

INFOWATCH

InfoWatch Traffic Monitor 6.11

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
2.3 Operating System and Network Server Configuration Requirements 13
3 Installing the System 14
3.1 Installing Traffic Monitor Server and Database 15
3.1.1 General Information on Installation Steps for Server Components 15
3.1.1.1 Configuring Time Synchronization (NTP-server) 15
3.1.1.2 Localization Setup 16
3.1.1.3 Configuring the Automatic Event Deletion from the Database 18
3.1.1.4 Completing the Installation 20
3.1.2 All-in-one Installation Mode of TM Enterprise and TM Standard 21
3.1.3 Distributed Installation of TM Enterprise 27
3.1.3.1 Installing Database 27
3.1.3.2 Installing Traffic Monitor Server 32
3.2 Installing Crawler Subsystem 35
3.3 Installing InfoWatch Device Monitor 41
3.3.1 InfoWatch Device Monitor Server End Setup 42
3.3.1.1 Database Deployment Managed by Microsoft SQL Server DBMS 42
3.3.1.2 Database deployment managed by Oracle DBMS 43
3.3.1.3 Database deployment managed by PostgreSQL DBMS 44
3.3.1.4 Server Setup Recommendations 44
3.3.1.5 InfoWatch Device Monitor Server End Installation Procedure 45
3.3.2 InfoWatch Device Monitor Agent Installation 54
3.3.2.1 Standard Agent Installation 56
3.3.2.2 Agent Installation via Software Distribution Tools 57
3.3.3 Deployment Scheme for InfoWatch Device Monitor 59
3.4 Pre-installed Server Parameters 62
4 Updating the System 64
4.1 Updating TM All-in-one Enterprise and Standard 67

4.2 Updating TM in case of Distributed Installation 94
4.3 Updating Crawler Subsystem 130
4.4 Updating InfoWatch Device Monitor 130
4.4.1 Updating InfoWatch Device Monitor Server End 131
4.4.2 Updating InfoWatch Device Monitor Agent 132
4.5 Merging Configuration Files 133
4.5.1 Merging configuration files in Midnight Commander 133
4.5.2 Merging configuration files by means of vimdiff 135
4.6 Updating PostgreSQL DBMS 136
4.6.1 Prepare for update 137
4.6.2 Update 138
4.6.3 Old DB backup removal 139
4.6.4 Update rollback 140
4.6.5 Error alert 140
5 Uninstalling the System 141
5.1 Deleting the Database Scheme 141
5.2 Deleting Crawler Subsystem 142
5.3 Uninstalling Device Monitor 142
5.3.1 Remove Agent Installed via Software Distribution Tools 144
5.4 Uninstalling Traffic Monitor 144
6 Appendix A. Username and Password Recommendations 146
7 Appendix B. Licenses for Third-Party Technologies 148

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
- Operating System and Network Server Configuration 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 workstations of a company. See the 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, the 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. See the requirements 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 or Mozilla Firefox browser of actual version.

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

- OCR is disabled for all interceptors;
- the 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 or Crawler you need to dedicate a separate servers for **iw_xapi_xapi** processes.

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 7.x (the latest version) with subscription, required for update	The server should have a network interface with the assigned IP address. Requirements imposed by the interceptors should be fulfilled*
TM Enterprise server, less than 10 GB per 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 7.x (the latest version) with subscription, required for update	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 per day to 50 GB per day				
RAID-array with fault tolerance	2SRVx2 CPU 10xC	32-48 GB for each server	OS Red Hat Enterprise Linux 7.x (the latest version) with subscription, required for update	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 per day				
RAID-array with fault tolerance	Calculated on demand	From 32GB for each server	OS Red Hat Enterprise Linux 7.x (the latest version) with subscription, required for update	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*
Oracle DB or PostgreSQL server (Provides storage for traffic of 1-2 thousand users by 3 months; in case OCR and Device Monitor are used, the requirements are to be calculated on demand)				

Disk subsystem	Processor	RAM	Software	Additional requirements
RAID-array with fault tolerance: 500 GB To store logs (redo log for Oracle, xlog for PostgreSQL) it is required to provide u01 directory with additional space equal to RAM of DBMS server. In case RAM is lower than 20 Gb, 20 Gb shoud be provided for logs storage.	2CPU от 6xC, 2,6 GHz	16GB and more depending on data volume, insertion and processing speed	ОS Red Hat Enterprise Linux 7.x (the latest version) with subscription, required for update	
Crawler server and scanner				
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 R2. Platform: • Microsoft .Net Framework 4.5.1.	• **iw_xapi_xapi** process autorun should be enabled on the TM server • 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.

