, type **Y** to confirm and press **Enter**.
11. Enter the name of Consul datacenter which was specified when installing DB server (TME DB server) and click **OK**.



12. Specify the server address for time synchronization (NTP-server). To do this, set asterisk (*) in the required field by pressing Space, then click **OK**.
13. Specify IP address of the database server and press **Enter**.

> **Note:**
>
> If you are using DHCP, it is necessary to tie issuing a certain IP-address to the MAC-address.

14. Check specified network settings. If they are incorrect, type **N** and specify correct parameters. If the settings are correct, type **Y** to confirm and press **Enter**.

During the installation, the System creates accounts listed in "Pre-installed Server Settings".

The server hostname will have the following format:
`iwtm-xxxxxxxxxxxxxxx.local`
where `xxxxxxxxxxxxxxx` is the Serial Number of the server.

Web console installation is performed in automatic mode. After the completion of the server-end installation the Management console is available through a browser: enter the URL of the Traffic Monitor Server.

The procedure of further System configuration is described in the document «*InfoWatch Traffic Monitor. Administration Guide*».

3.2 Installing Crawler Subsystem

Crawler interceptor is implemented via three services:

- `InfoWatch.Crawler.Scanner` – scans network folders and file storages according to settings configured by user;
- `InfoWatch.Crawler.Server` – manages scanning service and enables communication with Traffic Monitor Management Console.
- `Consul Agent` - registers services, detects and monitors Traffic Monitor components.

Warning!

For interaction with one database schema, **only one** instance of Crawler server can be used. One Crawler server can interact with **only one** instance of Crawler scanner.

Before installation, please read software and hardware requirements for computers where System components will be installed. Both components of Crawler subsystem (server and scanner) are installed from the same distribution.

Warning!

Both Crawler server and Crawler scanner must be installed on computers located in the same domain: the one which contains all the computers that will be scanned.

Warning!

Before the installation, make sure that the servers Traffic Monitor and Crawler are connected. For this, check Crawler server's availability by running the following command on Traffic Monitor server: ping <short name of Crawler server>. Otherwise, Crawler subsystem can be installed, but will not be displayed in Traffic Monitor management console.

To install Crawler:

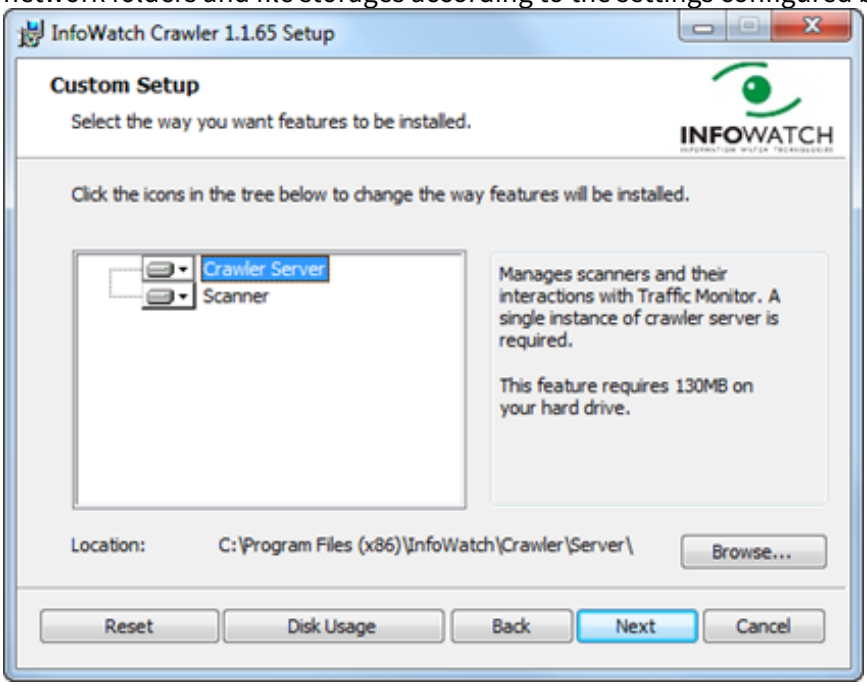
1. Run `Crawler_vx.x.x.xxx.msi` installation package, where x.x.x.xxx is a version number.

   Note:

   The language of the Installation Wizard is defined automatically and depends on the selected format (see**Start -> Control Panel -> Region and Language**, **Formats** tab).

2. In the Welcome screen of InfoWatch Crawler Installation Wizard, click **Next**.
3. In the Installation Scope screen, click **Next**.
4. At the **Custom Setup** step, specify which Crawler components should be installed and choose the installation directory:
   - **Server Crawler** – installing the `InfoWatch.Crawler.Server` service that manages scanning tasks and provides communication with the server, database and Traffic Monitor Management Console.

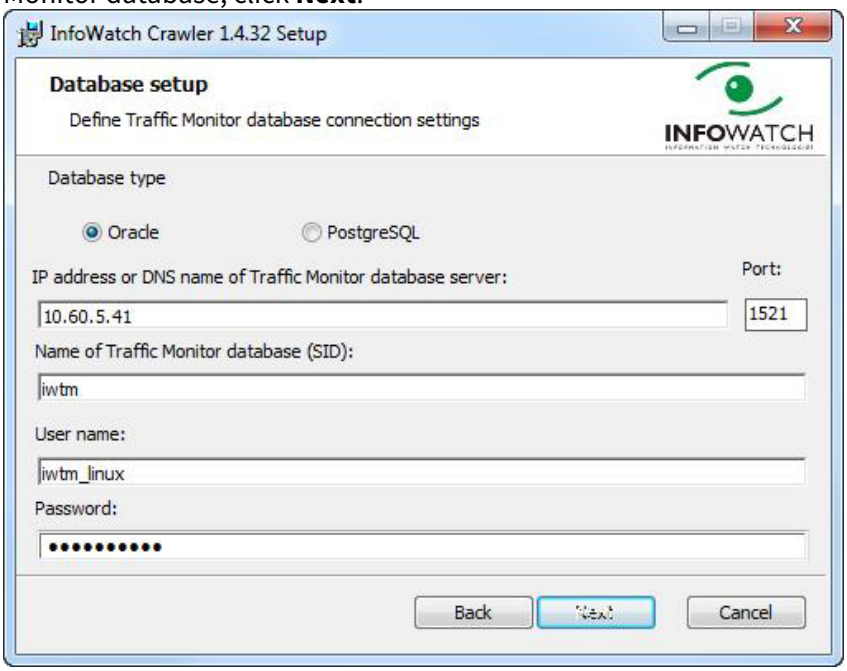
- **Scanner component** – installing the `InfoWatch.Crawler.Scaner` service that scans network folders and file storages according to the settings configured by a user.



If you do not want to install a particular component, click on this feature and select ✕**Entire feature will be unavailable**.

Specify paths to the directories where selected components will be installed and click **Next**.

5. If at the **Custom Setup** step, you have chosen the **Server Crawler**:
   a. Specify parameters for connection of the `InfoWatch.Crawler.Server` service with Traffic Monitor database, click **Next**.



Depending on used DBMS, connection settings may vary:

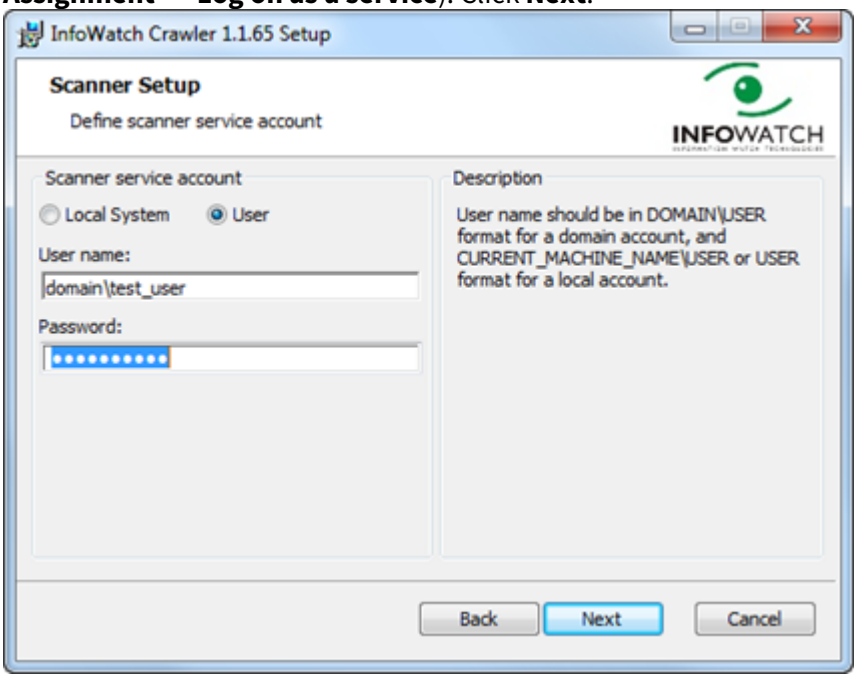
Setting	Oracle	PostgreSQL	Notes
IP address or DNS name	According to the TM DB server in use		
Port	1521	5433	
Database name	iwtm	postgres	The PostgreSQL needs SID or service name.
Username	iwtm_linux	iwtm_linux	User of the Linux part of DBMS on behalf of which the intercepted events will be downloaded to the database.
Password	xxXX1234	xxXX1234	If was not changed after Traffic Monitor server part installation.

b. Specify parameters to connect Consul agent to Traffic Monitor server, click **Next**.
To enter data in the fields **Consul datacenter name** and **Consul encryption key** the following actions are to be taken:
i. Connect to Traffic Monitor server where Consul is installed.
ii. Go to `/opt/iw/tm5/etc/consul` directory.
iii. Open the file `consul.json`.
iv. The data required for installation are located in the sections:
`datacenter` - **Consul datacenter name**
`encrypt` -**Consul encryption key**
v. Close the file with no changes of content.

c. Specify parameters of connection between `InfoWatch.Crawler.Server` and Traffic Monitor server, click **Next**.
In case of distributed installation, in **IP address or DNS name of Traffic Monitor Service Manager** field specify the IP address or DNS name of TM server (TME Node Server).

6. If on the **Custom Setup** step you have chosen the installation of **Scanner component**:
   a. specify an account that will be used to launch `InfoWatch.Crawler.Scaner` service. You can select a standard Local System account (recommended) or specify an account which has permissions for running services in the background mode (this option is configured in **Panel –> Administrative Tools –> Local Security Policy –> local policies –> User Rights**

Assignment –> Log on as a service). Click **Next**.



b. specify:
   - IP address or DNS name of the computer where the **Server** component is installed;
   - port number of the Crawler server;
   - path to the directory where the Scanner will temporary store files that are copied from checked resources.

> **Note:**
>
> If the **Temporary files directory** field is left blank then the installer will automatically select the last path value used in the operating system.

7. Click **Next**.
8. Click **Install** to start the installation. When the installation is complete, click **Finish**.
9. After installation of the Crawler server, start it with the following steps:
   a. go to the server where **iwtm-webgui** package is installed;
   b. go to the directory `/opt/iw/tm5/etc`, open the **web.conf** file and change the value of the `kickers.crawler` parameter from "0" to "1";
   c. execute the command: `service iwtm restart kicker`.

> **Important!**
>
> After completing the installation process it is required to make sure Traffic Monitor management console and Crawler server have been connected. For this, go to Traffic Monitor management console, open **Crawler** section and make sure Crawler settings are displayed there.

3.3 Installing InfoWatch Device Monitor

Installation is performed in the following order:

1. InfoWatch Device Monitor Server End Setup.
   Server end consists of the following elements:
   - Database
   - Device Monitor Server
   - Device Monitor Management Console.
2. InfoWatch Device Monitor Agent Installation.
   Agent is installed on each computer that should be controlled by InfoWatch Device Monitor.

Before installation, make sure that environment where the System will be deployed matches software and hardware requirements (see "Hardware and Software Requirements").

3.3.1 InfoWatch Device Monitor Server End Setup

InfoWatch Device Monitor server end is installed with universal Setup Wizard.
Universal Setup Wizard disk is available on your System installation CD (Setup.Unified directory). This program lets you install all System components except the Agent: database, Device Monitor Server, and Management Console.
The InfoWatch Device Monitor system can use Microsoft SQL Server or Oracle DBMS or PostgreSQL for managing the database.
Management Console connects to the primary server.
For more information on installation, see:

- Database deployment managed by Microsoft SQL Server DBMS
- Database deployment managed by Oracle DBMS
- InfoWatch Device Monitor Server Setup
- InfoWatch Device Monitor Server End Installation Procedure

Database deployment managed by Microsoft SQL Server DBMS

You must install Microsoft .NET Framework 2.0 Service Pack 1 and Microsoft .NET Framework 4.0 or higher before launching database scheme generation on your computer.

Database generation account must be configured in advance. Account type depends on database server authentication. Microsoft SQL Server DBMS supports two types of authentication:

- **Windows authentication**. Authentication uses accounts within Windows domain. Authentication data is processed by Microsoft Windows security.
- **SQL Server built-in authentication**. Uses Microsoft SQL Server accounts. Authentication is carried out via DBMS.

> **Important!**
>
> To ensure satisfactory safety level, we strongly recommend that you use **Windows authentication** method.

If you are going to use Windows authentication method:

1. Make sure Windows domain contains only one account that you will use for database generation. This account must have local administrator privileges on the computer used for database generation. If necessary, create a new account.
2. Add the account to Microsoft SQL Server DBMS and select **Windows authentication**.
3. Assign **dbcreator** role to the account.

If you plan to use SQL Server built-in authentication method:

1. Create a new Microsoft SQL Server account. When configuring an account: select **SQL Server built-in**, enter user name and password.
2. Assign **dbcreator** role to the account.

> **Note:**
>
> Integrated account name and password are specified when configuring the database (see "InfoWatch Device Monitor Server End Installation Procedure", step 6).

Database deployment managed by Oracle DBMS

жThe following components should be installed on the computer before launching the database schema generation:

- Microsoft .NET Framework 2.0 and Microsoft .NET Framework 4.5 packs
- Oracle DBMS client (only after Microsoft .NET Framework 2.0 and Microsoft .NET Framework 4.5 packs have been installed)
- Oracle Database Provider for .NET (ODP.NET)

> **Important!**
>
> Enable this feature by selecting the corresponding field in the Custom installation type. Installation must be run under the administrator account.

Before you start creating a database scheme, make sure that **tnsnames.ora** file contains database server connection parameters (see "Configuring ORACLE DBMS connection").

Configuring InfoWatch Device Monitor connection to Oracle DBMS server

To ensure proper connection to Oracle DBMS server for each computer with Oracle DBMS client, you must configure `tnsnames.ora` file located in `[ORACLE_HOME]\network\admin` directory.

Configuring tnsnames.ora

Specify Oracle DBMS server connection settings. To do this, add the following entry to `tnsnames.ora` file:

```
tns_name =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = host_name)(PORT = port_number))
(CONNECT_DATA =
```

```
(SERVER = DEDICATED)
(SERVICE_NAME = service_name)
)
)
```

Specify true values for the following parameters:

- `tns_name` – Oracle DBMS server alias;
- `host_name` – Oracle DBMS domain name or IP address;
- `port_number` – server port for listening to client connections;
- `service_name` – database service name.

Example of `tnsnames.ora` file:

```
IWDM =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = iwdm.example.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = orcl)
)
)
```

Important!

The `tnsnames.ora` file is format sensitive. If you copy an example to edit a file, make sure that the copied selection does not contain any blank strings.

Database deployment managed by PostgreSQL DBMS

There are the following preliminary requirements for the computer, where the database creation is to be started from:

- OS Microsoft Windows Server 2008 R2/2012/2012 R2;
- Microsoft .NET Framework 4.5.2 pack.

Download PostgreSQL 9.6 from the official site and install it with default parameters.

When installing the application, postgres superuser is to be created, to which the password should be granted. The related information is to be available in the utility pgAdmin III in "Entrance roles" section, a part installation pack.

Note:

To increase the System's response speed it is recommended installing OS, InfoWatch Device Monitor server end and PostgreSQL SMDB on different hard drives.

Server Setup Recommendations

To enhance the performance of Device Monitor, we recommend that you should deploy the server and database on separate computers.

Important!

When deploying a multiple-server pool, each server must have the same InfoWatch Device Monitor server application version installed that is compatible with the appropriate up-to-date database.

To make the InfoWatch Device Monitor Server able to install the Clients onto mobile devices, the server should have a long name. If the used server is not in the Windows domain then you need to configure FQDN. To do this:

1. In the **System Properties**, on the **Computer Name** tab click **Change**.
2. In the **Computer Name**/**Domain Changes** dialog window, click **More**.
3. In the **Change primary DNS suffix when domain membership changes** field, enter the domain name.
4. Click **OK**.
5. Make sure that the **Full computer name** field displays the long name.

While configuring the Server (see "InfoWatch Device Monitor Server End Installation Procedure"), you must specify the account that will be launching InfoWatch Device Monitor Server. Available options:

- **Local System**. Launch service from system account.
- **User**. Launch service from Windows domain account.

For Microsoft SQL Server DBMS database. If you select **Windows authentification** for database owner (see "Database deployment under Microsoft SQL Server DBMS"), while database and Server are on separate computers, select **User** variant.

Important!

It is not recommended to select Local System option. In this case, the user can obtain unlimited rights, which contradicts the security policy.

Create service account and grant write access to installation catalogue: `\Program Files\InfoWatch\Device Monitor\Server`

Windows domain account (**User**) must be configured in advance. To do this:

1. Allow the account to run process as a service:

- In the **Control Panel** open **Administration** > **Local security policy**.
- In the following dialog select **Local policies** > **Assign User Rights**.
- Double-click **Log on as service** in the right **Details** pane.
- On **Local security parameter** tab add the account.

- Add a new account to Microsoft SQL Server DBMS account list.
When setup finishes, allow the account to create new databases. When specifying database access permission, select **db_owner** role.

InfoWatch Device Monitor Server End Installation Procedure

Important!

Before starting the installation, see "Installing InfoWatch Device Monitor ".

Important!

When deploying a multiple-server pool, each of them must have the same InfoWatch Device Monitor server application version installed compliant with the appropriate up-to-date database.

1. **Running the Installation Wizard**
   Insert the installation CD into your CD-ROM drive. Then open `Server` directory. Run platform-specific setup file from this directory.
   You will be redirected to InfoWatch Device Monitor Setup Wizard welcome screen. Click **Next**.
2. **Accepting the License Agreement**
   Read the End User License Agreement. If you accept the licensing terms, select **I accept the terms in the License Agreement** and click **Next.**
3. **Selecting components to install**
   Custom Setup page has all components selected by default:
   - Server
   - Management Console
   - MSM module (Taiga) - component enabling Device Monitor Client installation to mobile devices (see details in "*InfoWatch Traffic Monitor. User Guide*", "Mobile Devices" section). Can be installed and used only together with the Management Console.

   You can change the list of components you want to install. For example, if you want to use an existing Management Console with a new Server, you do not need to install this feature: click **Management Console** and select **Entire feature will be unavailable**.
   You can also change the folder to install the component: select this component in the list, click **Browse** and specify the needed location.
   Click **Next**.
4. **Configuring server settings**
   On **Type of installed server** page select:
   - **Primary Server** - should be installed first. Clients and Management Console will connect to it.
   - **Secondary Server** - an additional server that balances Clients workload.

     Важно!

     Changing name of the Device Monitor server after installation could cause System malfunction.

     Note:

     To install secondary server it is required first to install the primary one to a separate workstation. Secondary server installation is described in point 14.

   To ensure rapid server status updates it is recommended that you select **Publish Server in Active Directory** option.

Important!

Workstations occasionally interact with Device Monitor server to update security policies. To let the newly added server handle workstations and notify the Clients about any possible server port changes it is recommended that you publish its details in domain during the installation.
To publish Device Monitordataindomain, the account that installs the server needs privileges to create and delete connection points.

If you have the Device Monitor database of the appropriate version, deselect **Install new Database** option.
Click **Next**.

5. **Choosing configuration file**
If the new database installation is not performed, this step is skipped.
To use the server configuration file exported before (see "*InfoWatch Traffic Monitor. User Guide*", "Import/Export Configuration" article), click **Open** and specify configuration file location.

Important!

The configuration file should be placed on the local hard or external device. The Setup Wizard does not support network locations.

Click **Next**.

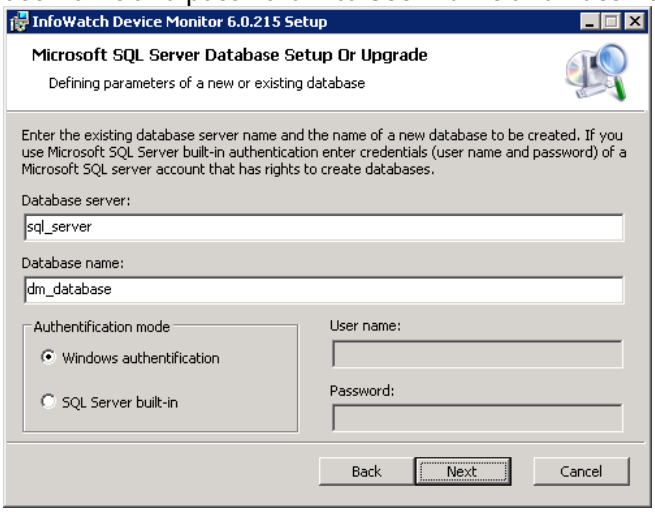
6. **Selecting database server**

Specify DBMS that will control Device Monitor database by choosing one of the following options:
- Microsoft SQL Server
- Oracle
- PostgreSQL

If you don't want to install a new database (**Install new Database** option has not been selected in Step 4), you need to specify connectivity settings for existing Device Monitor database.
Click **Next**.

7. **Database configuration**
You skip this step if you chose to use an existing database in Step 4.
Database configuration depends on DBMS type.
If you are using Microsoft SQL Server DBMS, specify the following parameters:
- **Database server**. NetBIOS Microsoft SQL Server name where the database will be created. Do not enter IP address in **DB server** box, since this will prevent you from connecting to the database server.
If there are any named instances on the database server, specify server name as follows: <server_name>\<instance_name>.
- **Database name**. New database name.
It may contain Latin letters, numbers, and other characters except spaces and special characters: «*», «?», «/», «\», «|», «^», «:», «"". Name must start with a Latin letter.
Name may be 1 to 123 characters long.