Disk subsystem	Processor	RAM	Software	Additional requirements
Device Monitor server				
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 12. If you install Device Monitor on x64 server OS, using x64 Oracle Client application is required; • Microsoft SQL Server 2005, 2008, 2012, 2014, 2016 (Standard, Enterprise); • PostgreSQL version 9.	▪ 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 ▪ TLS 1.2 should be supported
Device Monitor Agent for workstations				

Disk subsystem	Processor	RAM	Software	Additional requirements
Not less than 1 GB free space required for installation/ Also the free space is required for files temporary storage, which are to be sent for analysis.	From 2 cores	From 2,5 GB	OS: • [1] Microsoft Windows Vista Service Pack 2; • [2]Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 и 8.1; • Microsoft Windows 10; • [2]Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Astra Linux Special Edition "Smolensk" 1.6.	• Local DNS is required to convert domain names into addresses • TLS 1.2 should be supported
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 6.11.2.

[2] - starting from version 6.11.2 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 6.11.3 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 and7.15LTSR virtualisation environment.

* 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.

2.3 Operating System and Network Server Configuration Requirements

To install successfully the System, the server should meet with the following requirements:

- Have an OS installed OS Red Hat Enterprise Linux 7.x (last version);
- OS repositories should be configured to install the packages`redhat-lsb-core` и `lshw`.
  See how to configure a local repository on the Red Hat Enterprise Linux official website;
- Minimum Swap space is 500 Mb (for recommendations, see "Recommendations to Partition Server Disk Space during Installation in Different Modes.").
  You may see the information on Swap space by entering the command:
  `swapon -s`
  How to configure the swap space you may read on the Red Hat Enterprise Linux official website;
- Mount points options should not contain `nosuid` and `noxattr` command options (you can check this when opening the file `/etc/fstab`);
- The server settings should be done correctly as follows (if you have network problems, please contact your system administrator):
  - External DNS server should resolve your hostname into IP address which is specified on one of server network interfaces;
  - IP address should belong to the range of private IP addresses:
    10.0.0.0 — 10.255.255.255 (RFC1918);
    172.16.0.0 — 172.31.255.255 (RFC1918);
    192.168.0.0 — 192.168.255.255 (RFC1918).
  - The following command should be run:
    `ping -c 1 <hostname>`
    where `<hostname>` is your hostname.
    As a result of running command the package is successfully installed.

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 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 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 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 the installation of 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:

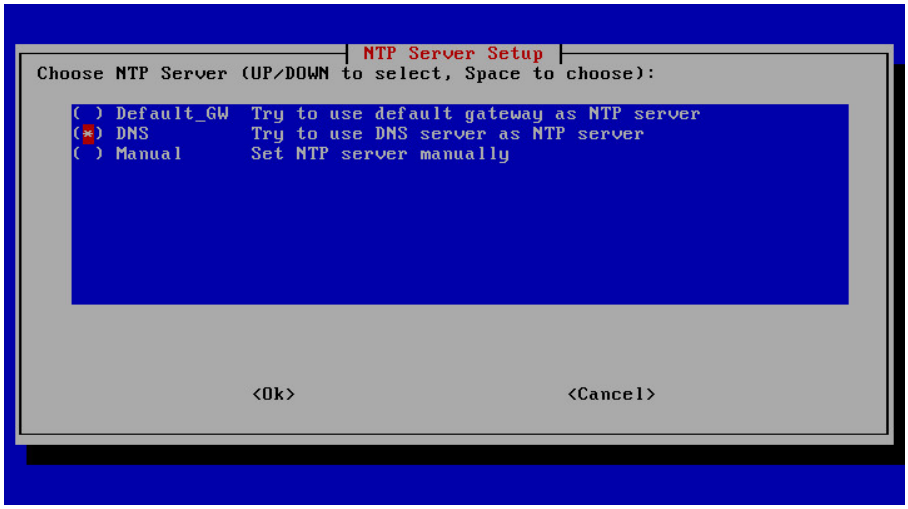
- General Information on Installation Steps for Server Components
- All-in-one Installation Mode of TM Enterprise and TM Standard
- Distributed Installation of TM Enterprise