- **Authentication mode**. Database owner authentication method. For this option, specify the authentication method selected during account preparation (see "Database deployment managed by Microsoft SQL Server DBMS").
  If the account uses Windows authentication, select **Windows authentification**. In this case, the database will be created by the domain user, who runs the installation.
  If the account uses SQL Server authentication, select **SQL Server built-in**. Then enter username and password into **User name** and **Password** fields respectively.



When using Oracle DBMS configure the following settings:

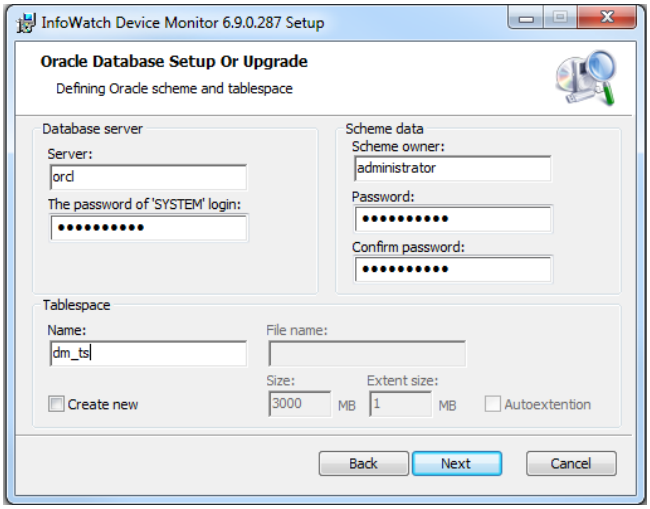
a. Set database server connection options:
   - **Database server**. Database server name. Use server alias from `tnsnames.ora` file for this parameter.
   - **The password of 'SYSTEM' login**. SYSTEM account password.

b. Specify the parameters of database schema owner account:

> **Important!**
>
> It is not recommended to use existing database scheme settings.

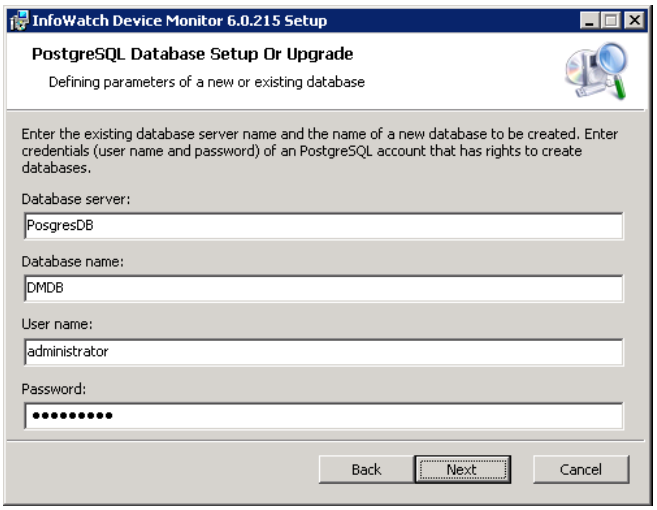
   - **Scheme owner**. Database schema owner account name.
   - **Password, Confirm password**. Database schema owner account password.
   Password is assigned basing on requirements specified in Oracle DBMS documentation.

c. Configure tablespace settings in **Tablespace** box.
   You can use existing tablespace or create a new one. If you are using existing tablespace, enter the tablespace name in **Name** field.
   To create a new tablespace, check the **Create new** box. Then specify tablespace options:
   - **Name**. Tablespace name.
   - **File name**. Name of the file where the new tablespace will be stored.
   - **Size**. Maximum size (in MB) of the data file (default size is 3000 MB).
   - **Extent size**. Maximum size (in MB) of continuous segment in data file (the default size is 1 MB).
   - **Autoextension**. Automatic file extension via Oracle DBMS. If Autoextension box is selected, automatic extension is enabled (this feature is disabled by default).



When using PostgreSQL configure the following settings:

- **Database server**. The name of the PostgreSQL DBMS where the database will be created. Default port -5432. If another port is to be used, it should be specified in the format `host:port`.
- **Database name**. The name of the newly creating database.
  It may contain Latin letters, numbers and other symbols excluding spaces and special symbols: «*», «?», «/», «\», «|», «^», «:», «"». Name must start with a Latin letter.
  Name may be 1 to 123 characters long.
- **User name** - the name of the account having rights for creating the DB on the PostgreSQL server.
- **Password** - the password of the account having rights for creating the DB on the PostgreSQL server.



After all necessary parameters have been configured, click **Next**.

8. **Configuring the server**

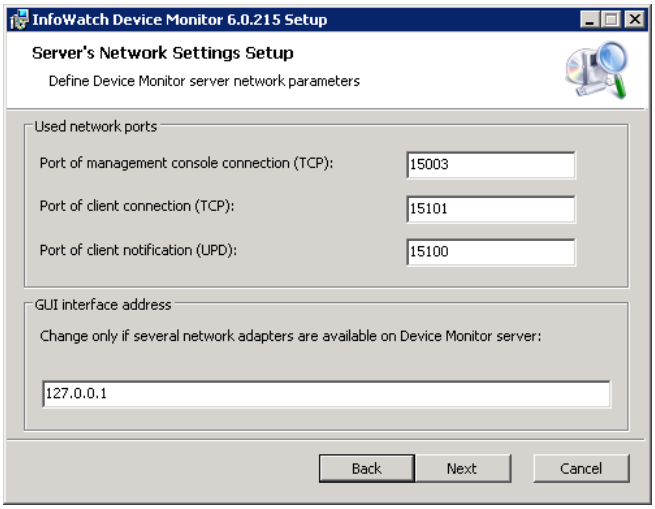
Configure Server parameters:

a. In **Used network ports** box set TCP and UDP ports used for:
   - **Management Console connection**;
   - **Clients connection** to transfer security schemes to managed workstations, send

information about events and shadow copies to server;
- **Clients notification** about security scheme changes.

b. In **GUI interface address**, enter the IP address that will be used for interaction between Server and Management Console.

> **Important!**
>
> This value should only be changed if the Server is installed on a computer with multiple network adapters connected to different networks. If there is one network adapter, this value must remain unchanged, otherwise Management Console won't be able to connect to Server.
> If you add more network adapters while working with Server, you can change this setting in Server configuration file.



After all necessary parameters have been configured, click **Next**.

9. **Configuring secure channel**

   Specify the port used for traffic transfer between the InfoWatch Device Monitor Client and Server.
   If you install a new database (Install new Database option was selected in Step 4), then in Secure channel key area select:
   - if you perform the first installation then leave the **Create new key** setting;
   - if you used the server of version 6.0 or higher and deleted it and then you install it again, then to make Device Monitor Clients could connect and bind to the new server, you should specify the encryption key used on the old server. The recommendations on saving the encryption key are listed in "Uninstalling Device Monitor". Select **Use existing key** and specify the path to the file of the encryption key.

   Click **Next**.
   If you selected **Create new key** setting, specify the path where Device Monitor will save file with a generated key.
10. **Configuring server account**
    Select an account that will launch InfoWatch Device Monitor according to "InfoWatch Device Monitor Server Setup Recommendations". If you select **User**, specify Windows domain account

name and password. Name is entered in DOMAIN\USERNAME format.
Click **Next**.

11. **Configuring server administrator account**
Provide credentials (username and password) for server administrator account. This will be a **Super user** account (for further details, see "*InfoWatch Traffic Monitor. User Guide*", "Managing Console Accounts" section): it is used when you first connect to the server from Management Console.
Click **Next**.
12. **Configuring InfoWatch Traffic Monitor connection parameters**

If at step 4 you decided to use an existing database (**Install New Database** option was not selected), then this step will be skipped.
Specify InfoWatch Traffic Monitor interaction options:

- **TM server address**. InfoWatch Traffic Monitor server address. Address must be entered in the following format:
`host:port`
Host parameter should contain domain name or IP address of InfoWatch Traffic Monitor server. The server address is the standard URI address (Uniform Resource Identifier) with its formal syntax described in RFC 3986 http://tools.ietf.org/html/rfc3986.
Port parameter contains InfoWatch Traffic Monitor server port that delivers events. InfoWatch Traffic Monitor default server port is 9100.

> **Important!**
>
> If you are going to integrate Device Monitor with Traffic Monitor 5.5 or earlier use format: `host:port, where port - 4101.`

- **Number of connections**. Number of InfoWatch Traffic Monitor server connections. You can specify from 1 to 32 connections.
- **Authorization token**. The token used for API connection. Required for Traffic Monitor v. 6.0 or higher. Please get this token from Traffic Monitor administrator.
- If Device Monitor deployment scheme is not integrated with InfoWatch Traffic Monitor, select **Work in standalone mode** box. In this case, you can save captured shadow copies in server installation directory by selecting **Save shadow copies** box.

Click **Next**.
13. **Completing the installation**
Click **Install** to start Server installation.
During installation, the permission to install Taiga system software will be requested. The permission is required to install drivers providing the support of mobile devices control. Click **Install**: otherwise the Wizard will finish its work prematurely and rollback the installation.

> **Important!**
>
> This message will appear if at Step 3 "Selecting Components to Install" you have selected the **MSM module (Taiga)** component.

Follow the instructions to complete installation.

> **Important!**
>
> Installing server end on Microsoft Windows Server 2012 or Microsoft Windows Server 2012 R2, you will see **Windows Security** dialog window, which installs InfoWatch virtual printer, required for processing printer jobs from metro-applications. To install virtual printer press **Install**.

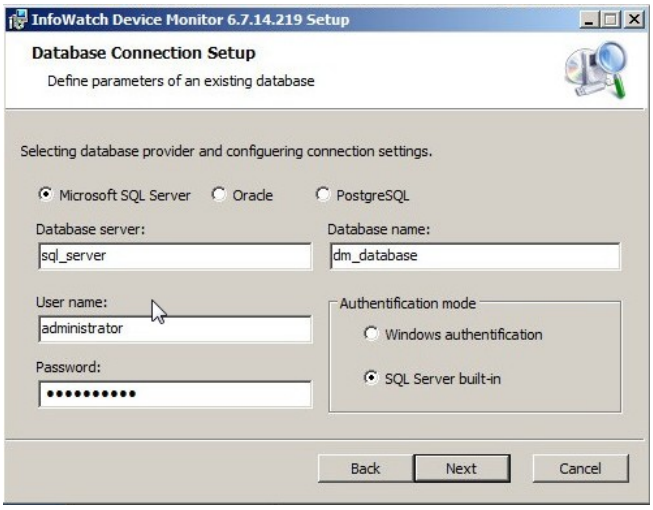
> **Note:**
>
> Signature installation may take a while (up to 30 minutes).

14. **Secondary server installation**
Secondary server activity is based on primary one, primary server settings deploy in secondary server thus guarantying Device Monitor servers connection.
    a. Running the installation Wizard
    Insert the installation CD into CD-ROM drive. Then open `Server` directory. Run platform-specific setup file from this directory. You will be redirected to InfoWatch Device Monitor Setup Wizard welcome screen. Click **Next**.
    b. Accepting the License Agreement
    Read the End User License Agreement. If you accept the license terms, select **I accept the terms in the |License Agreement** and click **Next**.
    c. Selecting components to install
    Custom Setup page has all components selected by default:
        - Server
        - Management Console
        - MSM module (Taiga) - component enabling Device Monitor Agent installation to mobile devices (see details in "*InfoWatchTraffic Monitor. User Guide*", "Mobile devices" section).

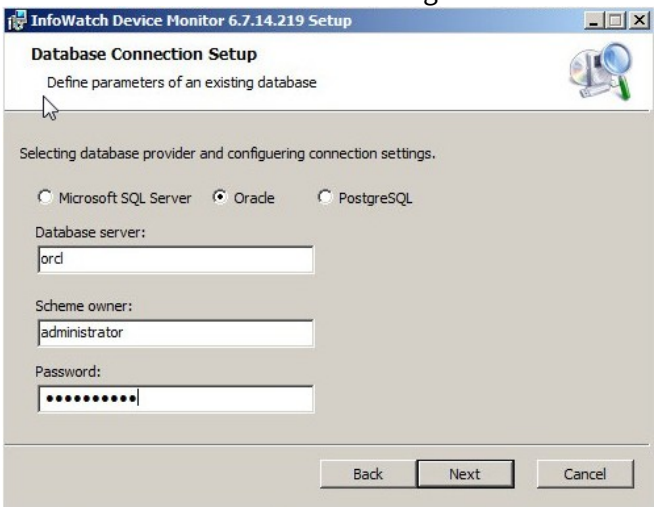
    You can change the list of components you want to install. For example, if you want to use an existing Management Console with a new Server, you do not need to install this feature: click **Management Console** and select ✕**Entire feature will be unavailable**. You can also change the folder to install the component: select this component in the list, click **Browse** and specify the needed location.
    Click **Next**.
    d. Configuring server settings
    Select **Secondary server** as a **Type of installed server**.

    > **Important!**
    >
    > Secondary server installation resists new database installation, that's why it is required to specify the parameters of existing database.

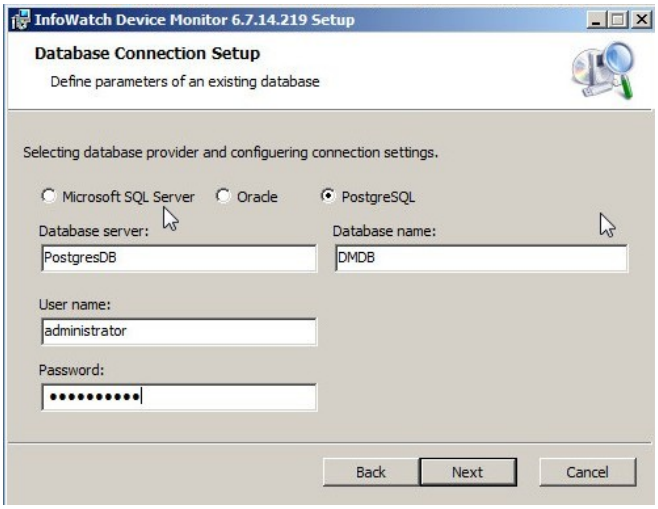
e. Database connection setup
Specify DBMS managing Device Monitor database and put in the rest connection parameters that were used while installing the primary server.
Microsoft SQL Server connection settings
If the account uses Windows authentication, and the database was created by domain user, **Windows authentication** should be selected. If the account uses SQL server build-in authentication, select **SQL server build-in**:



Oracle database connection settings:

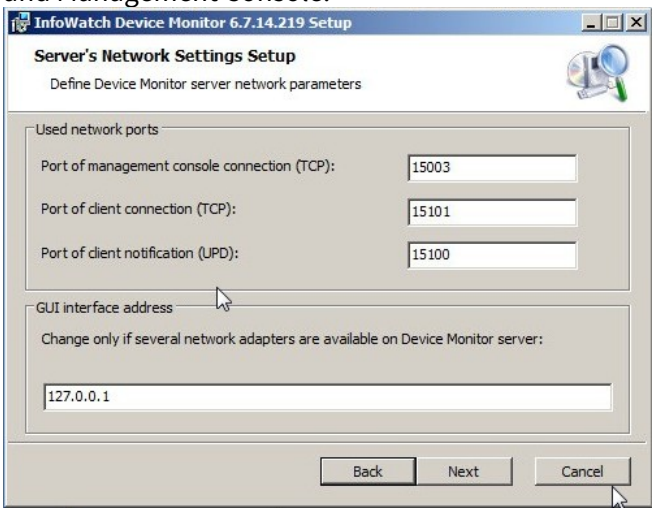


PostgreSQL database connection settings:



After all necessary parameters have been configured, click **Next**.

f. Server network parameters setup
Configure server parameters:
In **Used network ports** box set TCP and UDP ports used for:
- **Management Console connection**;
- **Agents connection** to transfer security schemes to managed workstations, send information about events and shadow copies to server;
- **Agents notification** about security scheme changes.
In **GUI interface address**, enter IP address that will be used for interaction between Server and Management Console.



After all necessary parameters have been configured, click **Next**.

g. Configuring server account
Select an account that will launch InfoWatch Device Monitor according to "InfoWatch Device Monitor Server Setup Recommendations". If you select **User**, specify Windows domain account name and password. Name is entered in DOMAIN\USERNAME format.
Click **Next**.

h. Completing the installation
Click Install to start server installation.
During the installation, permission to install Taiga system software will be requested. The permission is required to install drivers to support mobile devices control. Click Install: otherwise, the wizard will finish its work prematurely and rollback the installation.

> **Note:**
>
> This message will appear if at Step 3 "Selecting Components to install" you have selected **MSM Module (Taiga)** component.

Follow the instructions to complete the installation. Signature installation may take some time.

3.3.2 InfoWatch Device Monitor Agent Installation

InfoWatch Device Monitor Agent and Device Monitor server should be installed in the same time zone. This will ensure the event interception time is correct.

> **Warning!**
>
> InfoWatch Device Monitor Agent and InfoWatch Device Monitor server should not be installed on the same computer, otherwise this may cause the lack of server functionality.

InfoWatch Device Monitor Agent can be installed on workstations in the following ways:

- Local Installation. It uses the Setup Wizard on each computer.
- Remote installation using third-party software. It uses software distribution tools: for example, Microsoft Active Directory group policy.
- Remote installation through InfoWatch Device Monitor Management Console expansion tasks (for details, see "*Infowatch Traffic Monitor. User Guide",* "Agents Remote Installation, Updating and Uninstallation" section).

InfoWatch Device Monitor Agent is installed on mobile devices when adding this device to the security scheme (for details, see "*Infowatch Traffic Monitor. User Guide",* "Adding a Mobile Device through Appointment to Employee" and "Adding a Mobile Device to Computer Group" articles).

Follow the directions below to successfully install or update InfoWatch Device Monitor Agent:

1. Ensure the third-party DLP systems not to be run in parallel;
2. Include to the list of security exceptions InfoWatch Device Monitor Agent processes (the list of files you may find in "List of InfoWatch Agent's files to be added to antivirus exclusions group");
3. Disable antivirus self-protect function;
4. If possible, disable or remove the antivirus software installed when installing, updating and deleting InfoWatch Device Monitor Agent;
5. Ensure the ports required for InfoWatch Device Monitor Agent proper operation are available (list of ports you may find in "*Infowatch Traffic Monitor. Administration guide*", "Configuring InfoWatch Device Monitor Server*" section*);
6. To connect make sure the domain names of InfoWatch Device Monitor server and the computer, where InfoWatch Device Monitor Agent is to be installed are correctly resolved by DNS server into IP addresses;

Note:

To perform the check, run the following command within the console:
`nslookup <hostname>`
Example:
`nslookup dmserv`
If you have network problems, please contact your System Administrator.

7. If network connections settings (control panel) are not required to be used, disable it when creating InfoWatch Device Monitor Agent's distribution kit.
8. Install InfoWatch Device Monitor Agents on test workstations or on a small group of computers first;
   If there are no errors, reduced productivity, applications pending identified on test workstations during 2 or 3 days, you are advised to continue the installation on workstations.

Warning!

Turning off the computer during the installation/uninstallation process may lead to unstable operation of OS.

Warning!

During the agent installation, the Mozilla Firefox, and Mozilla Thunderbird applications (if they were running) will be closed.

Note:

Before installing the agent, it is required to run specific Windows updates for workstations on Windows 7 Service Pack 1 or Windows Server 2008 R2 OS (for details, see Hardware and Software Requirements).

Note:

When installing the agent on Windows 7 OS or Windows 2008 R2 Server it is recommended to consider the following point:

Corporate network control component will not be installed during the first installation of the agent. If needed, the component can be installed manually using the command line.

Note:

Start of InfoWatch Device Monitor Agent is performed automatically after the installation. Before restarting a computer the Agent's functionality is limited only by the following issues:

- traffic interception, sent via proxy server;
- network interception (when Agent is installed on OS Windows 8 and later);
- interception of copying to external devices.

Standard Agent Installation

> **Important!**
>
> It is not recommended to install InfoWatch Device Monitor Agents on computers that have the same name. These computers will be registered as a single computer, affected by the same policies, and register the same events, etc.

Client can be installed by computer's local administrator.

1. **Running the Installation Wizard**
   Insert the installation CD into your CD-ROM drive. Then open `Client` directory. Run platform-specific setup file from this directory.
   You will be redirected to InfoWatch Device Monitor Agent Installation Wizard welcome screen.
   Click **Next** to go to the next installation screen.

2. **Choose installation directory**
   Specify the path to Agent installation directory.

   > **Important!**
   >
   > Path to the catalogue may contain the following characters: 0-9, a-z, A-Z, ":", ".", "_", "-", "\", " ". If the path includes other characters, the agent installation will be incorrect.

   Click **Next**.

3. **Configuring settings**

   Specify InfoWatch Device Monitor server connection settings:
   - **Server**. InfoWatch Device Monitor server name.
   - **Port**. Port number used for communication between InfoWatch Device Monitor Agent and Server (port 15101 by default).

   Click **Next**.

4. **Completing the installation**

   Proceed to **Confirm installation** screen and click **Next** to start Agent installation. Follow the instructions to complete the installation. Restart your computer to finish the installation.

Agent Installation via Software Distribution Tools

> **Note:**

The corporate network administrator can perform Client centralized setup via software distribution tools. This section describes installation from Microsoft Active Directory.
Agent installation from Microsoft Active Directory is carried out via group policy. To do so, you have to select a group policy that covers all target workstations. This policy may be assigned to:

- Active Directory container that holds all target workstations
- the whole Active Directory domain, but not default domain policy. This policy should only cover the group that includes all controlled workstations.

1. **Creating Installation Package**

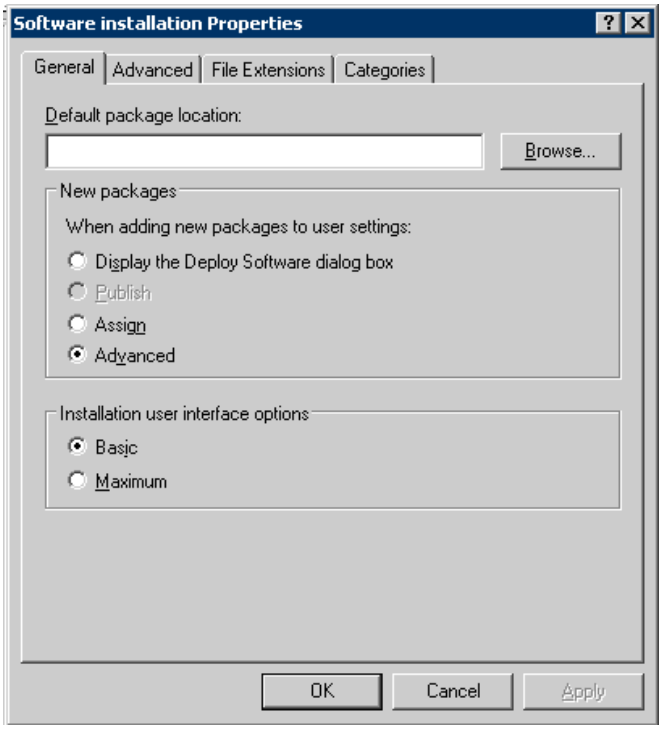
   Create `Client.en.msi` installation package as described in "*Infowatch Traffic Monitor. User Guide*", "Creating Installation Package" article). Put the installation package to the network directory that can be ready by all target computers within the domain.