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:

- Configuring Time Synchronization (NTP-server)
- Localization Setup
- Configuring the Automatic Event Deletion from the Database
- Completing the Installation

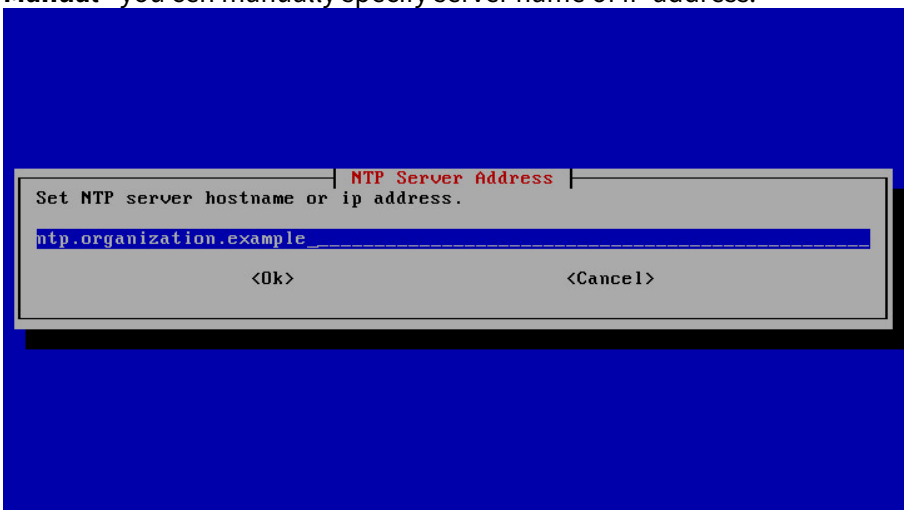
Configuring Time Synchronization (NTP-server)



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**.

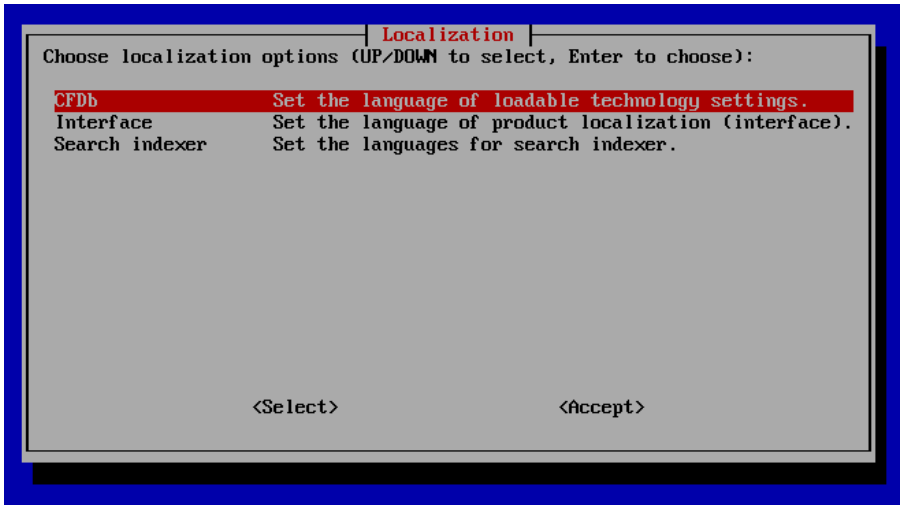
- **Default_GW** - default gateway

- **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*».