2. **Disable Microsoft Windows XP Professional fast logon option**
   Before you start agent setup via group policies, disable fast logon optimization for computers with Microsoft Windows XP Professional OS (so-called asynchronous logon mode). For more details on this functionality see Microsoft Knowledge Base (see KB305293).
   To disable the fast logon optimization feature:
   a. Open the group policy editor.
   b. In console tree, select **Computer Configuration** > **Administrative templates** > **System** > **Logon**. In details section, select **Always wait for the network at computer startup and logon**. Then set the value of this parameter to **Enabled** in properties screen.

   > **Note:**
   >
   > If this option has been turned off, you will need to reboot your computer again to let Windows group policy distribution mechanism finishes the installation.

3. **Editing Group Policy**

   Edit group policy before installing Agent from Active Directory.
   To edit group policy:
   a. Open **Active directory users and computers** (**Start** > **Settings** > **Control Panel** > **Administrative tools** > **Active directory users and computers**).
   b. In the console tree, select Active Directory container with all target workstations.
   c. Open **Group Policy**. To do this, click **Properties** in Active Directory container context menu. In the following dialog box, navigate to **Group policy** tab. On this tab, select group policy and click **Edit**.
   d. In the console tree, select **Software Installation** (**Computer Configuration** > **Software Settings**).
   e. In **Software Installation** context menu, select **Properties**. On General tab configure the following settings (see the picture below):
   - set **New packages** value to **Advanced**;
   - set **Installation user interface options** value to **Basic**.

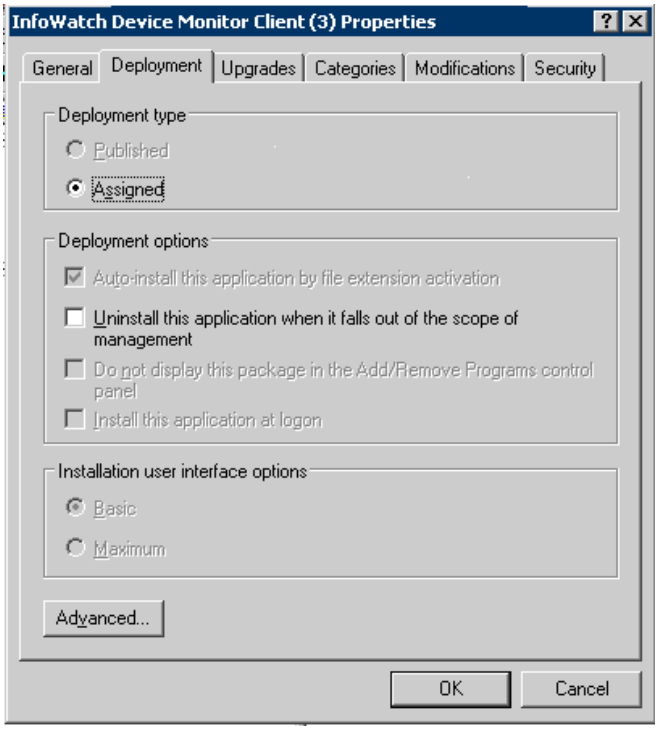


f. When the configuration is complete, click **OK**.

4. **Preparing Agent installation task**

Agent installation task is created and configured on **Group Policy Object Editor** screen:

a. After opening **Group Policy Object Editor** box select **Software Settings** (**Computer Configuration** > **Software Settings**) in the console tree. Right-click the selected item and then select **New** > **Package**.
b. In the following **Open** dialog specify agent module installation package `Setup.Client.msi` (first move the installation package to a network directory that is rreadable for all installation-target computers within the domain).
c. Configure new package properties:
- Make sure all settings in **Deployment** tab comply with the following figure.



- After all necessary settings have been configured, click **OK**.

d. In the console tree, select **Computer Configuration** > **Administrative templates** > **System** > **Scripts**. In details section, select **Run logon scripts synchronously**. Then set the value to **Enabled** in properties screen.

5. **Setup**

New task appears in **Software Installation** task list. The task is carried out as soon as the target computer is restarted. InfoWatch Device Monitor Agent starts automatically after its installation. Installation method is displayed in **Deployment state** column. **Assigned** status means that installation is forced, i.e. doesn't need an approval of target computer user. **Published** state means installation upon user's approval.

> **Important!**
>
> You can check if the Agent has been installed successfully in InfoWatch Device Monitor Management Console. All workstations the Agent has been successfully installed to must appear in the list in **Workstations** area. To view all managed workstations, click **Show all workstations** at the top of Navigation Pane. To obtain up-to-date Agent information, click **Update** in Toolbar.

Note:

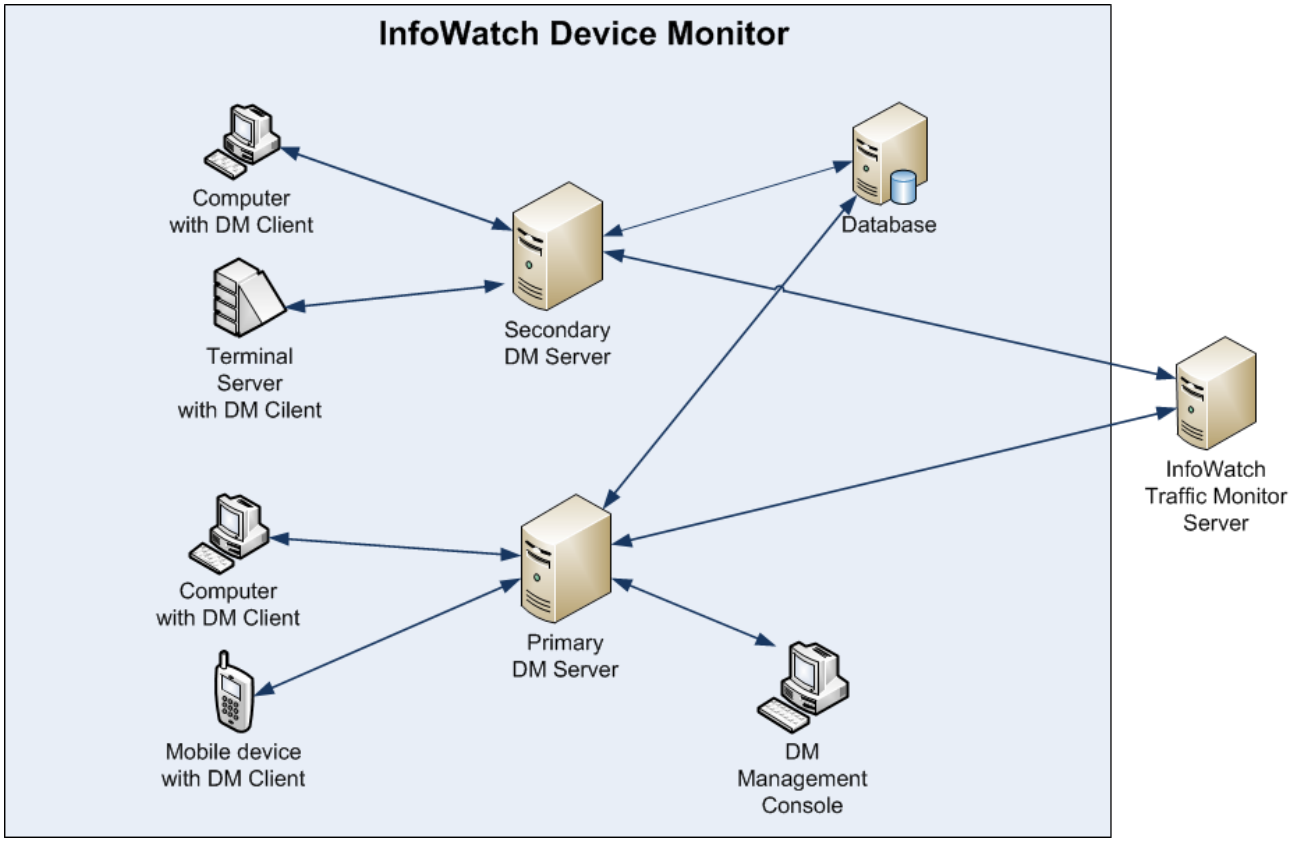
Disabling SMB1 protocol on Windows XP computers to perform Agent centralized update it is required to develop an installation pack and to install it by group policies means or using the distribution agent.

3.3.3 Deployment Scheme for InfoWatch Device Monitor

InfoWatch Device Monitor components are listed in the following table:

Component	Purpose
InfoWatch Device Monitor Client (InfoWatch device monitor client application, Agent)	Intercepting employees' actions on controlled computers and mobile devices
InfoWatch Device Monitor Server (InfoWatch device monitor server, Server)	Configuring agents, retrieving data from agents and sending it to InfoWatch Traffic Monitor
InfoWatch Device Monitor Database (database)	Storing data which is required for the operation of Device Monitor
InfoWatch Device Monitor Management Console (Management Console)	Managing Device Monitor
Servers Manager	Configuring roles and other attributes of Device Monitor servers

The following image illustrates interaction of Device Monitor components:



You can use clustering to enhance the performance. The same database schema will be used by multiple servers to store and distribute shared security schema.

Server and database can be hosted on a single computer. To increase the performance, it is recommended that you should host the database and server on separate computers.

The Management Console can only connect to the main server. From the Management Console, you can manage all servers in the cluster.

InfoWatch DeviceMonitor is deployed and works as follows:

1. The **primary server** is installed first (see the document "*Infowatch Traffic Monitor. User Guide*", "InfoWatch Device Monitor Server Manager" article).
2. When you install the primary server, you should specify the server that will be used by the **database**: DBMS can be stored separately or together with the primary server.
3. During installation of the primary server, a **database schema** is created, where the **security schema** and other Device Monitor parameters are stored.
4. You can install **secondary servers**, if needed, to balance the workload.
5. The **Management Console** can be installed on any computer. It connects to the primary server. The Management Console is used for configuring the security scheme according to the corporate security policy.
6. **Device Monitor Agents** are installed on **workstations** and **mobile devices**. Agents connect to any available Device Monitor Server via an encrypted channel with binding to the Server by the key, which is used for traffic encryption. Device Monitor agents ensure implementation of security schemes; they also retrieve shadow copies and send them to Device Monitor Server.
7. Device Monitor Server retrieves updated versions of the security scheme from the database and distributes them to controlled workstations and mobile devices. Information about events that subject to a security scheme rule and files shadow copies are sent from tThe controlled

workstations and mobile devices to the Server. Information about the events is sent to the database. Shadow copies are sent to InfoWatch Traffic Monitor.

Example 1

1. An employee who works at a controlled workstation tries to get access to a controlled peripheral (for example, attempts to print a document on a USB printer).
2. The Agent checks if the employee has permissions to access the peripheral. If not, access is denied (in this case, the document will not be printed).

Printing operations on local and network printers are monitored by Print Monitor interceptor. Print task copies are sent to InfoWatch Monitor Traffic for analysis. Employees can print documents, only if they are allowed to access the printer (this is checked by Device Monitor interceptor).

Example 2

There is a rule in Device Monitor that monitors writing to PDF files on a removable device. According to the rule, during this operation, a shadow copy of the document is created.

1. An employee who works at a controlled workstation writes data to a file on a removable device (for example, copies a file to USB flash drive).
2. If writing to a removable device is successful, InfoWatch Device Monitor Agent generates an event and creates a shadow copy of the file.
3. If the creation of a shadow copy fails (for example, there is no free space on the hard drive), writing to file will be performed without creating a shadow copy (this will be specified in the event data).
4. The Agent transmits data (the event and the file shadow copy) to InfoWatch Device Monitor Server. If there is not connection to the Server, the data is stored on the computer. Once the connection is restored, the data will be sent to Server.
5. The Server sends data to InfoWatch Traffic Monitor for analysis. If no there is no connection to InfoWatch Traffic Monitor server, the data is stored on the computer. Once the connection is restored, the data will be sent to InfoWatch Traffic Monitor.

Any attempts to write to files on removable devices are monitored by File Monitor interceptor. Obtained data is then passed to InfoWatch Traffic Monitor for analysis. At the same time, access to removable devices is controlled by Device Monitor interceptor. Therefore, employees can write data to file on a removable device only if they have access to the device.

Example 3

There is a rule in Device Monitor that monitors DOC files. According to the rule, during this operation, a shadow copy of the document is created.

1. An employee who works at a controlled workstation sends a document to print.
2. If the print job is created successfully, InfoWatch Device Monitor Agent generates an event and creates a shadow copy of the printed document.
3. If the creation of a shadow copy fails (for example, there is no free space on hard drive), print operation will be performed without creating a shadow copy (this will be specified in the event data).
4. The Agent transmits data (the event and the file shadow copy) to InfoWatch Device Monitor Server. If there is not connection to the Server, the data is stored on the computer. Once the connection is restored, the data will be sent to Server.
5. The Server sends data to InfoWatch Traffic Monitor for analysis. If no there is no connection to InfoWatch Traffic Monitor server, the data is stored on the computer. Once the connection is restored, the data will be sent to InfoWatch Traffic Monitor.

3.4 Pre-installed Server Parameters

During installation of the System, the installer creates a set of parameters. You may need to address these parameters when configuring or using the System.

The server hostname is **iwtm-xxxxxxxxxxxxxxxx.local** where xxxxxxxxxxxxxxxx is a Serial Number of the server.

System installation directories (can be placed on different servers):

- Traffic Monitor server – **/opt/iw**
- DB – **/u01** and **/u02**

> **Important!**
>
> You should change password for **oracle** and **postgres** users right after the System installation.

Parameters of Traffic Monitor database:

Settinng	Oracle	PostgreSQL
DB connection port	**1521**	**5433**
DB name / SID or service name	**iwtm**	**postgres**

oinstall - a group of the Oracle DBMS Client installation, which includes **iwtm**, **oracle** users for Oracle database and **iwtm**, **root** for PostgreSQL database.

Linux accounts:

Account	Name	Password
Superuser of Linux OS (root)	**root**	Specified during installation
Linux user on whose behalf the Traffic Monitor server processes will be executed	**iwtm**	No password
Database schema owner	**iwtm**	xxXX1234
Linux user on whose behalf Oracle database server processes will be executed **Note:** During installation of PostgreSQL database, this account is not created	**oracle**	xxXX1234
Linux user on whose behalf PostgreSQL server processes will be executed **Note:** During installation of Oracle database, this account is not created	**postgres**	xxXX1234

Database accounts:

Note:

Accounts are available after starting **sqlplus** for Oracle and **psql** for PostgreSQL.

Purpose	Oracle account name	PostgreSQL account name	Password
Accounts for database administration	**sys**	**postgres**	xxXX1234
	system		
Account for Linux processes to access the database	**iwtm_linux**		xxXX1234
Account for Management Web Console to access the database	**iwtm_web**		xxXX1234
Account for the monitoring subsystem (Nagios) to access the database	**iwtm_nagios**		xxXX1234

Web console accounts:

Purpose	Name	Password
User administrator	**administrator**	xxXX1234
Security officer	**officer**	xxXX1234

Sphinx index directory **/var/lib/sphinx**

Purpose	Name	Password
Linux user, which is used to run binary files and Sphinx indexes	**iwtm**	No password

4 Updating the System

Important!

Update to the required Traffic Monitor version is available from two previous releases. The update to 6.10 version can be installed from 6.9 and/or 6.7 versions. Releases history can be found in the article "Traffic Monitor: Main".

Note:

The System is installed from a connected repository.

A repository is a folder that contains files and other folders and provides them on demand to the operating system. In other words, a repository is a storage from which programs can be installed or updated. Before using the repository, you need to connect the repository so that the operating system could access it (the connection procedure is described below).

Important!

Before updating the System it is required to apply configuration. If configuration is not to be applied before the update, it is to be forced.

Important!

During the update, events are neiter intercepted, nor analyzed.

Before the update, make sure that you have:

- InfoWatch Traffic Monitor distribution disk of the current version;
- InfoWatch Traffic Monitor distribution disk of the version to which you want to update the System;
- access to a physical or a virtual server (or servers) which you want to update;
- password for the *root* user.

Also, before the update, you need to find out:

- the System installation type (it can be *All-in-one* or *Distributed installation (Node Server + Database Server)*) - this information is required to choose the right instruction for the update;
- which DBMS is used (Oracle or PostgreSQL) - this information is required for updating the database schema and server components;
- whether you are going to install a new classification base - this information is required when installing the repository. During the installation of a new classification base, the previous classification base (both standard and not standard) with all its modifications will be deleted;
- the server where `web-gui` is installed - this information is required to clear the server cache after updating the database schema.
  Tip: the package is installed on the server to which Traffic Monitor Management Console is connected.

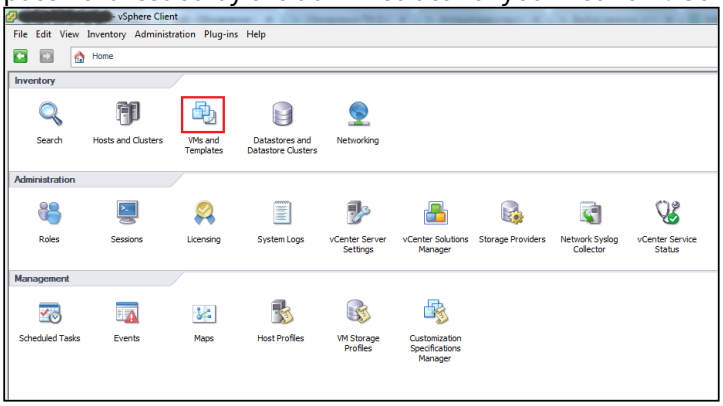
Before the update, take the following steps:

1. Turn on each server you want to update (in case it is off):

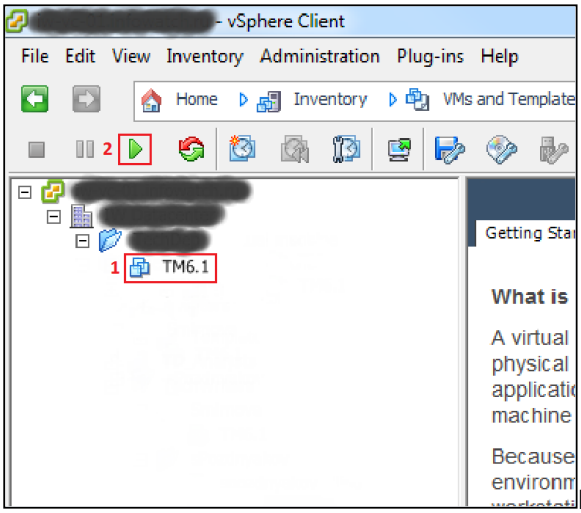
- for a physical server - press the power button on the server (for details, see instructions for the server);
- for the virtual server - run **Power On** command (see the example below).

> **Note:**
>
> This instruction contains examples of working with a virtual server in the client application of one of the most common virtualization environments - VMware vSphere (VMware vSphere Client).
> In frameworks, you can see interface areas that you need to click in the specified order to achieve the desired results.

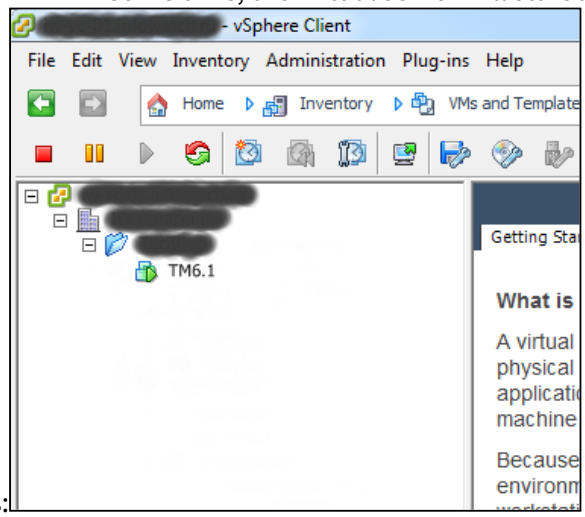
Run VMware vSphere Client application as administrator (right-click the application icon and select **Run as administrator**). Get authorized in the application using the login and password issued by the administrator of your network. Go to virtual machines:



Consistently expand all the nodes in the left side of the workspace until you see the required virtual server.
Turn on the virtual server:



In some time, the virtual server will start and the client application will look as follows:

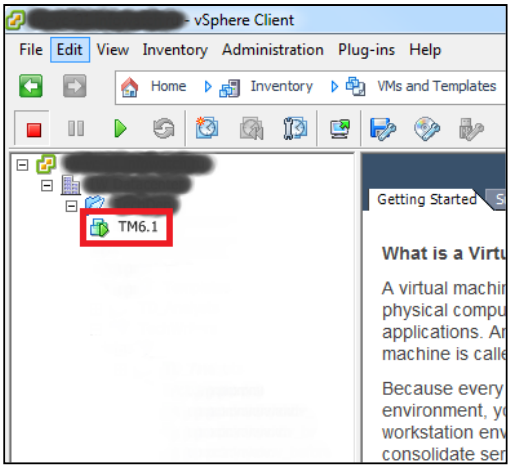


2. Connect InfoWatch Traffic Monitor distribution disk to the servers you want to update:
   - for a physical server:
     - if the distribution kit is on the optical disc - insert the disk into CD or DVD drive of the server and wait until the server reads the disk;
     - if the distribution kit is in the form of ISO-image - mount the disk image using tools of your operative system;
   - for a virtual server:
     - if the distribution kit is on the optical disc - insert the disk into CD or DVD drive of the computer where you are working and then connect the disk to the virtual server (see the example below);
     - if the distribution kit is in the form of ISO-image - mount the disk image using tools of your operative system and then connect the disk to the virtual server (see the example below).