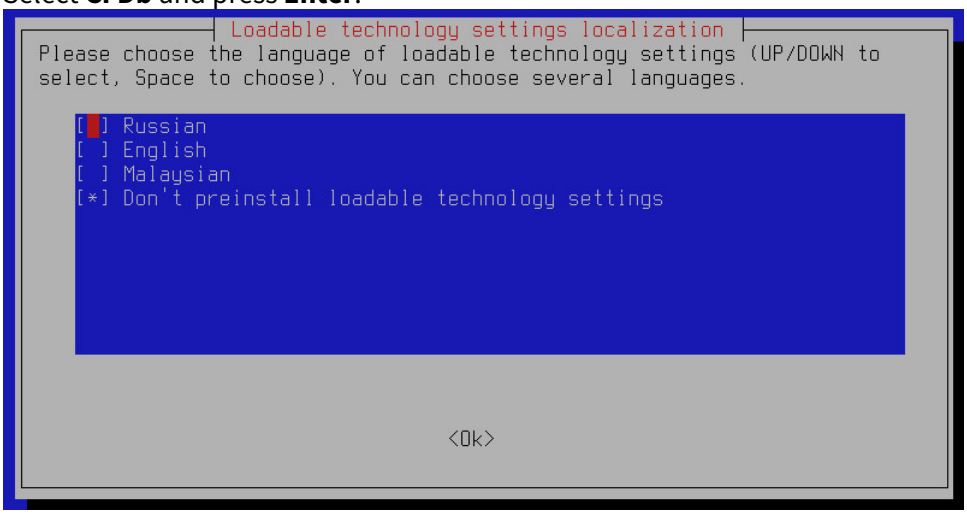
Localization Setup



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**.



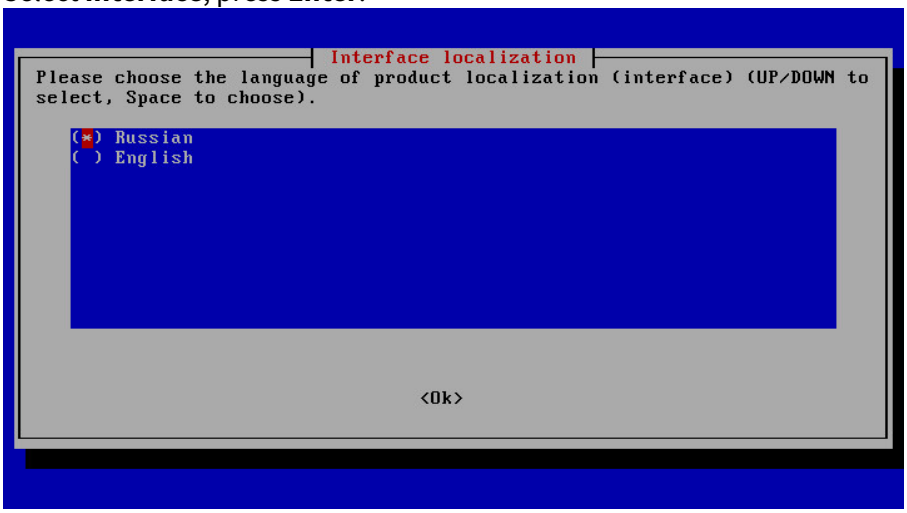
There are three languages available:

- *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 basic language to be used for user interface of Management Console, date and time displaying format, preset configuration.
   a. Select **Interface**, press **Enter**.