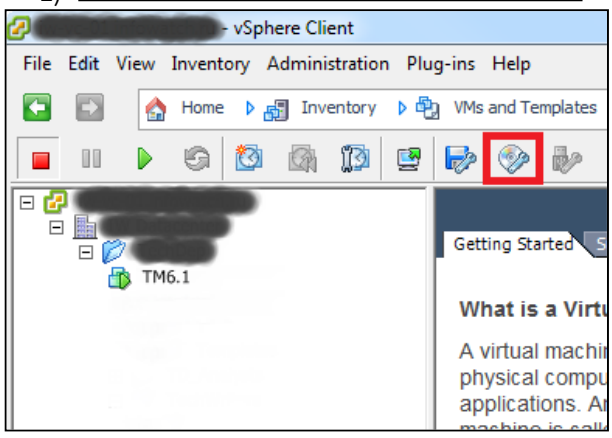
Note:

The example assumes that the distribution disc is in the **F** device of the computer from which TM virtual server is being updated (i.e., the computer from which we logged into VMware vSphere Client).

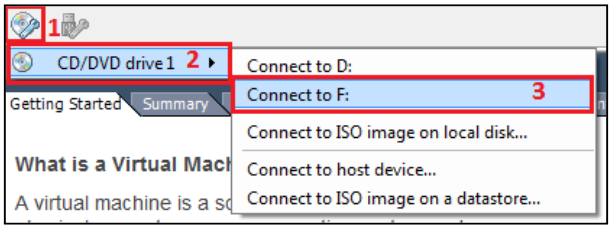
1)



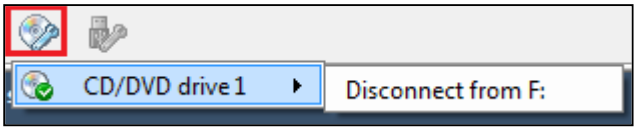
2)



3)



Almost immediately after clicking **Connect to F:** the disk will be connected to the virtual server and the menu will look as follows:



When the distribution disk is installed, everything is ready for the update. Update the servers, following these instructions:

- Updating TM All-in-one Enterprise and Standard - updating the server with "All-in-One" installation type (*Enterprise* or *Standard*);
- Updating TM in case of distributed installation - updating the server with a distributed installation type (database and TM servers are installed separately);

Note:

For information how to update Device Monitor Server and Agents, see " Updating InfoWatch Device Monitor".

Note:

After the System update the pre-installed privilleges for complete queries and reports management are unavailable for users with *Security officer* and *Administrator* roles.

.

4.1 Updating TM All-in-one Enterprise and Standard

The update will be done through a console of the server being updated. A console (or a terminal) is a window of a Linux-based operating system where you can type commands in a text form - as strings. Depending on the server type, when started, the console may display general information on the server and an invitation to log in or just an invitation to log in without general information. In any case, you have to enter the user login that will be used for working the console.

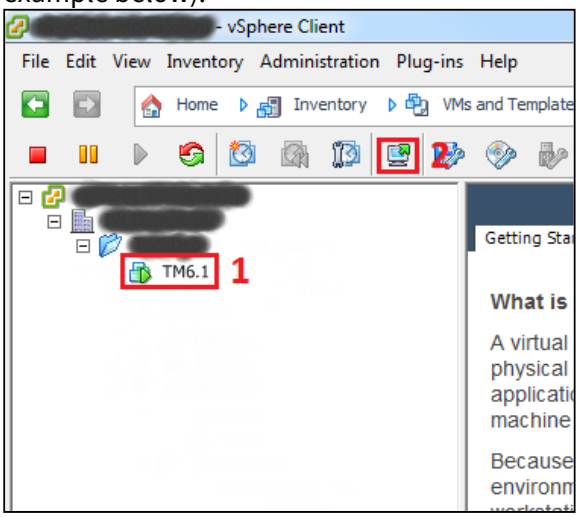
The console looks as follows:



To update the System, perform the following actions:

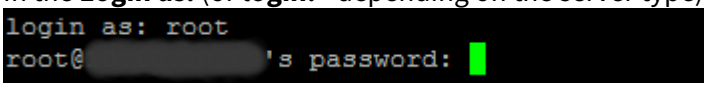
1. Open the console of the server being updated:
   - in the case of a physical server - the console is displayed on the screen of a monitor connected to the server;

- in the case of a virtual server - run **Launch Virtual Machine Console** command (see an example below).

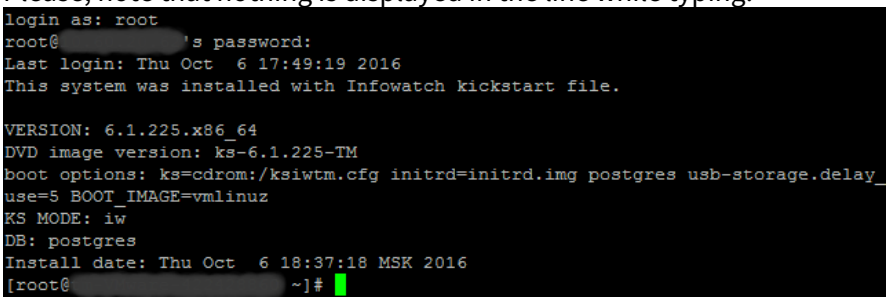


A window with the server console will open.

2. In the **Login as:** (or **login:** - depending on the server type) line, enter *root* and press **Enter**.



3. In the **root@<server_address>'s password:** (or **Password:** - depending on the server type) line, enter a password of the *root* user (superuser) and press **Enter**.
Please, note that nothing is displayed in the line while typing.



The screen will display the service information and (in the last line) an invitation to enter the command (command line).

> **Tip:**
>
> The commands within the console are entered from the keyboard and must be confirmed by pressing **Enter**. So, if the instruction tells you to enter the command, it means that you should enter the command and then press **Enter**. Once the command is executed, the invitation is displayed again - it is ended with # or $ (depending on the user who logged in). Before typing the next command, make sure that an invitation is displayed at the command line.

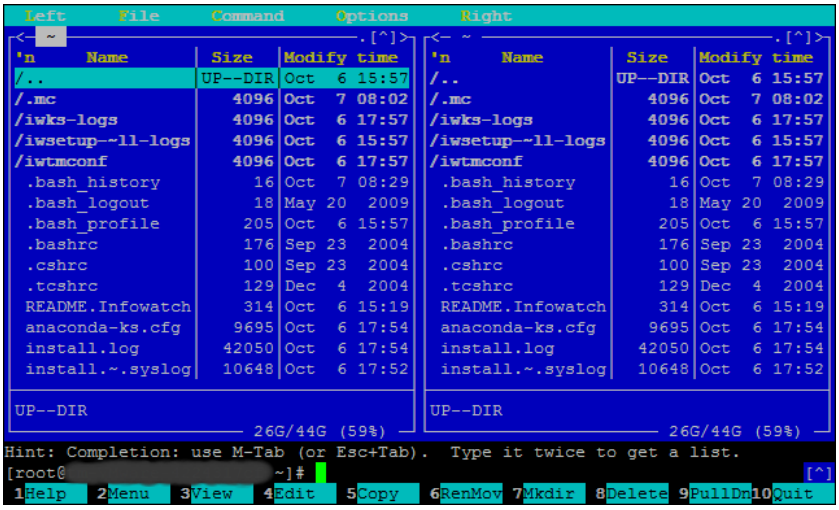
Note:

If you connect remotely via SSH, it is recommended using the Screen utility. Thus you can avoid problems in case of lost connection with updating server. When disconnecting from the utility, all the prcocesses started are not to be interrupted and you may safely continue the System update.
Important! Using Screen is highly recommended when working with DB and updating DBMS.
Basic commands:

- `screen` - start the utility;
- `Ctrl+a d` - disconnect from screen (to be input within the screen window);
- `screen -ls` - display the list of screen running;
- `screen -r` - connect to screen again;
- `screen -r name` - connect to specific screen with «name»;
- `exit` - exit screen (to be input within the screen window).

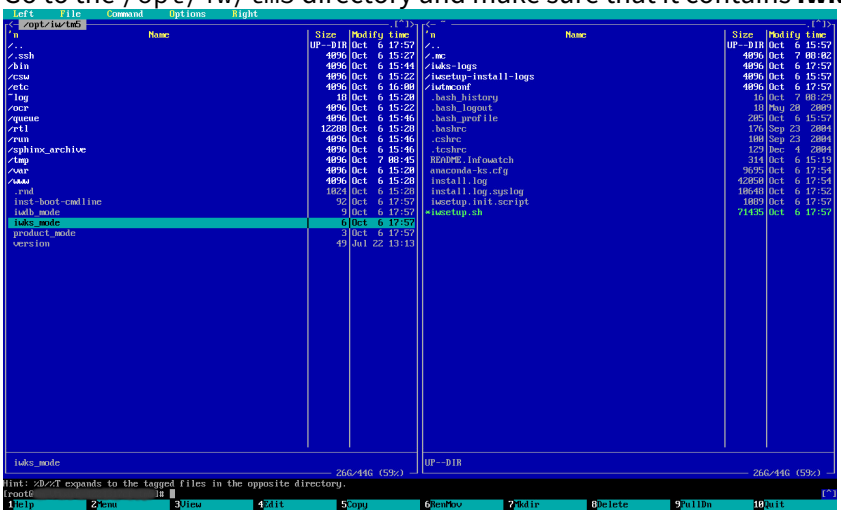
4. Enter the command to call the file manager:

```
mc
```



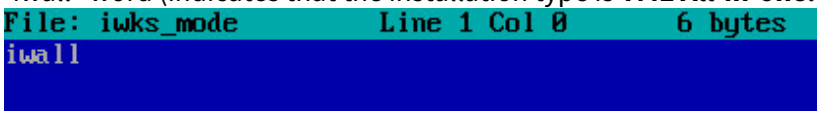
The screen will display a window of *Midnight Commander* file manager where you can view files. You can navigate in the file manager using keyboard arrows and the **Enter** key or with a mouse. Besides, you can enter commands at the command line which is displayed in the lower part of the screen (for entering commands, no additional actions are required).
To go up one level, position the cursor in the **/..** field (the first line in the file manager) and press **Enter**.

5. Go to the `/opt/iw/tm5` directory and make sure that it contains **iwks_mode** file.

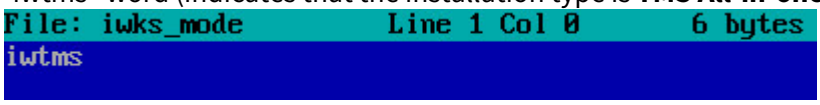


> **Note:**
>
> If **iwks_mode** file is missing in the directory, you need to create it. For this, enter the command:
> `touch iwks_mode`

6. Position the cursor on the **iwks_mode** fine and press **F3**.
   Depending on the System edition (*Enterprise* or *Standard*) the content of **iwks_mode** file will be displayed on the screen:
   - "iwall" word (indicates that the installation type is **TME All-in-one: TM+DB server**)

     ;
   - "iwtms" word (indicates that the installation type is **TMS All-in-one: TM+DB server**)

     .

   > **Note:**
   >
   > If the file content is different:
   > 1. press **F3** again.
   > 2. press **F4**.
   > 3. in the window that opens, delete all characters and depending on the System edition, enter `iwall` or `iwtms`
   > 4. press **F2**.
   > 5. in the window that opens, confirm the file saving by clicking **Save**.
   > 6. press **F10**.
   > 7. press **F3** and make sure that the file content is correct.

7. Press **F3**.

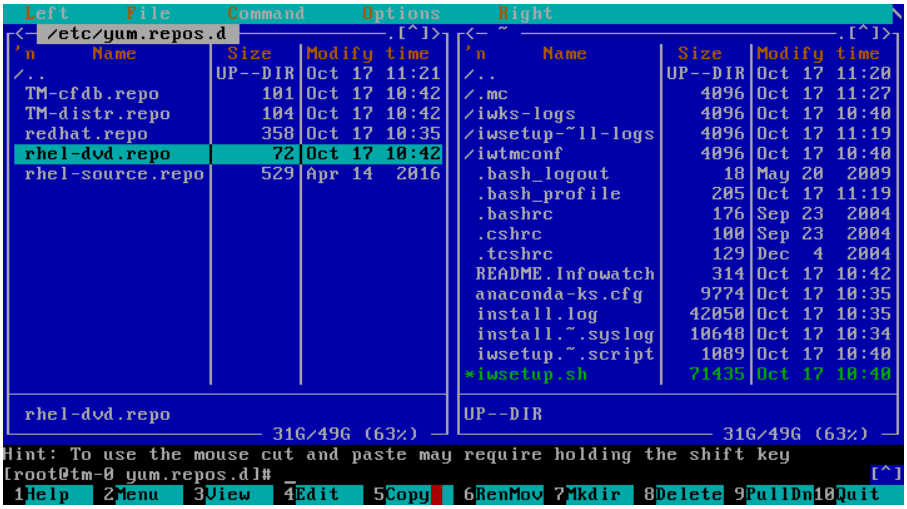
8. Enter the command:
   `mkdir -p /mnt/rhel-dvd`
   The `/mnt/rhel-dvd` directory will be created.
9. Make sure that a distribution disk with InfoWatch Traffic Monitor is connected to the server (see "Updating the System", step 2).
10. Enter the command:
    `mount /dev/cdrom /mnt/rhel-dvd`

> **Note:**
>
> There is a space between 2 commands "/dev/cdrom" and "/mnt/rhel-dvd".

The distribution disk, located in the `/dev/cdrom` section will be connected as a repository in the `/mnt/rhel-dvd` directory.

11. Go to the `/mnt/rhel-dvd` directory and make sure that in contains files and folders. If the directory is empty, repeat steps 9 and 10.
12. Go to the `/etc/yum.repos.d` directory and make sure that it contains **rhel-dvd.repo** file (this file is required to specify the path to the update files).

> **Note:**
>
> Taking into account, that in the file manager the elements are sorted in the alphabetic order, folders precede files (as they begin with a slash (/)). So the **/yum.repos.d** directory is one of the last in the last of folders list which begin with "/", but is before the first file .



> **Note:**
>
> If the **rhel-dvd.repo** file is missing in the directory, you need to create it. For this, enter the command:
> `touch rhel-dvd.repo`

13. Position the cursor on the **rhel-dvd.repo** file and press **F4**.
14. Make sure the file content includes the following text:

```
[rhel-dvd]
name=Red Hat Enterprise Linux $releasever - $basearch - DVD
baseurl=file:///mnt/rhel-dvd/
enabled=0
gpgcheck=0
[rhel-dvd-iwtm]
name=DVD_IWTM
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/Linux/
enabled=0
gpgcheck=0
[rhel-dvd-iwtm-cfdb]
name=DVD_IW-CFDB
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/cfdb/
enabled=0
gpgcheck=0
```

> **Important!**
>
> If the text of the file is different, replace it with the specified one.

15. In the `[rhel-dvd]`, `[rhel-dvd-iwtm]` and `[rhel-dvd-iwtm-cfdb]` blocks, change the values of the `enabled` parameter from `0` to `1`. The changes in content filtration base, implemented during the operation are to be saved after the update.
16. Press **F2**.
17. In the window that opens, confirm the file saving by clicking **Save**.
18. Press **F10**.
19. Press **F3** and make sure that the file content is correct, then press **F3** again to close the file.
20. To exit the file manager (is required to better control command execution), enter the command:
    `exit`
21. Enter the command to clean the package manager cache:
    `yum clean all`
22. Enter commands to stop the interceptors:

```
service iwtm stop icap
service iwtm stop smtpd
service iwtm stop expressd
service iwtm stop sniffer
service iwtm stop xapi_xapi
service iwtm stop xapi_puppy
```

23. Enter the command to call the file manager again:
    `mc`
24. Wait until all events which are in the queue for processing are processed. Events in the queue are located in the following directories:
    `/opt/iw/tm5/queue/analysis/.db/`
    `/opt/iw/tm5/queue/analysis/.in/`
    `/opt/iw/tm5/queue/analysis/.out/`
    `/opt/iw/tm5/queue/db/.db/`
    `/opt/iw/tm5/queue/db/.in/`
    `/opt/iw/tm5/queue/db/.out/`
    `/opt/iw/tm5/queue/smtp/.db/`
    `/opt/iw/tm5/queue/smtp/.in/`
    `/opt/iw/tm5/queue/smtp/.out/`
    When all the events are processed, these directories will be empty.

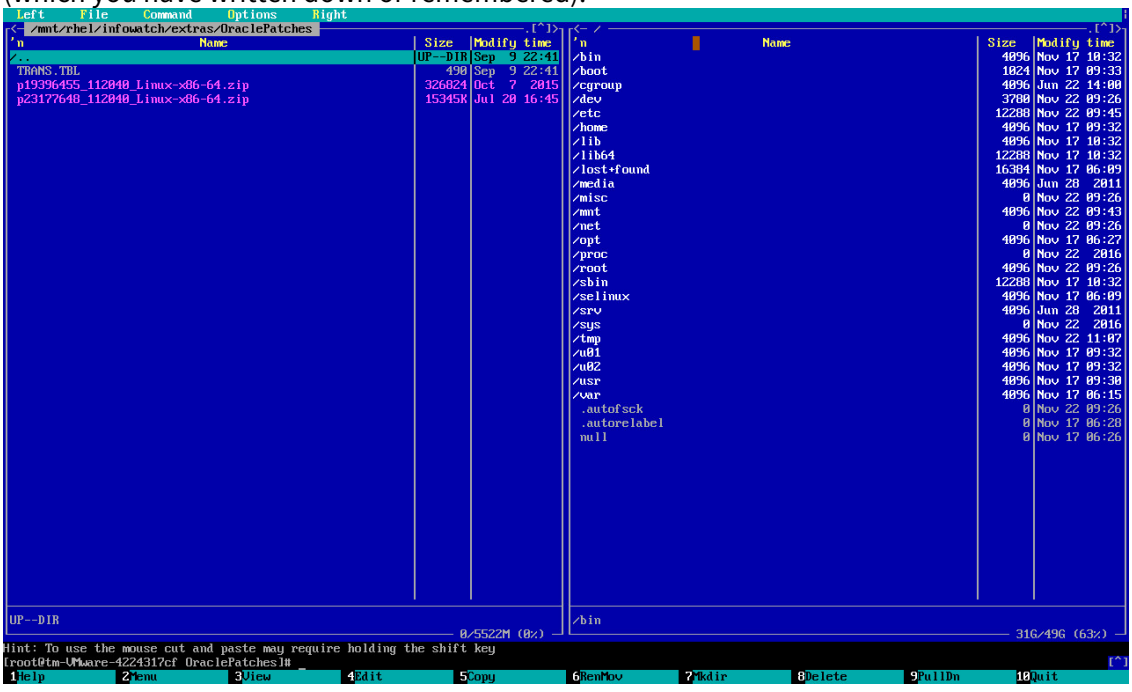
    > **Important!**
    >
    > To continue the update, make sure that all specified directories are empty. Otherwise, we cannot guarantee that the System will be updated correctly and will operate properly after the update.
    > If for some reason, you cannot wait until the processing is complete, you can delete events from the queue; such events will be completely removed from the System.
    > To delete the event, go to the required directory in the file manager, position the cursor on the event you want to delete and press **F8**. Then, confirm the deletion by clicking **Yes** in the confirmation window that opens.

25. To exit the file manager (is required to better control command execution), enter the command:
    `exit`
26. To stop services of Traffic Monitor server, enter the command:
    `service iwtm stop`
27. If Oracle DBMS is used in the System, do the following actions:
    a. Enter the command to stop DBMS Oracle:
       `service oracle stop`
    b. Enter the command to switch to the desired user:
       `su - oracle`
    c. Enter the command to get the list of patches installed in the System:
       `/u01/app/oracle/product/db_1/OPatch/opatch lsinventory | grep "Patch" | grep "applied"`

```
[oracle@                    ]$ /u01/app/oracle/product/db_1/OPatch/opatch lsinventory | grep "Patch" | grep "applied"
Patch  21538567     : applied on Tue Nov 22 12:37:41 MSK 2016
Patch  21538558     : applied on Tue Nov 22 12:37:39 MSK 2016
Patch  21538485     : applied on Tue Nov 22 12:37:32 MSK 2016
Patch  21352646     : applied on Tue Nov 22 12:37:31 MSK 2016
Patch  21179898     : applied on Tue Nov 22 12:37:29 MSK 2016
Patch  21051862     : applied on Tue Nov 22 12:37:19 MSK 2016
Patch  21051858     : applied on Tue Nov 22 12:36:56 MSK 2016
Patch  21051852     : applied on Tue Nov 22 12:36:43 MSK 2016
Patch  21051840     : applied on Tue Nov 22 12:36:42 MSK 2016
Patch  21051833     : applied on Tue Nov 22 12:36:41 MSK 2016
Patch  20631274     : applied on Tue Nov 22 12:36:39 MSK 2016
Patch  20506715     : applied on Tue Nov 22 12:36:31 MSK 2016
Patch  20506699     : applied on Tue Nov 22 12:36:24 MSK 2016
Patch  20142975     : applied on Tue Nov 22 12:36:19 MSK 2016
Patch  19972569     : applied on Tue Nov 22 12:36:17 MSK 2016
Patch  19972568     : applied on Tue Nov 22 12:36:14 MSK 2016
Patch  19972566     : applied on Tue Nov 22 12:36:13 MSK 2016
Patch  19972564     : applied on Tue Nov 22 12:36:07 MSK 2016
Patch  19584068     : applied on Tue Nov 22 12:36:00 MSK 2016
Patch  19544839     : applied on Tue Nov 22 12:35:57 MSK 2016
Patch  19463893     : applied on Tue Nov 22 12:35:43 MSK 2016
Patch  18203838     : applied on Tue Nov 22 12:35:37 MSK 2016
Patch  18203837     : applied on Tue Nov 22 12:35:35 MSK 2016
Patch  18203835     : applied on Tue Nov 22 12:35:28 MSK 2016
Patch  17811447     : applied on Tue Nov 22 12:35:27 MSK 2016
Patch  17811438     : applied on Tue Nov 22 12:35:25 MSK 2016
Patch  17811429     : applied on Tue Nov 22 12:35:19 MSK 2016
Patch  19396455     : applied on Tue Nov 22 12:34:40 MSK 2016
```

The screen will display the list of patches installed in the System. Write down or remember all numbers specified after the word "Patch" (the patch number can also be the first eight digits after the letter "**p**". For example, for **p19972569_112040_Linux-x86-64.zip** the patch number is 19972569). There numbers are required to compare installed patches and patches that are needed for the update.

d. Enter the command to call the file manager again:
   `mc`
e. Go to the `/mnt/rhel-dvd/infowatch/extras/OraclePatches` directory and make sure that patch numbers in the directory are in the list of patch numbers installed in the System (which you have written down or remembered).