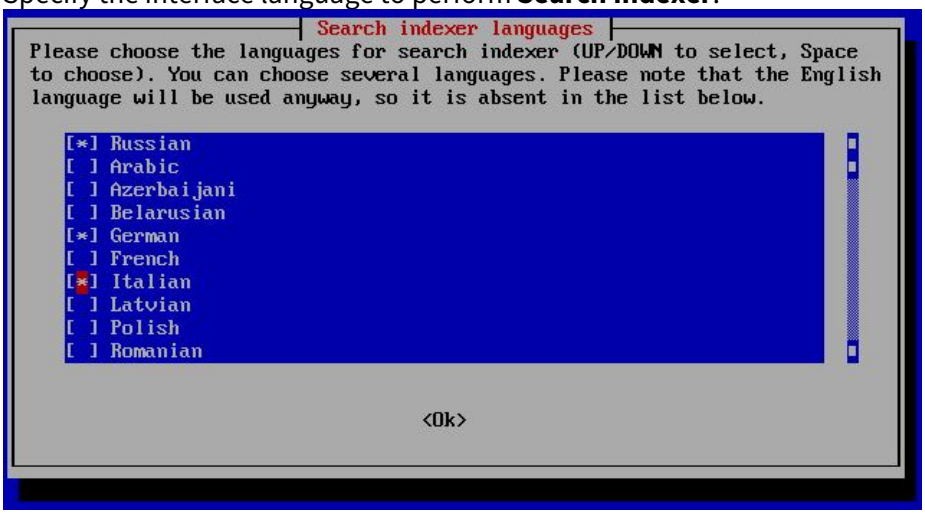


There are two languages available:

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

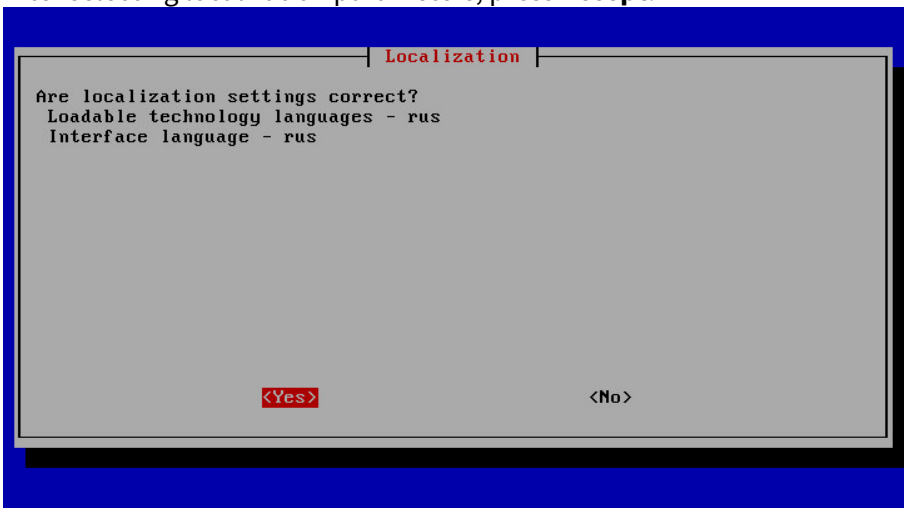
   b. select required interface language and press **OK**.

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



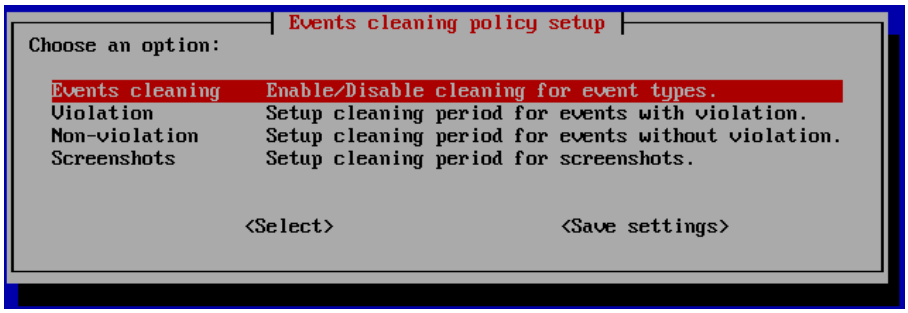
To select the language set the cursor on the needed field and click space keyboard key until an asterisk (*) appeared. You can select one or more languages.