Note:

If any patch from `/mnt/rhel-dvd/infowatch/extras/OraclePatches` directory is not in the list of installed patches, you need to install this patch.
Before installing the patch, OPatch utility is required to be updated. The following actions are to be taken to do that:

i. If *Midnight Commander* file manager is running, to exit it (is required for better control command execution) enter the command:
`exit`
ii. To make a backup copy, enter the command:
`mv /u01/app/oracle/product/db_1/OPatch /u01/app/oracle/product/db_1/OPatch_backup`
iii. To extract the archive with a new version, enter the command:
`unzip /mnt/rhel-dvd/infowatch/extras/OraclePatches/p6880880_112000_Linux-x86-64.zip -d /u01/app/oracle/product/db_1`
iv. To grant the oracle user rights for operating the directory and files, enter the command:
`chown oracle:oinstall -R /u01/app/oracle/product/db_1/OPatch`

To install the patch, the following actions are to be taken (below you can see the example of patch number 12345678 - p12345678_112040_Linux-x86-64.zip):

i. If *Midnight Commander* file manager is running, to exit it (is required for better control command execution) enter the command:
`exit`
ii. Enter the command to extract the patch:
`unzip /mnt/rhel-dvd/infowatch/extras/OraclePatches/p12345678_112040_Linux-x86-64.zip -d /tmp/`
iii. To go to the required directory, enter the command:
`cd /tmp/12345678/`
iv. In accordance with patch type, enter the command to install the patch :
    - `/u01/app/oracle/product/db_1/OPatch/opatch napply . -silent -ocmrf /mnt/rhel-dvd/infowatch/extras/OraclePatches/ocm0.rsp` (in case of composite patch);
    - `/u01/app/oracle/product/db_1/OPatch/opatch apply -silent -ocmrf /mnt/rhel-dvd/infowatch/extras/OraclePatches/ocm0.rsp` (in case of a single patch).

    When the patch is installed, the screen will display the message:
    ```
    OPatch completed with warnings.
    Press any key to continue..._
    ```
    Press any key to continue.
    Then, the changed SQL files should be downloaded into DB.
v. Enter the command to switch to the `root` user again:
`exit`

vi. Enter the command to start the Oracle DBMS:
`service oracle start`
vii. Enter the command to switch to the required user:
`su - oracle`
viii. In each separate base within the Oracle home, where the patch is installed it is required switching using SQL*Plus. Login as SYSDBA and run the script `catbundle.sql`, to do this the following command are to be entered:
```
cd $ORACLE_HOME/rdbms/admin
sqlplus /nolog
CONNECT / AS SYSDBA
@catbundle.sql cpu apply
QUIT
```
The `catbundle.sql` script running is displayed within the `dba_registry_history` as package set updates (PSU).
ix. To delete the files that are no more needed, enter the command:
```
cd /tmp/ && rm -rf /tmp/12345678/ && rm -f /tmp/
PatchSearch.xml
```

Details on the installation can be found within the README file, located in a specific directory named after each patch.

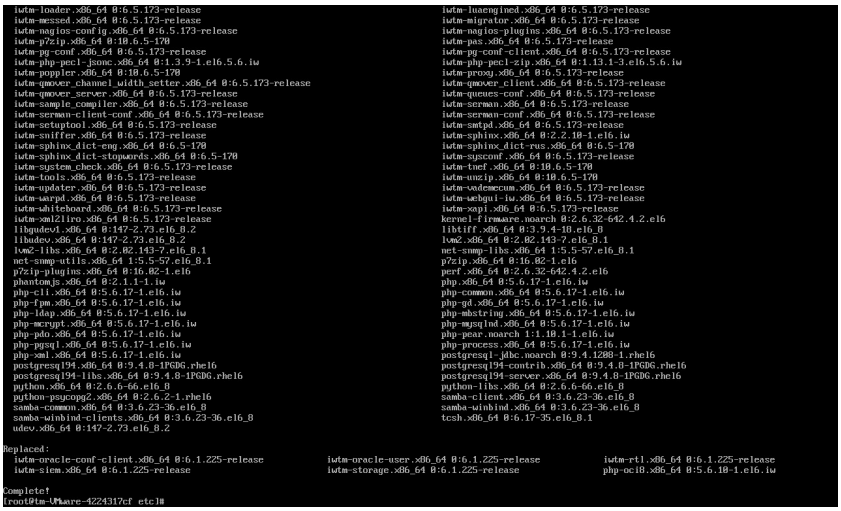
f. If *Midnight Commander* file manager is running, exit it (required for better command execution control) with the command:
```
exit
```
g. to switch back to the *root* user, enter the command:
`exit`
h. to start Oracle DBMS, enter the command:
```
service oracle start
```

28. **Depending on the DBMS used, enter the command to start the packages update process:**

- `yum upgrade --exclude=iwtm-rtl-pg,iwtm-siem-pg` (if **Oracle DBMS** is used)
- `yum upgrade --exclude=iwtm-rtl-oracle,iwtm-siem-oracle` (if **PostgreSQL DBMS** is used)

29. Before loading the files required for installation, the screen will display a request as follows:
```
Total download size: 4.4 M
Is this ok [y/N]:
```
. To continue, type **Y** and press **Enter**.
Downloading packages from the repository and then installing the packages will begin. This may

take some time.



30. Enter the command within the file manager to find and display the list of files with **.rpmnew** extension:
    `find / -name "*rpmnew*" -print`
    If the files mentioned have been found, they should be correctly merged with configuration files (see "Merging configuration files").

> **Important!**
>
> If PostgreSQL DBMS is used in the System, it is necessary to take the following steps when updating Traffic Monitor version 6.0 or 6.1 to 6.5 and higher:
> This page has not yet been translated to English.

31. Enter the command to call the file manager:
    `mc`
32. Go to `/opt/iw/tm5/etc/scripts/` directory and make sure the file **iwssid.lua.upgrade** is in place. The file **iwssid.lua.upgrade** is not being used by the System, it is an information source to restore the System operation in case of complete customization.
33. Also `/opt/iw/tm5/etc/scripts/` directory should contain the file **iwssid.lua that** is recommended to remain with no changes implemented in case any term from the following is complied:
    - System's update is held as per version 6.9;
    - **iwssid.lua** file has not been edited before the update.

    Otherwise, this should be correctly merged with **iwssid.lua.rpmnew** file (see "Merging configuration files").
34. **Depending on DBMS** used go to the directory:
    - `/opt/iw/tm5/csw/oracle` (if **Oracle DBMS** is used);
    - `/opt/iw/tm5/csw/postgres` (if **PostgreSQL DBMS** is used).

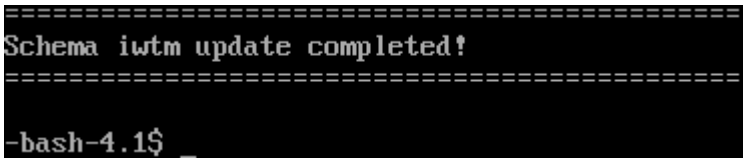
35. Select the **database.conf** file.



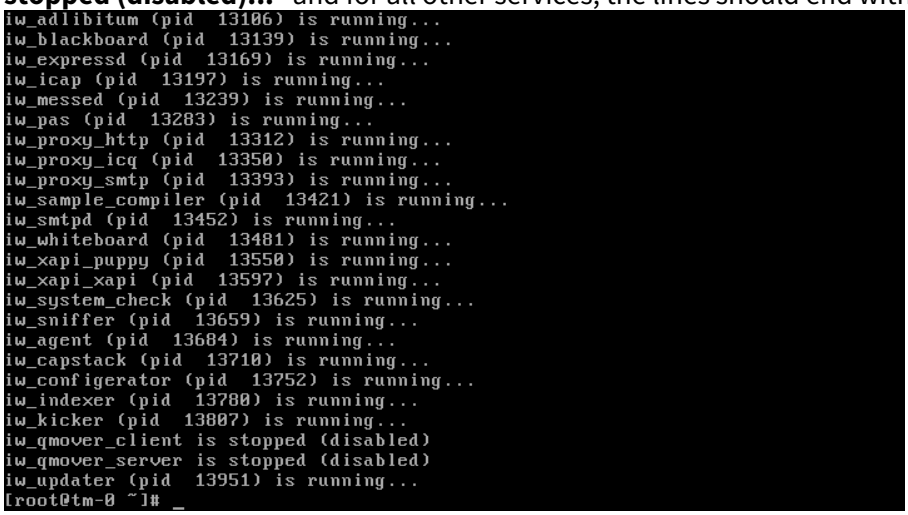
36. Press **F3**.
37. Make sure that for the `\set schema_version` parameter, a version to which you are updating the System is specified. If an old version is specified, repeat steps 27 - 36.
38. Press **F3**.
39. To exit the file manager (is required to better control command execution), enter the command:
    `exit`
40. To stop services, enter the commands one by one:
    ```
    service iwtm stop
    service iwtm-php-fpm stop
    service nagios stop
    ```

> **Note:**
>
> If the Crawler subsystem is a part of System, it is required to stop the services of this subsystem (on Crawler server). This is to be done on the server, where the subsystem is installed with Windows standard tools: **Start** - **Control Panel** - **Administrative Tools** - **Services**, then select the service in the list and click **Stop service**.

41. If **PostgreSQL DBMS** is used in the System, perform Updating PostgreSQL DBMS.
42. **Depending on DBMS used**, enter the command to switch to the required user:
    - `su - oracle` - to switch to the *oracle* user (if **Oracle DBMS** is used in the System)
    - `su - postgres` - to switch to the *postgres* user (if **PostgreSQL DBMS** is used in the System)
43. **Depending on DBMS used**, enter the command to go to the required directory:
    - `cd /opt/iw/tm5/csw/oracle` - (if **Oracle DBMS** is used in the System)
    - `cd /opt/iw/tm5/csw/postgres` - (if **PostgreSQL DBMS** is used in the System)
44. Enter the command to start the database update script:
    `./update.sh`
    The process of updating the database scheme will start. It may take some time. When the update is complete, the screen will display an information message and a command prompt:



45. Enter the command to clear the cache:
    `redis-cli flushall`
46. To switch back to the *root* user, enter the command:
    `exit`
47. Enter the command to call the file manager:
    `mc`
48. Go to `/etc/yum.repos.d`, place cursor on the file **rhel-dvd.repo** and press **F4.**
49. In the `[rhel-dvd],[rhel-dvd-iwtm] and [rhel-dvd-iwtm-cfdb]` blocks, change values of the `enabled` parameter from `1` to `0`.
50. Press **F2**.
51. Click **Save** in the opened window to confirm saving the file.
52. Press **F10**.
53. Press **F3** and make sure the file is correct, then press **F3** again to close the file.
54. To exit the file manager (required for beeter commands execution)б enter the command:
    `exit`
55. Enter the command to restart the server:
    `reboot`
56. Wait until the server is started and repeat steps **2** and **3** of this instruction to log in the console.
57. Enter the command to check if the processes are started:
    `service iwtm status`
    The screen will display the list of processes and their status. Generally, `iw_qmover_client` and `iw_qmover_server` services are stopped and all other services are started. For `iw_qmover_client` and `iw_qmover_server` services, the lines should end with "**is stopped (disabled)...**" and for all other services, the lines should end with "**is running...**":



Note:

If the Crawler subsystem is a part of System, it is required to start the services of this subsystem (on Crawler server). This is to be done on the server where the subsystem is installed with Windows standard tools: **Start** - **Control Panel** - **Administrative Tools** - **Services** , then select the service in the list and click **Start service**.

Updating Traffic Monitor All-in-one server is complete. Version of the System in the **About** window of the Management Console will be changed. If the System includes other servers or subsystems to be updated, follow instructions in this section.

Warning!

If automatic synchronizations with LDAP servers are configured in the System, then after update, perform synchronizations manually to guarantee load of entities (see "*Infowatch Traffic Monitor. User Guide*", "Running Synchronization with Server Manually").

Note:

For the Management Console to be displayed correctly, delete the cache in your browser before you start working in the Management Console. This is done with browser standard tools.

4.2 Updating TM in case of distributed installation

The update will be done through a console of the server being updated. A console (or a terminal) is a window of a Linux-based operating system where you can type commands in a text form - as strings. Depending on the server type, when started, the console may display general information on the server and an invitation to log in or just an invitation to log in without general information. In any case, you have to enter the user login that will be used for working the console.

The console looks as follows:



All TM servers (TME Node Server installation type) and DBMS server (TME DB Server) must be updated.

Note!

Each server should have a unique correct FQDN.

Note:

If you connect remotely via SSH, it is recommended using the utility Screen. Thus, you can avoid problems in case of lost connection with updating server. When disconnecting from the utility, all the prcocesses started are not to be interrupted and you may safely continue the System update.

Important! Using Screen is highly recommended when working with DB and updating DBMS.

Basic commands:

- `screen` - start the utility;
- `Ctrl+a d` - disconnect from the screen (to be input within the screen window);
- `screen -ls` - display the list of screen running;
- `screen -r` - connect to screen again;
- `screen -r name` - connect to a specific screen with «name»;
- `exit` - exit the screen (to be input within the screen window).

The update is done in the following order:

Step 1. Updating all TM servers (TME Node Server).

Step 2. Updating DBMS server (TME DB Server).

Step 3. Healthcheck of internal services of the System.

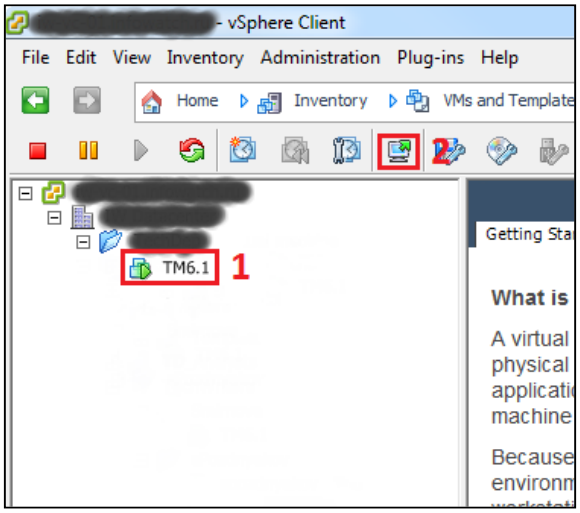
Step 4. Restarting DBMS server (TME DB Server).

Step 5. Restarting all TM servers (TME Node Server).

STEP 1. UPDATING ALL TM SERVERS (TME Node Server)

To update TM servers (TME Node Server), take the following steps on each of them:

1. Open the console of the server being updated:
   - in the case of a physical server - the console is displayed on the screen of a monitor connected to the server;
   - in the case of a virtual server - run **Launch Virtual Machine Console** command (see the example below).



A window with the server console will open.

2. In the **Login as:** (or **login:** - depending on the server type) line, enter *root* and press **Enter**.

```
login as: root
root@[redacted]'s password:
```

3. In the **root@<server_address>'s password:** (or **Password:** - depending on the server type) line, enter a password of the *root* user (superuser) and press **Enter**.
Please, note that nothing is displayed in the line while typing.

```
login as: root
root@[redacted]'s password:
Last login: Thu Oct  6 17:49:19 2016
This system was installed with Infowatch kickstart file.

VERSION: 6.1.225.x86_64
DVD image version: ks-6.1.225-TM
boot options: ks=cdrom:/ksiwtm.cfg initrd=initrd.img postgres usb-storage.delay_
use=5 BOOT_IMAGE=vmlinuz
KS MODE: iw
DB: postgres
Install date: Thu Oct  6 18:37:18 MSK 2016
[root@[redacted] ~]#
```

The screen will display the service information and (in the last line) an invitation to enter the command (command line).

> **Tip:**
>
> In the console, commands are entered from the keyboard and must be confirmed by pressing **Enter** . So, if the instruction tells you to enter the command, it means that you should enter the command and then press **Enter** . Once the command is executed, the invitation is displayed again - it is ended with `#` or `$` (depending on the user who logged in). Before typing the next command, make sure that an invitation is displayed at the command line.

4. Enter the command to call the file manager:
`mc`



The screen will display a window of *Midnight Commander* file manager where you can view files. You can navigate in the file manager using keyboard arrows and the **Enter** key or with a mouse. Besides, you can enter commands at the command line which is displayed in the lower part of the screen (for entering commands, no additional actions are required).
To go up one level, position the cursor in the **/..** field (the first line in the file manager) and press **Enter**.

5. Go to the `/opt/iw/tm5` directory and make sure that it contains **iwks_mode** file.



> **Note:**
>
> If **iwks_mode** file is missing in the directory, you need to create it. For this, enter the command:
> `touch iwks_mode`

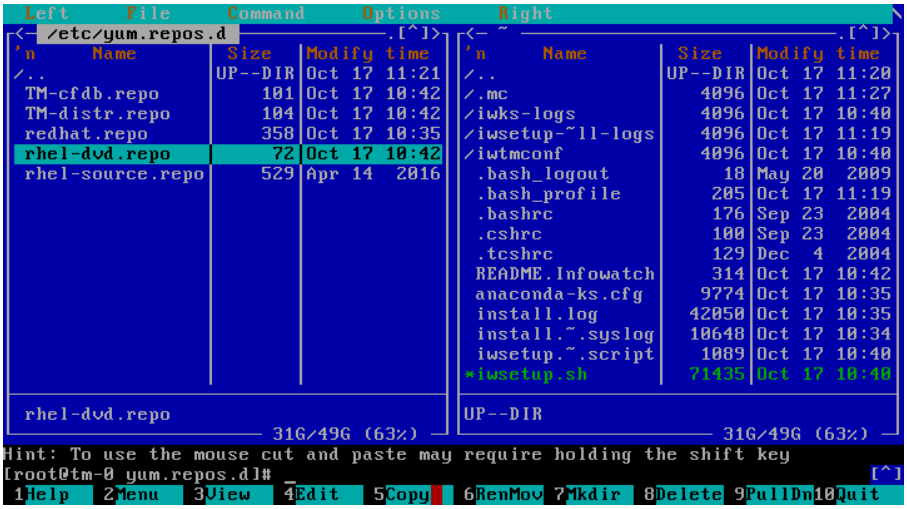
6. Position the cursor on the **iwks_mode** fine and press **F3**.
The screen will display the content of **iwks_mode** file: "iwtm" word (indicated that the installation type is **TME Node server**).

> **Note:**
>
> If the file content is different:
> 1. press **F3** again.
> 2. press **F4**.
> 3. in the window that opens, delete all characters and enter `iw tm`
> 4. press **F2**.
> 5. in the window that opens, confirm the file saving by clicking **Save**.
> 6. press **F10**.
> 7. press **F3** and make sure that the file content is correct.

7. Press **F3**.
8. > **Note:**
   >
   > If you update the System from version **6.10.x**, after this please go to action 9 .

   To prepare the System for update the following actions should be taken:
   a. **On DBMS server (TME DB Server)**:
   i. Take the actions 1-7 of Step 2 (see below).
   ii. Go to `/opt/iw/tm5/etc` directory, position the cursor on **serman.conf** file and press **F3**.
   iii. In `DefaultInterface` find the IP address.
   b. On all **TM (TME Node Server) servers**
   i. Go to `/opt/iw/tm5/etc` directory, position the cursor on **serman.conf** file and press **F4**.
   ii. Find `SermanHost` block.
   Compare its value with IP address, specified in **serman.conf** on **DBMS server (TME DB Server)** .
   iii. In case they don't match, replace the value of `SermanHost` block on **TM serves (TME Node Server)** with IP address, specified in `DefaultInterface` block of **serman.conf** file on **DBMS server (TME DB Server)** .
   iv. Press **F2**.
   v. In the opened window make sure the file is to be saved by pressing **Save**.
   vi. Press **F10**.
   c. On **DBMS server (TME DB Server)**, press F3 to exit the **serman.conf** file viewing mode.
9. Go to `/etc/yum.repos.d` directory and make sure that it contains the **rhel-dvd.repo** file (this file is required to specify the path to the update files).

> **Note:**
>
> Taking into account that elements are sorted in the file manager in the alphabetic order, folders precede files (as they begin with a slash (**/**)) . So the **/yum.repos.d** directory is one of the last in the last of folders which begin with "/", but is before the first file .



> **Note:**
>
> If the **rhel-dvd.repo** file is missing in the directory, you need to create it. To do this, enter the command:
> `touch rhel-dvd.repo`

10. Position the cursor on the **rhel-dvd.repo** file and press **F4**.
11. Make sure that the file content includes the following text:

```
[rhel-dvd]
name=Red Hat Enterprise Linux $releasever - $basearch - DVD
baseurl=file:///mnt/rhel-dvd/
enabled=0
gpgcheck=0
[rhel-dvd-iwtm]
name=DVD_IWTM
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/Linux/
enabled=0
gpgcheck=0
[rhel-dvd-iwtm-cfdb]
name=DVD_IW-CFDB
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/cfdb/
enabled=0
gpgcheck=0
```

> **Important!**
>
> If the text of the file is different, replace it with the specified one.

12. In the `[rhel-dvd]` and `[rhel-dvd-iwtm]` blocks, change values of the `enabled` parameter from `0` to `1`.
13. Press **F2**.
14. In the window that opens, confirm the file saving by clicking **Save**.

15. Press **F10**.
16. Press **F3** and make sure that the file content is correct, then press **F3** again to close the file.
17. To exit the file manager (is required to better control command execution), enter the command:
    `exit`
18. Enter the command to clear the package manager cache:
    `yum clean all`
19. Enter commands to stop the interceptors:
    ```
    service iwtm stop icap
    service iwtm stop smtpd
    service iwtm stop expressd
    service iwtm stop sniffer
    service iwtm stop xapi_xapi
    service iwtm stop xapi_puppy
    ```

    Note:

    If there are 2 and more interception servers within the System, the next action is to be taken only when the previous one was taken for each of the servers.

20. Enter the command to call the file manager again:
    `mc`
21. Wait until all the events in the queue for processing are processed. Events in the queue are stored in the following directories:
    ```
    /opt/iw/tm5/queue/analysis/.db/
    /opt/iw/tm5/queue/analysis/.in/
    /opt/iw/tm5/queue/analysis/.out/
    /opt/iw/tm5/queue/db/.db/
    /opt/iw/tm5/queue/db/.in/
    /opt/iw/tm5/queue/db/.out/
    /opt/iw/tm5/queue/smtp/.db/
    /opt/iw/tm5/queue/smtp/.in/
    /opt/iw/tm5/queue/smtp/.out/
    ```
    When all the events are processed, these directories will be empty.

    Important!

    To continue the update, make sure that all specified directories are empty. Otherwise, we cannot guarantee that the System will be updated correctly and will operate properly after the update.
    If for some reason, you cannot wait until the processing is complete, you can delete events from the queue, such events will be completely removed from the System.
    To delete the event, go to the required directory in the file manager, position the cursor on the event you want to delete and press **F8**. Then, confirm the deletion by clicking **Yes** in the confirmation window that opens.

22. To exit the file manager (is required to better control command execution), enter the command:
    `exit`

23. Enter the command:
`mkdir -p /mnt/rhel-dvd`
The following directory will be created: `/mnt/rhel-dvd`

> **Note:**
>
> If you update the System from version **6.10.x**, after this please go to action 29.

24. Connect a disk with the **current version** of InfoWatch Traffic Monitor to the server (see Updating the System, action 2).
25. Enter the command:
`mount /dev/cdrom /mnt/rhel-dvd`

> **Note:**
>
> There is a blank betwenn "/dev/cdrom" and "/mnt/rhel-dvd".

The distributive, located in `/dev/cdrom` will be connected as a repository in `/mnt/rhel-dvd` directory.
26. Go to `/mnt/rhel-dvd` directory and make sure the files and folders are in place. In case the directory is empty, repeat actions 24 and 25.
27. Enter the command:
`yum install iwtm-qatools`
Before downloading the packages required for installation, the following request will display:
```
================================================================================
==========================================
Package Arch Version Repository Size
================================================================================
==========================================
Installing:
iwtm-qatools x86_64 6.7.21.419-release TM-distr 3.9 M
Installing for dependencies:
iwtm-adlibitum-tool x86_64 6.7.21.419-release TM-distr 121 k
iwtm-liro2json x86_64 6.7.21.419-release TM-distr 405 k
Transaction Summary
================================================================================
==========================================
Install 3 Package(s)
Total download size: 4.4 M
Installed size: 22 M
Is this ok [y/N]:
```
To continue, type **Y** and press **Enter** on the keyboard.
28. After the package installation, enter the command:
`umount /mnt/rhel-dvd`
29. Connect the **new version** of InfoWatch Traffic Monitor distributive to the server (see Updating the System, action 2).

30. Enter the comand to clear the package manager cache:
    `mount /dev/cdrom /mnt/rhel-dvd`
31. Enter the comand to clear the package manager cache:
    `yum clean all`

> **Note:**
>
> If you update the System from version **6.10.x**, after this please go to action 34.

32. It is required to get the file (file name is - **sd_nodes.out**), containing IP-adresses of nodes for update. For this purpose, run the script entering the command:

In case of 2 nodes:	`bash /mnt/rhel-dvd/infowatch/upgrade/generate_serman_services_nodes_for_consul.sh`
In case of more then 2 nodes:	`bash /mnt/rhel-dvd/infowatch/upgrade/generate_serman_services_nodes_for_consul.sh --tm_nodes_count=<number_of_nodes>`

where `<number_of_nodes>` is the number of servers, including DBMS server.
In current example the command is as follows: `bash /mnt/rhel-dvd/infowatch/upgrade/generate_serman_services_nodes_for_consul.sh`
There is a model of console interface:

```
Will write to log file:
/var/log/infowatch/generate_serman_services_nodes_for_consul.log
WARNING: bad or empty input tm_nodes_count=, will use 2
OK: TM nodes count is 2
iwtm-serman-client-conf-6.7.21.419-release.x86_64
package iwtm-consul is not installed
OK: serman_prober reported 2 nodes
==> /opt/iw/tm5/tmp/sd_nodes.out <==
10.20.30.40 server
10.20.30.41 client
OK: Please copy the file to all nodes before upgrading TM on them, e.g.:
scp /opt/iw/tm5/tmp/sd_nodes.out 10.20.30.40:/opt/iw/tm5/tmp/sd_nodes.out
```

33. Copy the file **sd_nodes.out** to all the nodes specified, except the one, where it was created.
    Enter the following command:
    `scp /opt/iw/tm5/tmp/sd_nodes.out <node_address>:/opt/iw/tm5/tmp/sd_nodes.out`

    where `<node_address>` - is an IP-address or node's domain name, where the file **sd_nodes.out** should be copied to.
    Below is the command in accordance with our example:
    `scp /opt/iw/tm5/tmp/sd_nodes.out 10.20.30.40:/opt/iw/tm5/tmp/sd_nodes.out`

After entering the command, the following request will display:

```
Are you sure you want to continue connecting (yes/no)?
```

To continue, click **Yes** and press **Enter** on the keyboard.
Then enter the password for the receiving node and press **Enter**.

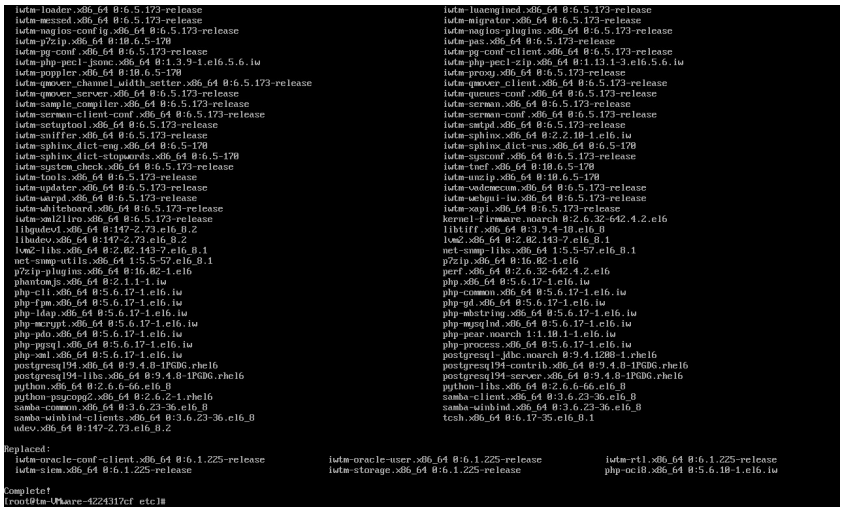
> **Important!**
>
> Make sure the file **sd_nodes.out** is located in `/opt/iw/tm5/tmp` directory on all the servers to be updated, including DBMS server, otherwise you should relocate the file to the directory specified.

> **Note:**
>
> Take the actions 23-27, 31 and 32 only on one node. You can choose any node.

34. To stop Traffic Monitor server services, enter the commands:
    `service iwtm stop`
    `service php-fpm stop` (if update is required for **6.7.x** or **6.9.x** version
    `service iwtm-php-fpm stop` (if update is required for **6.10.x** version)
    `service nagios stop`
35. **In accordance with the DBMS used**, enter the command to start the process of packages update:
    - `yum upgrade --exclude=iwtm-rtl-pg,iwtm-siem-pg` (if **Oracle DBMS** is used)
    - `yum upgrade --exclude=iwtm-rtl-oracle,iwtm-siem-oracle,` (if **PostgreSQL DBMS** is used)
36. Before loading files required for installation, the screen will display a request like this

```
Total download size: 4.4 M
Is this ok [y/N]:
```

. To continue, type **Y** and press **Enter**.
Downloading packages from the repository and then installing the packages will begin. This may take some time.



37. Enter the command to find and display the list of files with **.rpmnew** extension:
    `find / -name "*rpmnew*" -print`
    If the list of files is found, they should be correctly merged with configuration files accordingly (see " Merging configuration files").

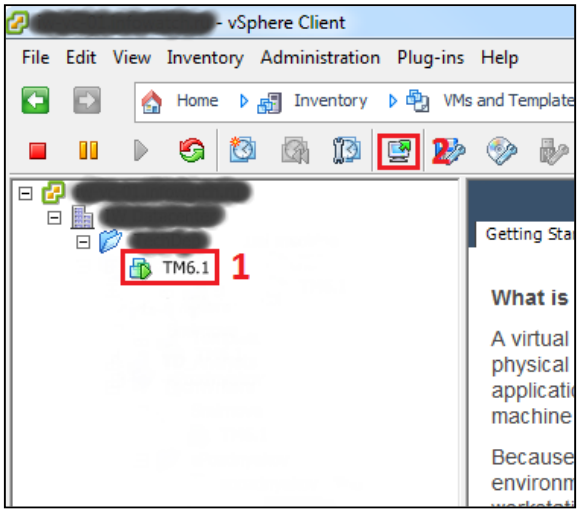
> **Important!**
>
> When updating Traffic monitor from 6.0 or 6.1 version to 6.5 and later, the following actions are to be obligatory taken:
> This page has not yet been translated to English.

38. Enter the command to call the file manager:
    `mc`
39. Go to `opt/iw/tm5/etc/scripts/` directory and make sure the file **iwssid.lua.upgrade** is in place. The file **iwssid.lua.upgrade** is not being used by the System, it is an information source to restore the System operation in case of complete customization.
40. Also `/opt/iw/tm5/etc/scripts/` directory should contain the file **iwssid.lua that** is recommended to remain with no changes implemented in case any term from the following is complied :
    - System Update ifs done from version 6.9;
    - The file **iwssid.lua** was not edited before the update.
    Otherwise, it should be correctly merged with **iwssid.lua** configuration file (see "Merging configuration files").
41. To leave the file manager, enter the command:
    `exit`
42. Update the DBMS server (TME DB Server) - see the description below.

STEP 2. UPDATING DBMS SERVER (TME DB Server)

To update the DBMS server (TME DB Server), take the following steps:

1. Open the console of the server being updated:
   - in the case of a physical server - the console is displayed on the screen of a monitor connected to the server;
   - in the case of a virtual server - run **Launch Virtual Machine Console** command (see an example below).



A window with the server console will open.

2. In the **Login as:** (or **login:** - depending on the server type) line, enter *root* and press **Enter**.

3. In the **root@<server_address>'s password:** (or **Password:** - depending on the server type) line, enter a password of the *root* user (superuser) and press **Enter**.
   The screen will display the service information and (in the last line) an invitation to enter the command (command line).
4. Enter the command to call the file manager:
   `mc`



   The screen will display a window of *Midnight Commander* file manager where you can view files. You can navigate in the file manager using keyboard arrows and the **Enter** key or with a mouse. Besides, you can enter commands at the command line which is displayed in the lower part of the screen (for entering commands, no additional actions are required).
   To go up one level, position the cursor in the **/..** field (the first line in the file manager) and press **Enter**.
5. Go to the `/opt/iw/tm5` directory and make sure that it contains **iwks_mode** file.



> **Note:**
>
> If **iwks_mode** file is missing in the directory, you need to create it. For this, enter the command:
> `touch iwks_mode`

6. Position the cursor on the **iwks_mode** file and press **F3**.
   The screen will display the content of **iwks_mode** file: "iwdb" word (indicates that the installation type is **TME DB server**).

   > **Note:**
   >
   > If the file content is different:
   > 1. press **F3** again.
   > 2. press **F4**.
   > 3. in the window that opens, delete all characters and enter `iwdb`
   > 4. press **F2**.
   > 5. in the window that opens, confirm the file saving by clicking **Save**.
   > 6. press **F10**.
   > 7. press **F3** and make sure that the file content is correct.

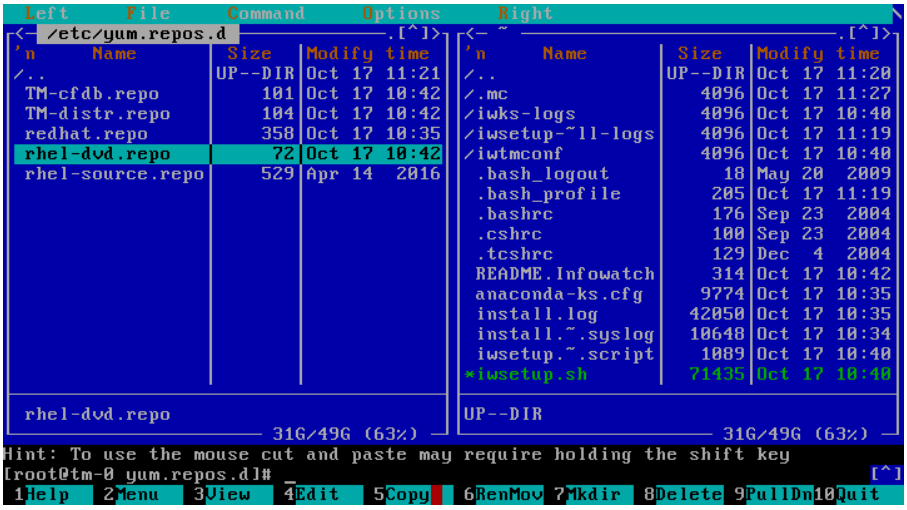
7. Press **F3**.
8. Enter the command:
   `mkdir -p /mnt/rhel-dvd`
   The `/mnt/rhel-dvd` directory will be created.
9. Make sure the distribution disk with InfoWatch Traffic Monitor is connected to the server (see "Updating the System", action 2).
10. Enter the command:
    `mount /dev/cdrom /mnt/rhel-dvd`

    > **Note:**
    >
    > There is a space between 2 commands "/dev/cdrom" and "/mnt/rhel-dvd".

    The distribution disk, located in `/dev/cdrom` section will be connected as a repository in the `/mnt/rhel-dvd` directory.
11. Go to `/mnt/rhel-dvd` directory and make sure that in contains files and folders. If the directory is empty, repeat steps 9 and 10.
12. Go to `/etc/yum.repos.d` directory and make sure that it contains **rhel-dvd.repo** file (this file is required to specify the path to the update files).

Note:

As, in the file manager, the elements are sorted in the alphabetic order, folders precede files (as they begin with a slash (/)) . So the **/yum.repos.d** directory is one of the last in the last of folders which begin with "/", but is previous to the first file .



Note:

If the file**rhel-dvd.repo** is missing in the directory, you need to create it. To do this, enter the command:
`touch rhel-dvd.repo`

13. Position the cursor on the file **rhel-dvd.repo** and press **F4**.
14. Make sure the file content includes the following text:

```
[rhel-dvd]
name=Red Hat Enterprise Linux $releasever - $basearch - DVD
baseurl=file:///mnt/rhel-dvd/
enabled=0
gpgcheck=0
[rhel-dvd-iwtm]
name=DVD_IWTM
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/Linux/
enabled=0
gpgcheck=0
[rhel-dvd-iwtm-cfdb]
name=DVD_IW-CFDB
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/cfdb/
enabled=0
gpgcheck=0
```

> **Important!**
>
> If the text of the file is different, replace it with the specified one.

15. In the `[rhel-dvd]`,`[rhel-dvd-iwtm]` and `[rhel-dvd-iwtm-cfdb]` blocks, change values of the `enabled` parameter from `0` to `1`. The content filtration base changes implemented during the operation are to be saved after the update.
16. Press **F2**.
17. In the window that opens, confirm the file saving by clicking **Save**.
18. Press **F10**.
19. Press **F3** and make sure that the file content is correct, then press **F3** again to close the file.
20. To exit the file manager (is required to better control command execution), enter the command:
    `exit`
21. Enter the command to clear the package manager cache:
    `yum clean all`
22. To stop services, enter the commands one by one:
    `service iwtm stop`

> **Note:**
>
> If in the System, the Crawler subsystem is installed you need to stop services of this subsystem (on Crawler server). This is done on the server where the subsystem is installed with Windows standard tools: **Start - Control Panel - Administrative Tools - Services**, then select the service in the list and click **Stop service**.

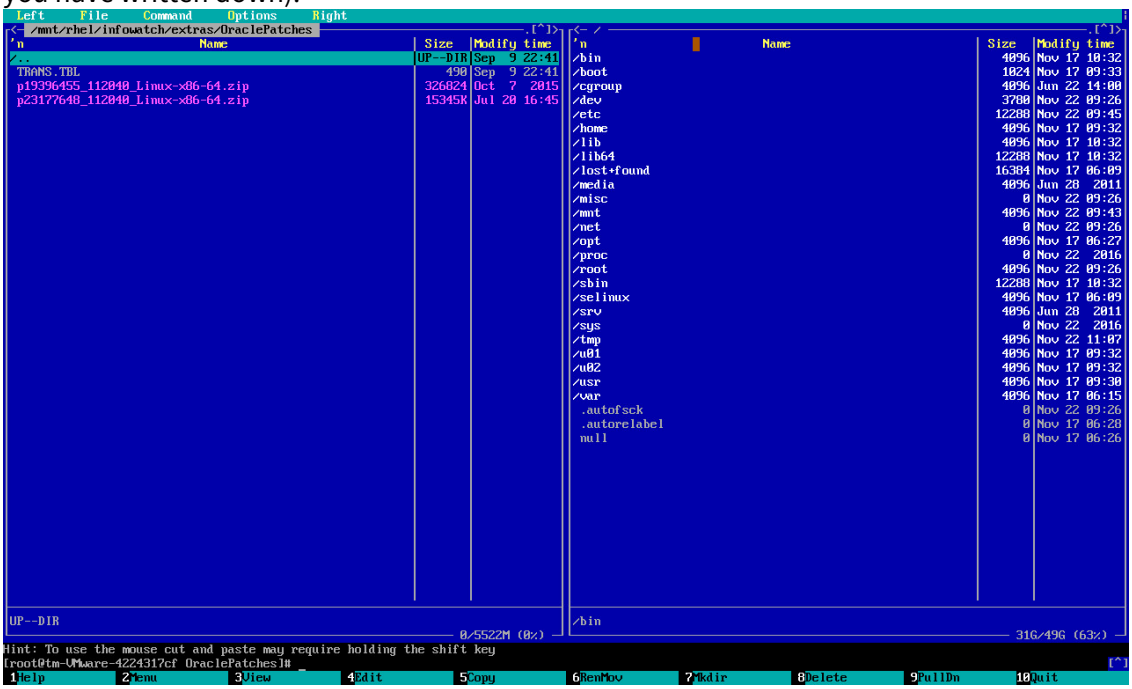
23. If Oracle DBMS is used in the System, perform the following steps:

    a. Enter the command to stop Oracle DBMS:
       `service oracle stop`
    b. Enter the command to switch to the required user:
       `su - oracle`
    c. Enter the command to get the list of patches installed in the System:
       `/u01/app/oracle/product/db_1/OPatch/opatch lsinventory | grep "Patch" | grep "applied"`

```
[oracle@                    ]$ /u01/app/oracle/product/db_1/OPatch/opatch lsinventory | grep "Patch" | grep "applied"
Patch  21538567     : applied on Tue Nov 22 12:37:41 MSK 2016
Patch  21538558     : applied on Tue Nov 22 12:37:39 MSK 2016
Patch  21538485     : applied on Tue Nov 22 12:37:32 MSK 2016
Patch  21352646     : applied on Tue Nov 22 12:37:31 MSK 2016
Patch  21179898     : applied on Tue Nov 22 12:37:29 MSK 2016
Patch  21051862     : applied on Tue Nov 22 12:37:19 MSK 2016
Patch  21051858     : applied on Tue Nov 22 12:36:56 MSK 2016
Patch  21051852     : applied on Tue Nov 22 12:36:43 MSK 2016
Patch  21051840     : applied on Tue Nov 22 12:36:42 MSK 2016
Patch  21051833     : applied on Tue Nov 22 12:36:41 MSK 2016
Patch  20631274     : applied on Tue Nov 22 12:36:39 MSK 2016
Patch  20506715     : applied on Tue Nov 22 12:36:31 MSK 2016
Patch  20506699     : applied on Tue Nov 22 12:36:24 MSK 2016
Patch  20142975     : applied on Tue Nov 22 12:36:19 MSK 2016
Patch  19972569     : applied on Tue Nov 22 12:36:17 MSK 2016
Patch  19972568     : applied on Tue Nov 22 12:36:14 MSK 2016
Patch  19972566     : applied on Tue Nov 22 12:36:13 MSK 2016
Patch  19972564     : applied on Tue Nov 22 12:36:07 MSK 2016
Patch  19584068     : applied on Tue Nov 22 12:36:00 MSK 2016
Patch  19544839     : applied on Tue Nov 22 12:35:57 MSK 2016
Patch  19463893     : applied on Tue Nov 22 12:35:43 MSK 2016
Patch  18203838     : applied on Tue Nov 22 12:35:37 MSK 2016
Patch  18203837     : applied on Tue Nov 22 12:35:35 MSK 2016
Patch  18203835     : applied on Tue Nov 22 12:35:28 MSK 2016
Patch  17811447     : applied on Tue Nov 22 12:35:27 MSK 2016
Patch  17811438     : applied on Tue Nov 22 12:35:25 MSK 2016
Patch  17811429     : applied on Tue Nov 22 12:35:19 MSK 2016
Patch  19396455     : applied on Tue Nov 22 12:34:40 MSK 2016
```

The list of patches installed in the System will be displayed on the screen. Write down all numbers which go after "Patch" (or it can be the first eight 8 digits after **p**. For example, for **p19972569_112040_Linux-x86-64.zip** patch, the number is 19972569). These numbers are needed to compare installed patches with patches which are needed for the update.

d. Again, enter the command to call the file manager:
   `mc`
e. Go to the `/mnt/rhel-dvd/infowatch/extras/OraclePatches` directory and make sure that patch numbers in the directory are in the list of patches installed in the System (which you have written down).



Note:

If any patch from the `/mnt/rhel-dvd/infowatch/extras/OraclePatches` directory is not in the list of installed patches, you should install this patch.
Before installing the patch, OPatch utility is required to be updated. The following actions are to be taken to do that:

i. If *Midnight Commander* file manager is running, to exit it (is required for better control command execution) enter the command :
`exit`
ii. To make a backup copy, enter the command:
`mv /u01/app/oracle/product/db_1/OPatch /u01/app/oracle/product/db_1/OPatch_backup`
iii. To extract the archive with a new version, enter the command:
`unzip /mnt/rhel-dvd/infowatch/extras/OraclePatches/p6880880_112000_Linux-x86-64.zip -d /u01/app/oracle/product/db_1`
iv. To grant the oracle user rights for operating the directory and files, enter the command:
`chown oracle:oinstall -R /u01/app/oracle/product/db_1/OPatch`

To install the patch, the following actions are to be taken (below you can see the example of patch number 12345678 - p12345678_112040_Linux-x86-64.zip):

i. If *Midnight Commander* file manager is running, to exit it (is required for better control command execution) enter the command:
`exit`
ii. Enter the command to extract the patch:
`unzip /mnt/rhel-dvd/infowatch/extras/OraclePatches/p12345678_112040_Linux-x86-64.zip -d /tmp/`
iii. Enter the command to go to the required directory:
`cd /tmp/12345678/`
iv. In accordance with patch type, enter the command to install the patch :

- `/u01/app/oracle/product/db_1/OPatch/opatch napply . -silent -ocmrf /mnt/rhel-dvd/infowatch/extras/OraclePatches/ocm0.rsp` (in case of composite patch);
- `/u01/app/oracle/product/db_1/OPatch/opatch apply -silent -ocmrf /mnt/rhel-dvd/infowatch/extras/OraclePatches/ocm0.rsp` (in case of a single patch).

When the patch is installed, the screen will display the message:

```
OPatch completed with warnings.
Press any key to continue..._
```

Press any key to continue.
Then download the changed SQL file to the DB.

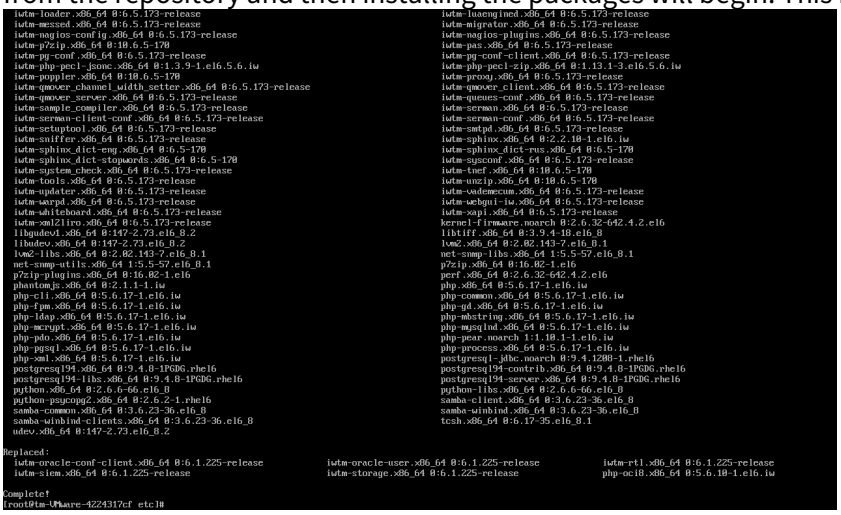
v. Enter the command to switch to `root` (superuser) again:
`exit`
vi. Enter the command to start Oracle DBMS:
`service oracle start`
vii. Enter the command to switch to the required user:
`su - oracle`
viii. In each separate base within the Oracle home, where the patch is installed it is required switching using SQL*Plus. Login as SYSDBA and run the script `catbundle.sql`, to do this the following command are to be entered:
```
cd $ORACLE_HOME/rdbms/admin
sqlplus /nolog
CONNECT / AS SYSDBA
@catbundle.sql cpu apply
QUIT
```
The `catbundle.sql` script running is displayed within the `dba_registry_history` as package set updates (PSU).
ix. To delete the files that are no more needed, enter the command:
`cd /tmp/ && rm -rf /tmp/12345678/ && rm -f /tmp/PatchSearch.xml`

Details on the installation can be found within the README file, located in a specific directory named after each patch.

f. if *Midnight Commander* file manager is running, enter the command to exit it (this is required for better control of command execution):
`exit`
g. Enter the command to switch to the *root* user:
`exit`
h. enter the command to start Oracle DBMS:
`service oracle start`

24. **Depending on the DBMS used**, enter the command to start the process of packages update:
    - `yum upgrade --exclude=iwtm-rtl-pg,iwtm-siem-pg` (if **Oracle DBMS** is used)
    - `yum upgrade --exclude=iwtm-rtl-oracle,iwtm-siem-oracle` (if **PostgreSQL DBMS** is used)
25. Before loading files required for installation, the screen will display a request like this
```
Total download size: 4.4 M
Is this ok [y/N]:
```
. To continue, type **Y** and press **Enter**.Downloading packages

from the repository and then installing the packages will begin. This may take some time.



26. Enter the command within the file manager to find and display the list of files with **.rpmnew** extension:
    ```
    find / -name "*rpmnew*" -print
    ```

> **Important!**
>
> When updating Traffic monitor from 6.0 or 6.1 version to 6.5 and later, the following actiona are to be obligatory taken:
> This page has not yet been translated to English.

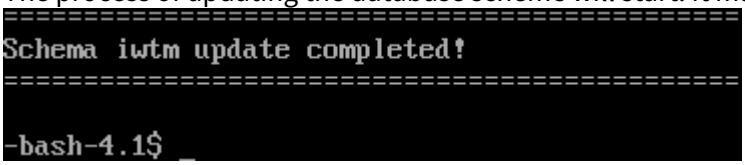
27. Enter the command to call the file manager:
    `mc`
28. Go to `/opt/iw/tm5/etc/scripts/` directory and make sure the file **iwssid.lua.upgrade** is in place. The file **iwssid.lua.upgrade** is not being used by the System, it is an information source to restore the System operation in case of complete customization.
29. Also `/opt/iw/tm5/etc/scripts/` directory should contain the file **iwssid.lua that** is recommended to remain with no changes implemented in case any term from the following is complied:
    - System's update is held as per version 6.9;
    - **iwssid.lua** file has not been edited before the update

    Otherwise, this should be correctly merged with iwssid.lua file (see "Merging configuration files").
30. **Depending on DBMS used**, go to the directory:
    - `/opt/iw/tm5/csw/oracle` (if **Oracle DBMS** is used);
    - `/opt/iw/tm5/csw/postgres` (if **PostgreSQL DBMS** is used).

31. Select the **database.conf** file.



32. Press **F3**.
33. Make sure that for the `\set schema_version` parameter, a version to which you are updating the System is specified. If an old version is specified, repeat steps 24 - 32.
34. Press **F3**.
35. To exit the file manager (is required to better control command execution), enter the command:
    `exit`
36. To stop services, enter the commands one by one:
    `service iwtm stop`
37. Make sure that there are no active users connected to the server via the management console.
38. If **PostgreSQL DBMS** is used in the System, Updating PostgreSQL DBMS should be performed.
39. **Depending on DBMS used**, enter the command to switch to the required user:
    - `su - oracle` - to switch to the *oracle* user (if **Oracle DBMS** is used in the System)
    - `su - postgres` - to switch to the *postgres* user (if **PostgreSQL DBMS** is used in the System)
40. **Depending on DBMS used**, enter the command to go to the required directory:
    - `cd /opt/iw/tm5/csw/oracle` - (if **Oracle DBMS** is used in the System)
    - `cd /opt/iw/tm5/csw/postgres` - (if **СУБД PostgreSQL DBMS** is used in the System)
41. Enter the command to start the database update script:
    `./update.sh`
    The process of updating the database scheme will start. It may take some time.



42. To switch back to the *root* user, enter the command:
    `exit`
43. Enter the command to open the file manager again:
    `mc`
44. Go to `/etc/yum.repos.d` directory and set the cursor on the file **rhel-dvd.repo** and press **F4**.
45. Make sure the `enabled` parameters of `[rhel-dvd]`, `[rhel-dvd-iwtm]` and [rhel-dvd-iwtm-cfdb] blocks are set to `0` values. Otherwise, replace the values from `1` to `0`.
46. Press **F2**.
47. In the opened window save the file, pressing **Save**.

48. Press **F10**.
49. Press **F3** and make sure the file is correct, then press **F3** again to close the file.
50. To leave the file manager (required of better commands execution) enter the command:
    `exit`
51. Check the performance of system internal services - see the description below.

STEP 3. HEALTCHECK OF THE SYSTEM INTERNAL SERVICES

Start the iw_bookworm, iw_licensed, iw_updater, and iw_kicker services on those servers, where they have been installed to and added into autorun, check their state .

Important!

If the service start has failed, check error messages in the log file of the service and contact our technical support: support@infowatch.com.

Or you can visit our website:

http://www.infowatch.com/support.

Log files to be checked:

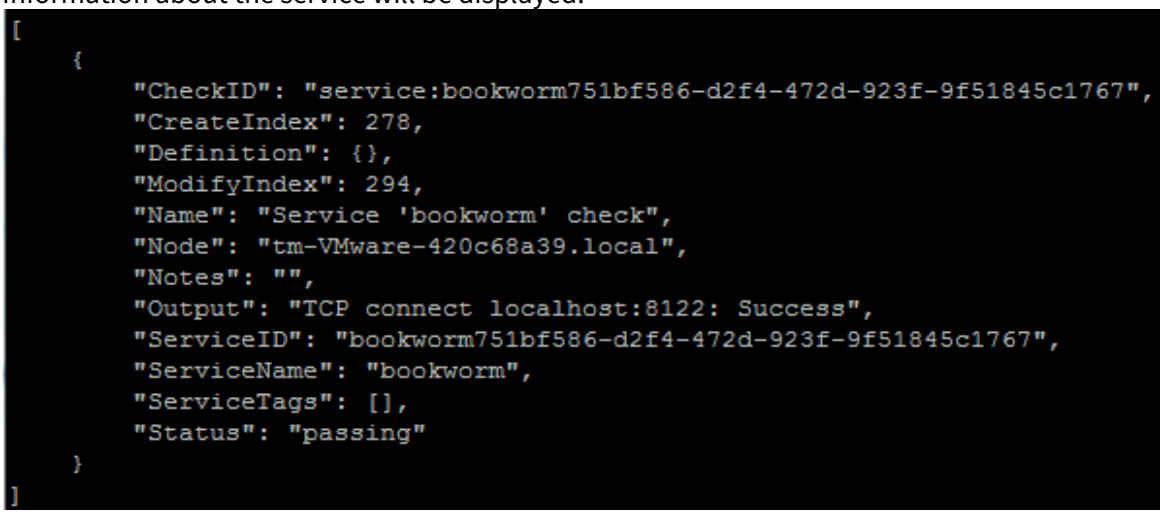
- /opt/iw/tm5/log/bookworm.log - for the iw_bookworm service
- /opt/iw/tm5/log/updater.log - for the iw_updater service
- /opt/iw/tm5/log/licserv.log - for the iw_licensed service
- /opt/iw/tm5/log/web-console-error.log - for the iw_kicker service

We recommend checking log files even if services have been started successfully: to make sure that there are no errors.
We recommend choosing the INFO or higher logging level for the check. If no errors have occurred, the log file can be missing.

To run the health check, take the following steps:

1. Enter the command to start the service:
   service iwtm start bookworm
2. Starting the service may take some time. To check the service state, run the following command:
   `curl -s http://localhost:8500/v1/health/checks/bookworm | python -mjson.tool`

Information about the service will be displayed:



3. Check values of the "Node" and "Status" blocks:
    a. The "Node" block should include the node name in the Consul cluster where the service is installed.
    b. The "Status" block should contain "passing".

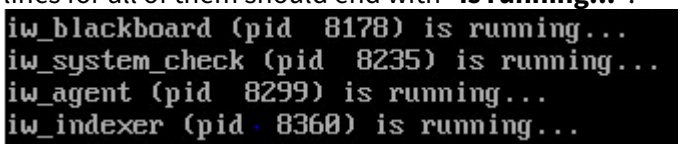
1. Run the following command to start the `iw_updater` service:
   `service iwtm  start update`
2. Starting the service may take some time. To check the `iw_updater` service state, see if the `/opt/iw/tm5/log/updater.log` file contains update errors.
   Make sure that the address in the command is correct and then run the following command:
   `grep -r 'error' /opt/iw/tm5/log/updater.log || echo "All good"`
   If there are no errors, the `All good` message will be displayed.
3. Run the following command to start the `iw_kicker` service:
   `service iwtm  start kicker`
4. Starting the service may take some time. To check the `iw_kicker` service state, see if theйл `/opt/iw/tm5/log/web-console-error.log` file contains update errors.
   Make sure that the address in the command is correct and then run the following command:
   `grep -r 'error' /opt/iw/tm5/log/web-console-error.log || echo "All good"`
   If there are no errors, the `All good` message will be displayed.
5. Run the following command to stop services:
   `service iwtm stop`
6. Complete the DBMS server update - see the description below.

STEP 4. COMPLETING UPDATE ON DBMS SERVER (TME DB Server)

To complete update on DBMS server (TME DB Server), take the following actions:

1. Enter the command to restart the server:
   reboot
2. Wait until the server is started and log in under *root* (STEP 1, actions **2** and **3** in this instruction).
3. Enter the command to check if the processes are started:
   service iwtm status
   The screen will display the list of processes and their status. The services are to be running and the

lines for all of them should end with "**is running...**":



4. Start all TM servers (TME Node Server) - see the description below.

STEP 5. RESTARTING TM SERVERS (TME Node Server)

To restart TM servers (TME Node Server), take the following actions on each of them:

1. On TM server, where web-gui package is installed (TME Node Server), enter the command to clear the cache:
   redis-cli flushall
2. Enter the command to open the file manager again:
   `mc`
3. Go to /etc/yum.repos.d directory, set the cursor on the file **rhel-dvd.repo** and press **F4**.
4. Make sure the enabled parameters of [rhel-dvd],[rhel-dvd-iwtm] and [rhel-dvd-iwtm-cfdb] blocks are set to 0 value. Otherwise, replace the values from 1 to 0.
5. Press **F2**.
6. In the opened window save the file, pressing **Save**.
7. Press **F10**.
8. Press **F3** and make sure the file is correct, then press **F3** again to close the file.
9. To leave the file manager (required of better commands execution) enter the command:
   exit
10. Enter the command to restart the server:
    `reboot`
11. Wait until the server is started and log in under *root* (STEP 1, actions **2** and **3** in this instruction).
12. Enter the command to check if the processes are started:
    service iwtm status
    The screen will display the list of processes and their status.
    Generally, iw_qmover_client, iw_qmover_server and iw_image2test_fre_batch services are stopped and all other services are started. For iw_qmover_client, iw_qmover_server and iw_image2test_fre_batch services the lines should end with "**is stopped (disabled)...**" and for all other services the lines should end with "**is running...**":



Note:

If the System contains the Crawler subsystem installed, it is required to start the services of this subsystem (on Crawler server). This is done on the server where the subsystem is installed with Windows standard tools: **Start** - **Control Panel** - **Administrative Tools** - **Services**, then select the service in the list and click **Start service** .

Updating Traffic Monitor servers of the distributed type is complete. Version of the System in the **About** window of the Management Console will be changed. If the System includes other servers or subsystems to be updated, follow instructions in this section.

Warning!

If automatic synchronizations with LDAP servers are configured in the System, then after update, perform synchronizations manually to guarantee load of entities (see "*Infowatch Traffic Monitor. User Guide*", "Running Synchronization with Server Manually").

Note:

For the Management Console to be displayed correctly, delete the cache in your browser before you start working in the Management Console. This is to be done with browser standard tools.

4.3 Updating Crawler Subsystem

To update the Crawler subsystem:

1. Delete the current version of Crawler as described in "Deleting the Crawler Subsystem".
2. Install the new version of Crawler as described in "Installing the Crawler Subsystem".

4.4 Updating InfoWatch Device Monitor

If you have InfoWatch Device Monitor installed, you can update it to a later version.

System update is similar to its installation:

1. Updating InfoWatch Device Monitor Server End (database, server, and Management Console).

   Important!

   If it is required to update IW Device Monitor to version 6.10 this should be done in sequence - first you should update to intermediate version. For example, updating Device Monitor 6.7 up to 6.9 version, first update to 6.9 and only after this you can update Device Monitor to 6.10 version.
   If you want to update System version 3.4 - 4.0, delete the old server version (don't remove the database) and re-install the server, configuring the connection to existing database.
   Starting version 4.0, updates use the standard procedure.
   When updating Device Monitor version 6.0 by deleting and then installing the Server, you must perform the following actions to let Device Monitor Agents to connect to the new Server:
   1. When deleting - save encryption key stored in DM Server installation folder, `SSLServerKey.pfx` file.
   2. When installing - specify the path to the saved encryption key used on the old Server.

2. Updating InfoWatch Device Monitor Agent.
   Device Monitor supports earlier Agent versions starting build 3.4.875. Therefore, Agent is updated when needed.

   Important!

   Device Monitor Agents should be updated after the Device Monitor Server and Traffic Monitor Server have been updated.

4.4.1 Updating InfoWatch Device Monitor Server End

Important!

If you want to update Device Monitor version **3.4** - **4.0**, delete the old server version (don't remove the database) and re-install the server, configuring the connection to existing database.

Starting from version **4.0**, the update is fulfilled without deletion of previous version.

When updating the System version **6.0** by deleting and then installing the Server, you must perform the following actions to let Device Monitor Agents to connect to the new Server:

1. When deleting - save encryption key stored in DM Server installation folder, `SSLServerKey.pfx` file.
2. When installing - specify the path to the saved encryption key used on the old Server.

Step 1. Start update

Important!

When several servers are used, the main server shall be updated first. All the secondary servers shall be turned off at the same time. All the servers are to be updated in turn after the main one.

Open the folder where Device Monitor distribution kit is kept. Then open Server directory. Run platform-specific setup file from this directory.

You will be redirected to InfoWatch Device Monitor Installation Wizard welcome screen. Click **Next** to go to the next installation screen.

Step 2. Accepting the License Agreement

Read the End User License Agreement. If you accept the licensing terms, select **I accept the terms** in **the License Agreement** and click **Next**.

Step 3. Database configuration

Database is preserved during the update, and **Configure Database Connection** box automatically displays old database parameters. However, depending on DBMS, you need to specify particular settings.

Built-in Database Update

Skip this step if you are using built-in DB.

Update Database Under Microsoft SQL Server DBMS

On **Authentication Method** panel, select authentication method for the user, who updates the database. For this option, specify the authentication method selected during account preparation (see "Database deployment under Microsoft SQL Server DBMS").

If the account uses Windows authentication, select **Windows authentication**.

If the account uses built-in SQL Server authentication, select **SQL Server built-in**. Then enter login and password into **User name** and **Password** fields respectively.

Note:

You can specify old or new authentication parameters as the update proceeds. For guidelines on authentication methods and account preparation see section "Database deployment under Microsoft SQL Server DBMS".

Update Database Under Oracle DBMS

On **DB Server** panel, specify **Password for 'SYSTEM'** - password for SYSTEM account that manages the database, which is being updated.

On **Scheme Information** panel, fill in **Password**, **Confirm password** fields - password for database scheme owner's account used for database update.

Update PostgreSQL Database

Enter the password of the account that manages the updated database into **Password** field.

After you have configured all parameters, click **Next**.

Step 4. update Completion

Go to the next screen and click **Install** to run System server update.

Follow Setup Wizard's instructions to complete System server update.

Note:

While updating Device Monitor server the filters conversion cannot be supported.

4.4.2 Updating InfoWatch Device Monitor Agent

The system supports agent versions starting from build 3.4.875. Therefore, updated system components can work with older agent versions. However, you can update to a later version.

Agent update is similar to its installation:

- local update using Setup Wizard;
- remote update using software distribution tools;
- centralized update via Management Console (for details, see "*InfoWatch Traffic Monitor. User Guide*", "Agent Remote Installation, Updating and Uninstallation" article).

To successfully install or update InfoWatch Device Monitor Agent, follow the directions as per InfoWatch Device Monitor Agent Installation.

In case you need to update Device Monitor Agent on a large number of Workstations, you need to take the following steps:

1. Update agent on a group of 10 Workstations. Make sure that there are no performance errors for 2-3 days.
2. Update agent on a group of 50 Workstations. Make sure that there are no performance errors for 2-3 days.
3. Update agent on a group of 500 Workstations. Make sure that there are no performance errors for 2-3 days.
4. Update agent on a group of 1000 Workstations. Make sure that there are no performance errors for 2-3 days.

5. Complete the update procedure with the rest of the Workstations.

> **Note:**
>
> When updating the agent on Windows 7 OS or Windows 2008 R2 Server it is recommended to consider the following point:
>
> If Corporate network control component was installed before, it will be removed during update. If needed, the component can be installed manually using the command line.

4.5 Merging Configuration Files

During the update of Traffic Monitor server nconfiguration files (e.g, with **.conf**, **.cfg**, and **.lua** extensions) that were modified when using the previous version, cannot be overwritten with the new files. The new files are created in the same directories and with the same names, but with **.rpmnew** extension respectively.This is done to support the ability to change the structure of new file versions. For correct operation of the System it is required merging files of an old and a new version.

Use any files merging type specified below.

4.5.1 Merging configuration files in Midnight Commander

Let's consider an example to merge **postgresql.conf** and **postgresql.conf.rpmnew** files.

> **Tip**
>
> To view the file content, press **F3**. For editing, press **F4**.

The **postgresql.conf** file looks like:

```
{
    "DB": "postgres",
    "Host": "localhost",
    "Password": "xxXX1234",
    "Port": 5433,
    "Username": "iwtm_linux"
}
```

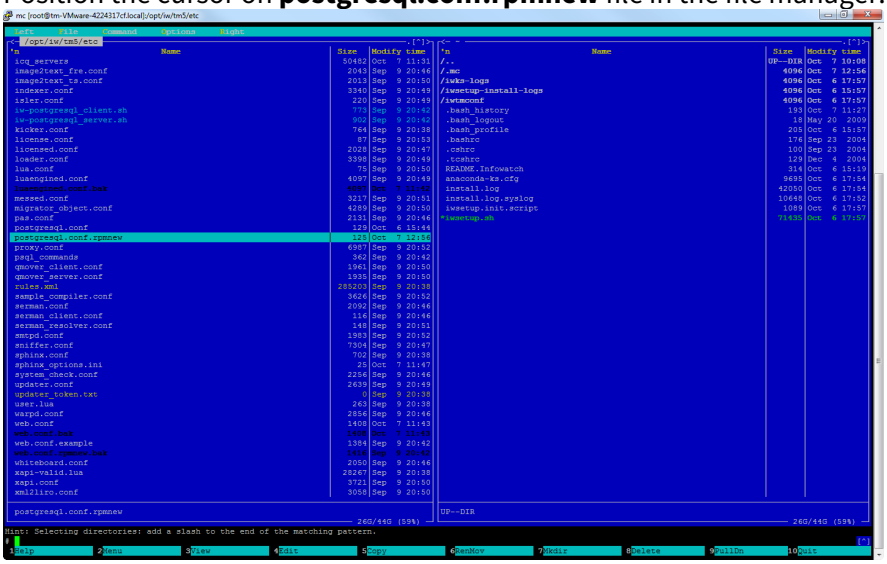
The **postgresql.conf.rpmnew** file looks like:

```
{
    "DB": "put postgresql database name here",
    "Password": "put postgresql password here",
    "Username": "put postgresql username here",
    "Port": 5432,
    "Host": "put postgresql host address here"
}
```

To merge these files, you need to copy data from sections of the **postgresql.conf** file to the corresponding sections of the **postgresql.conf.rpmnew** file. For this:

1. Go to `/opt/iw/tm5/etc` directory.

2. Position the cursor on **postgresql.conf.rpmnew** file in the file manager.



3. Press **F4**.
4. Replace the values in the file sections with the values from correspondings sections of the **postgresql.conf** file. The result looks like this:

```
{
    "DB": "postgres",
    "Password": "xxXX1234",
    "Username": "iwtm_linux",
    "Port": 5433,
    "Host": "localhost"
}
```

> **Note:**
>
> For the distributed installation type, the value of the "Host" field will be an IP address of the server where the DBMS is installed. For example, `"Host": "10.60.23.6",`

5. Press **F2**.
6. In the window that opens, confirm the file saving by clicking **Save**.
7. Press **F10**.
8. Position the cursor on the **postgresql.conf** file in the file manager.
9. Press **F8** to delete the **postgresql.conf** file.
10. In the window that opens, confirm the deletion by clicking **Yes**.
11. Select the **postgresql.conf.rpmnew** file in the file manager.
12. Press **F6**.
13. In the **to** field, enter `/opt/iw/tm5/etc/postgresql.conf` and press **Enter**.
    Now the System has only one PostgreSQL configuration file, which is **postgresql.conf**. It has a

structure of the new version and the required content:



4.5.2 Merging configuration files by means of vimdiff

To work with vimdiff the editor Vim should be installed on a server.

Let's consider an example of merging **user.lua** and **user.lua.rpmnew** files. After the update, the **user.lua. rpmnew** file appears (if the original **user.lua** file has been changed). You should copy all earlier specified values of parameters and settings from **user.lua** to **user.lua.rpmnew**. To do this:

1. Go to `/opt/iw/tm5/etc/scripts` directory.
2. In the command line, enter:
   `vimdiff user.lua.rpmnew user.lua`
3. Go into edit mode (**Insert** key).
4. If parameter values are different, copy the values from **user.lua** to **user.lua.rpmnew** manually.
5. Exitthe edit mode (**Esc** key).
6. Save the changes within **user.lua.rpmnew** and exit the editor (input **:wq**)
7. Close the file **user.lua** as moot (input **:q**).
8. Rename **user.lua.rpmnew** to **user.lua**.

Important!

To avoid data loss and System errors (Traffic Monitor server part configuration files) it is required following the instructions.

In case of any trouble while merging the configuration files you are recommended contacting InfoWatch service desk via support@infowatch.com.

Service desk is available from 7 AM till 9 PM Moscow time, from Monday to Friday, except weekends and public holidays.

You can also find the required info on www.infowatch.com/support.

Important!

To avoid System's improper operation you should avoid merging the following files with the files from older versions:

1. /etc/rc.d/init.d/postgresql-9.6.rpmnew
2. /etc/sgml/docbook/xmlcatalog.rpmnew

4.6 Updating PostgreSQL DBMS

Updating PostgreSQL DBMS from version **9.4** to version **9.6** is performed in the console of the server which you update.

The update process can be performed in two modes:

- BACKUP - in this mode entire DB is being copied, including all the IWTM DB scheme tablespaces. In BACKUP mode, it is recommended to store files on the following devices only:
  - External disk having file systems Ext4, XFS;
  - Remote block device connected via protocols iSCSI, NFS;
  - Block device connected locally, having file systems Ext4, XFS.

  The disk, where IWTM DB scheme tablespaces are located should contain as much free space as they have already taken;

- LINK - in this mode DB files are not being copied and the hard links are created from new folders instead of long-time DB. Once the new version is installed and launched, the old one doesn't operate. That's why before updating the DB in the LINK mode it is required totally backing up the previous DB including all the tablespaces. In this mode you may require up to 100 Mb free space.

Note:

If you connect remotely via SSH, it is recommended using the Screen utility. Thus you can avoid problems in case of lost connection with updating server. When disconnecting from the utility, all the prcocesses started are not to be interrupted and you may safely continue the System update.

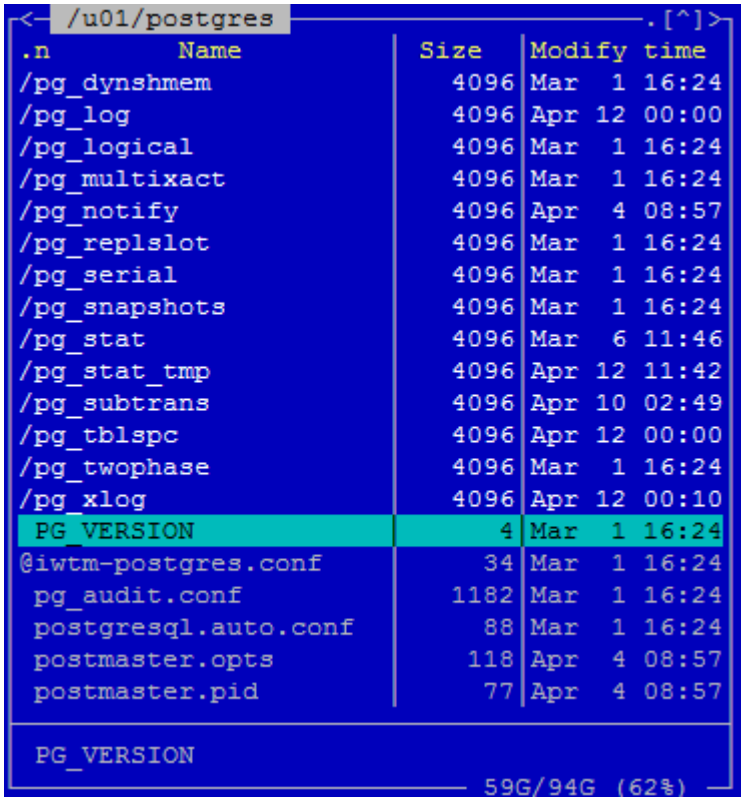
Important! Using Screen is highly recommended when working with DB and updating DBMS.

Basic commands:

- `screen` - start the utility;
- `Ctrl+a d` - disconnect from screen (to be input within the screen window);
- `screen -ls` - display the list of screen running;
- `screen -r` - connect to screen again;
- `screen -r name` - connect to specific screen with «name»;
- `exit` - exit screen (to be input within the screen window).

4.6.1 Prepare for update

1. Back up DB.
2. Before updating the DBMS, Traffic Monitor packages are required updating up to actual version, new version PostgreSQL packages are to be installed along with it.
3. To successfully update PostgreSQL DBMS to version **9.6**, version **9.4** must be installed in the System. Check the version of DBMS installed. For this purpose:
   a. Enter the command to open the file manager:
   `mc`
   b. Go to /u01/postgres directory
   c. Select the file **`PG_VERSION`**, where the current DBMS version is specified and press **F3** to view

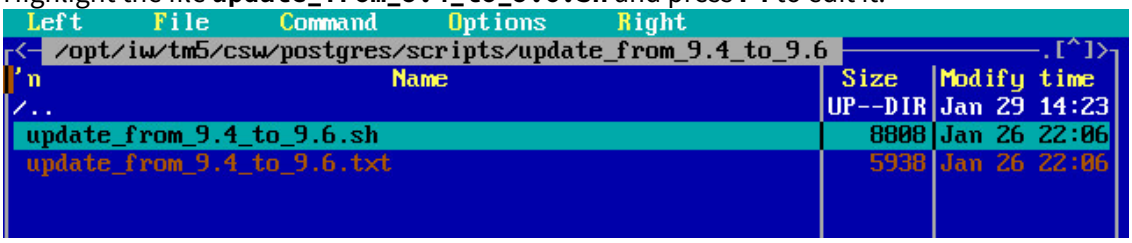


the content:

d. Press **F3** to close the file.

If version **9.6** is already installed in the System, then do not run DBMS update and follow the instruction on updating the System.

4. Set up the update script. For this purpose:
   a. Go to `/opt/iw/tm5/csw/postgres/scripts/update_from_9.4_to_9.6` directory.
   b. Highlight the file **`update_from_9.4_to_9.6.sh`** and press **F4** to edit it.



   c. Depending on the mode you've selected replace the value of `UPDATEMODE` parameter with `BACKUP` or `LINK` (by default - `BACKUP`).
   d. Set the value of `PARALLEL_DEGREE` parameter equal to the number of DB server CPU cores (by default - `8`). This parameter influences the update processing speed.
   e. Press **F2**.
   f. In the opened window ensure saving the file by clicking **Save**.
   g. Press **F10**.
   h. Press **F3** and make sure the file is correct, then press **F3** again to close the file.
   i. Enter the command to close file manager:
   ```
   exit
   ```

5. Before updating the DBMS all Traffic Monitor services should be stopped. Enter the commands for this purpose:
   a. For Traffic Monitor All-in-one installation:
   ```
   service iwtm stop
   ```

```
service iwtm-php-fpm stop
service nagios stop
```

b. For Traffic Monitor distributed installation:

i. On Traffic Monitor server:

```
service iwtm stop
service iwtm-php-fpm stop
service nagios stop
```

ii. On DB server:

```
service iwtm stop
```

4.6.2 Update

1. Enter the command to go to the required directory:
   `cd /opt/iw/tm5/csw/postgres/scripts/update_from_9.4_to_9.6`
2. Set up the update script. For this purpose enter the command:
   `bash ./update_from_9.4_to_9.6.sh`

   Once the update is over, the following message will be displayed: `Update completed.`
3. After the update process is over, connect to DB and check its working capacity:
   a. To connect to DB server from console, enter the command:
   ```
   su - iwtm
   psql postgres iwtm -p 5433
   ```
   b. Enter the commands:
   ```
   select version();
   select* from version;
   explain (analyze, buffers) select * from object_comment;
   ```
   The commands have to be executed with no mistakes.
   c. To exit enter the command:
   `\q`
   d. Enter the command:
   `exit`

   > **Note:**
   >
   > Also, this check can be performed on Windows managed computers. pgAdmin should be used for this purpose.
   > The check is to be performed using the same commands (step b).

4. Follow the System updates instructions.

4.6.3 Old DB backup removal

If BACKUP update mode is used, the System creates an old DB backup.

Note:

Before removing the new version, working capacity should be checked: make sure the events are loaded into DB and the events search is active. Few days are required for this purpose.

Removing is to be performed within the DB server console. To remove old DB backup, enter the command:

1. Enter the command to go to the required directory:
   `cd /var/log/infowatch/update/postgres96_update_`**`date`**
   where **`date`** - update date.
   Example:
   `cd /var/log/infowatch/update/postgres96_update_2018-01-29_15:37:06`
2. Set up the removal script. For this purpose enter the command:
   `bash ./delete_old_cluster.sh`
3. Removal process cannot be displayed within the console and is successful in case there is no error message.

Important!

Once backup is removed, back to remain is impossible.

4.6.4 Update rollback

Note:

DBMS update rollback is used only in case of repeated update, once the error occured.

The update rollback is possible, when:

- The update was performed in BACKUP mode;
- Before the update backup was manually created in LINK mode.

The update rollback is to be performed within the DB console. To rollback the update it is required:

- If the update was performed in BACKUP mode:
  a. Enter the command to go to the required directory:
     `cd /opt/iw/tm5/csw/postgres/scripts/update_from_9.4_to_9.6`
  b. To run the update rollback script, enter the command:
     `bash ./update_from_9.4_to_9.6.sh rollback`
- If the update was performed in LINK mode:
  a. To stop `postgresql` and `pgagent` services of old and new versions, enter the commands:
     ```
     service pgagent-9.4 stop
     service pgagent-9.6 stop
     service postgresql-9.4 stop
     service postgresql-9.6 stop
     ```

b. Replace the updated files and DB directories with the ones that were created as the reserved copies.
c. To start `postgresql` and `pgagent` services of old version, enter the commands:
```
service pgagent-9.4 start
service postgresql-9.4 start
```

4.6.5 Error alert

If an error occurs, the logs should be collected and sent to Service Desk.

If an error occurred:

- During the update or when the update services were started:
  a. Logs from the update folder.
  Example: `/var/log/infowatch/update/postgres96_update_2018-01-29_15:37:06`
  b. All the logs from folders `/u01/postgres*/pg_log`.
- During the update rollback:
  a. File named `rollback.log` from updates lost folder.
  Example: `/var/log/infowatch/update/postgres96_update_2018-01-29_15:37:06`
  b. All the logs from folders `u01/postgres*/pg_log`.

5 Uninstalling the System

The System uninstalling implies the deletion of all packages of the System as well as removal of a used database scheme. To completely delete the operating system and the DBMS you, for example, can execute formatting of used partitions by standard tools.

- See details on DB schema removal (Oracle as well as PostrgreSQL) in "Deleting the Database Scheme".
- See details on Device Monitor removal (Server and Clients) in "Uninstalling Device Monitor".
- The Crawler subsystem (server as well as scanner) can be removed by standard OS Windows tools: **Start -> Control panel -> Programs and components**, a **Delete** command.
- To delete a certain package, execute a command:
  `rpm -e package_name`
- All Traffic Monitor server components (Management console, Sniffer, IW ICAP, remote database interaction module, and the others) can be deleted using the following command:
  `yum remove `rpm -qa | grep iwtm``

After the InfoWatch Traffic Monitor Server removal completion please return the external infrastructure set to Traffic Monitor to original state:

- if there was an integration with a mail relay server – please make sure the Postfix settings are set to the original state;
- if the System performed interception and filtering of SMTP traffic – please configure the SMTP mail delivery through a corporate mail server, bypassing the InfoWatch Traffic Monitor server.

After removal, the following entities are left on the computer:

- the operating system;
- configuration files where changes were made (**.rpmsave** suffix is being assigned to the changed files - for example, **detector.conf.rpmsave**; files that was not changed will be deleted);
- objects queue (see details on deletion of files from the OS temporary directory and data from IW Traffic Monitor file queue directories in «*InfoWatch Traffic Monitor. Administrator Guide*», "*Deleting Temporary Files*" article);
- categories and terms;
- license file;
- account of a user which is a IW Traffic Monitor owner and the group to which this user belongs.

5.1 Deleting the Database Scheme

This instruction is relevant for the Oracle Database and PostrgreSQL.

> **Important!**
>
> Do not delete the database scheme from which the daily tablespaces were distracted for archiving.Otherwise, you will not be able to restore data from these tablespaces.

1. **Checking the Oracle DBMS**
   Make sure that:
   - the version of the installed database scheme corresponds to a version of a software package used for its removal;
   - the DBMS server is running;

- in configuration file **database.conf** the name and the password of an account having SYSDBA permissions are specified correctly (values of parameters `sysdba` and `sysdba_password`).

2. **Stopping TrafficMonitor**
   a. Stop all TM server processes:
      `service iwtm stop`
   b. Close all copies of the Management console;
   c. Stop the service:
      `service iwtm-php-fpm stop`
   d. Stop all the connections with a database scheme executed from other programs.
3. **Starting the schema removing**
   a. Go to directory
      `/opt/iw/tm5/csw/oracle` or `/opt/iw/tm5/csw/postgres`
   b. Run script:
      ./uninstall.sh

Important!

When deleting the database scheme, the following components are also deleted from the System:

- policies, including preinstalled ones (see "*Infowatch Traffic Monitor. User guide*", "Preinstalled Policies" article);
- queries and reports (see *Infowatch Traffic Monitor. User guide*", "Queries" and "Reports" sections);
- plugins and tokens (see "*Infowatch Traffic Monitor. User guide*", "Plugins" article).

To restore Device Monitor plugin, preinstalled queries, reports and to redeploy preinstalled policies after the deletion, the following actions are to be taken:

1. Create **/opt/iw/tm5/www/backend/protected/runtime/first_run** file on behalf of **iwtm** user;
2. Restart **iw_kicker** process:
   `service iwtm restart kicker`

Then you need to manually add other plugins (see "*Infowatch Traffic Monitor. Administration guide*", "Adding plugin" article) and create required policies (see "*Infowatch Traffic Monitor. User guide*", "Creating Data Protection Policy" and "Creating Person Control Policy" articles).

5.2 Deleting Crawler Subsystem

Crawler subsystem (both **Server** and **Scanner**) can be deleted using standard Windows tools: **Start -> Control Panel -> Programs and components**, the **Delete** command.

5.3 Uninstalling Device Monitor

Important!

If you are planning to install Device Monitor Server again, then to make Device Monitor Agents could connect and bind to the new server, then starting from version 6.0 you must save the encryption key of the old server.

The encryption key is stored in the installation folder of the InfoWatch Device Monitor Server, `SSLServerKey.pfx` file.

To remove InfoWatch Device Monitor server end with Management Console:

1. Take one of the following steps:
   - Open `Setup\Unified` catalogue on the Installation CD. Run platform-specific setup file from this directory.
   - Run **Uninstall or remove programs** from Windows Control Panel, select **InfoWatch Device Monitor** and click **Change**.
2. On **Change, repair or remove…** screen select **Remove**.
3. To remove the system and its database, flag **Remove database** on **Remove database…** screen. Then specify parameters for uninstalling: parameters depend on your DBMS:
   - **Microsoft SQL Server** – specify your authentication method by selecting it in Authentication Method pane (see "Database deployment managed by Microsoft SQL Server DBMS").
     In case of SQL-server based authentication (**Integrated into SQL Server**) enter the credentials you used to connect to the database in **Login** and **Password** boxes of **Database Administrator** pane.
   - **Oracle** – enter the password into **The password of 'SYSTEM' login** box. This will remove database schema owner account and all its objects except the tablespace.
   - **PostgreSQL** –enter the credentials used to create the DB during server setup into User name and Password boxes (see "InfoWatch Device Monitor Server End Installation Procedure").
4. **Important!**

   If the database is not working or working partially, then to delete the InfoWatch Device Monitor you should uncheck the **Remove database** field, otherwise, the deletion can be performed incompletely.
5. After specifying the parameters click **Next** and then click **Remove** to start uninstallation.

To remove only InfoWatch Device Monitor server end or Management Console:

1. Run **Add or remove programs** and click **Change**.
2. In **Custom Setup** click  to the left of the elements you want to remove and select **Disable this element**. Click **Next**.
3. If you selected server uninstallation at the previous step, specify whether you want to remove the database and enter the authorized account parameters, if necessary, on **Remove database…** screen (see details above).

4. Click **Change** to start uninstallation.

To remove InfoWatch Device Monitor Agent:

run **Add or remove programs**, select **InfoWatch Device Monitor Agent** and click **Remove**.

You can also use centralized uninstallation to remove Agents:

- with Active Directory tools (if Agents were installed via software distribution tools) as described in "Remove Agent Installed via Software Distribution Tools".
- with Management Console distribution tasks (for details, see "*InfoWatch Traffic Monitor. Administration Guide*", "Agents Remote Setup, Updating and Uninstallation" section).

> **Important!**
>
> Turning off the computer during the installation/uninstallation process may lead to unstable operation of OS.

The order of deleting the Agents from mobile devices is described in "*InfoWatch Traffic Monitor. Administration Guide*", "Deleting the Mobile Device" article.

5.3.1 Remove Agent Installed via Software Distribution Tools

If the agent was installed via software distribution tools, you can use them to remove it.

For example, if Agents were installed via Microsoft Active Directory, the corporate network administrator can use group policy to remove the installation task. Group policy editing procedure is described in "Agent Installation via Software Distribution Tools", step 3.

To remove Agent from all managed workstations:

1. Select the installation task you want to remove. Then right-click the selected row and select **All tasks** > **Remove**.
2. Select **Remove software** in **Immediately uninstall software from users and computers** dialog.

   > **Note:**
   >
   > Other options remove installation task without uninstalling all existing Agents. After that, you won't be able to remove these Agents with Microsoft Active Directory tools.

3. Click **OK**.

The Agent will be removed from all computers under selected group policy.

6 Appendix A. Username and Password Recommendations

Requirements for usernames

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

Requirements for passwords

- The user password should be 8-128 characters long.
- The user password may cinclude the characters in accordance with any three conditions from the follwing four:
- Capital letters in Latin characters (A-Z)
- Lowercase letters in Latin characters (a-z)
- Arabic numerals (0-9)
- Characters: «#», «$», «!» or «%»
- The user password should not contain username or a part of username.
- The password is case-sensitive.

Recommendations for strong passwords

- Recommended password length is 10-30 characters.
- The password must contain letters, digits, and characters.
- It is not advised to:
    - Include whole words or phrases into a password.
    - Use a series of the same character.
    - Start and end the password with the same character.
    - Create a new password by adding characters to your current password.

General recommendations

It is not recommended beginning a username or password with combinations: SYS_ and ORA_.
It is not recommended using Oracle reserved words in usernames or passwords:

ACCESS	EXCLUSIVE	MODE	SELECT
ADD	EXISTS	MODIFY	SESSION
ALL	FILE	NOAUDIT	SET
ALTER	FLOAT	NOCOMPRESS	SHARE
AND	FOR	NOT	SIZE
ANY	FROM	NOWAIT	SMALLINT
AS	GRANT	NULL	START
ASC	GROUP	NUMBER	SUCCESSFUL
AUDITBETWEEN	HAVING	OF	SYNONYM

BY	IDENTIFIED	OFFLINE	SYSDATE
CHAR	IMMEDIATE	ON	TABLE
CHECK	IN	ONLINE	THEN
CLUSTER	INCREMENT	OPTION	TO
COLUMN	INDEX	OR	TRIGGER
COMMENT	INITIAL	ORDER	UID
COMPRESS	INSERT	PCTFREE	UNION
CONNECT	INTEGER	PRIOR	UNIQUE
CREATE	INTERSECT	PRIVILEGES	UPDATE
CURRENT	INTO	PUBLIC	USER
DATE	IS	RAW	VALIDATE
DECIMAL	LEVEL	RENAME	VALUES
DEFAULT	LIKE	RESOURCE	VARCHAR
DELETE	LOCK	REVOKE	VARCHAR2
DESC	LONG	ROW	VIEW
DISTINCT	MAXEXTENTS	ROWID	WHENEVER
DROP	MINUS	ROWNUM	WHERE
ELSE	MLSLABEL	ROWS	WITH

7 Appendix B. Licenses for Third-Party Technologies

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 uses 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 (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