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



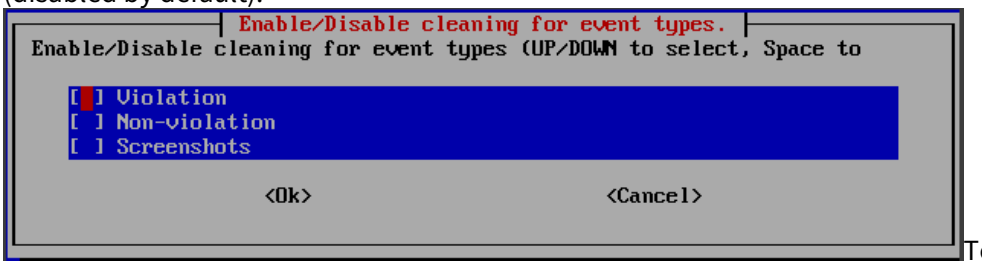
5. In the window that opens, make sure that selected languages for pre-installed entities, interface, and indexing are specified correctly, then press **Yes**.

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**:

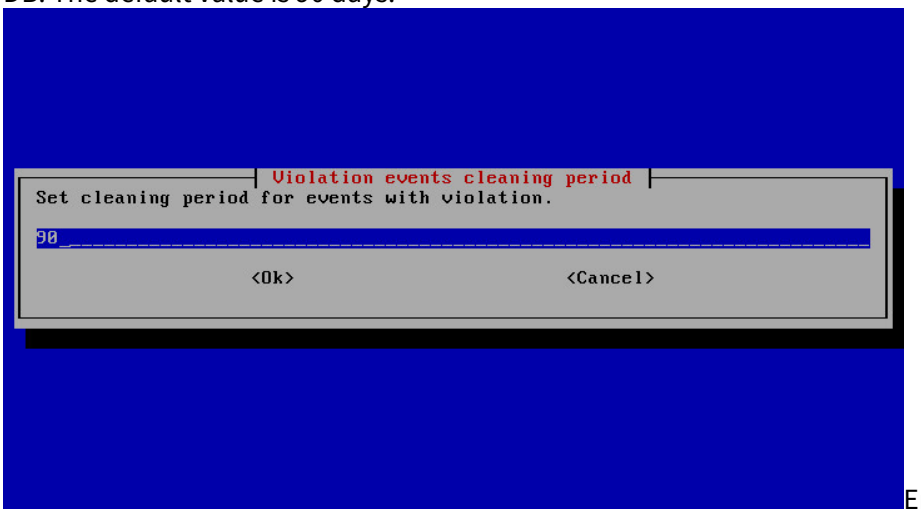
- **Events cleaning** – configures enabling and disabling of the automatic deletion of two event types (disabled by default).



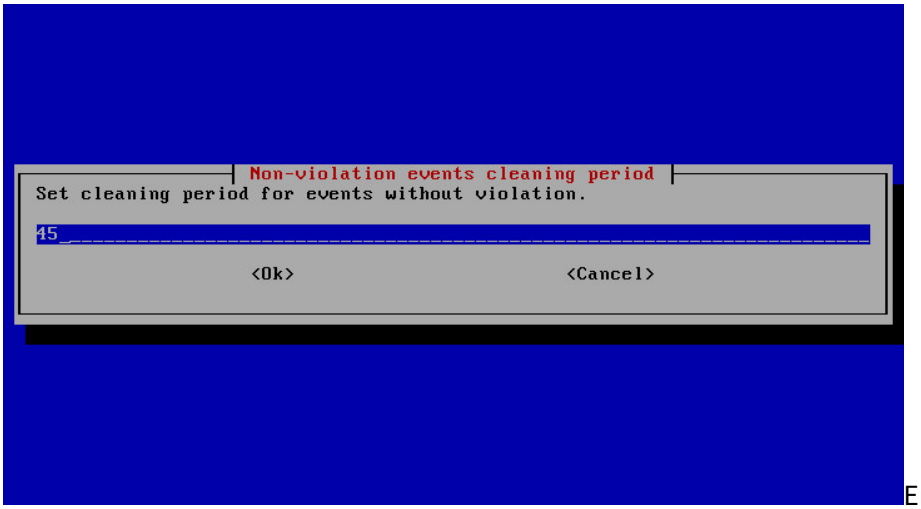
To select the option set the cursor on the needed field and click space keyboard key until an asterisk (*) appeared:
  - **Violation** – enables automatic deletion of events which violate the security policy (see details on policies in "*InfoWatch Traffic Monitor. User Guide*")
  - **Non-violation** – 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.

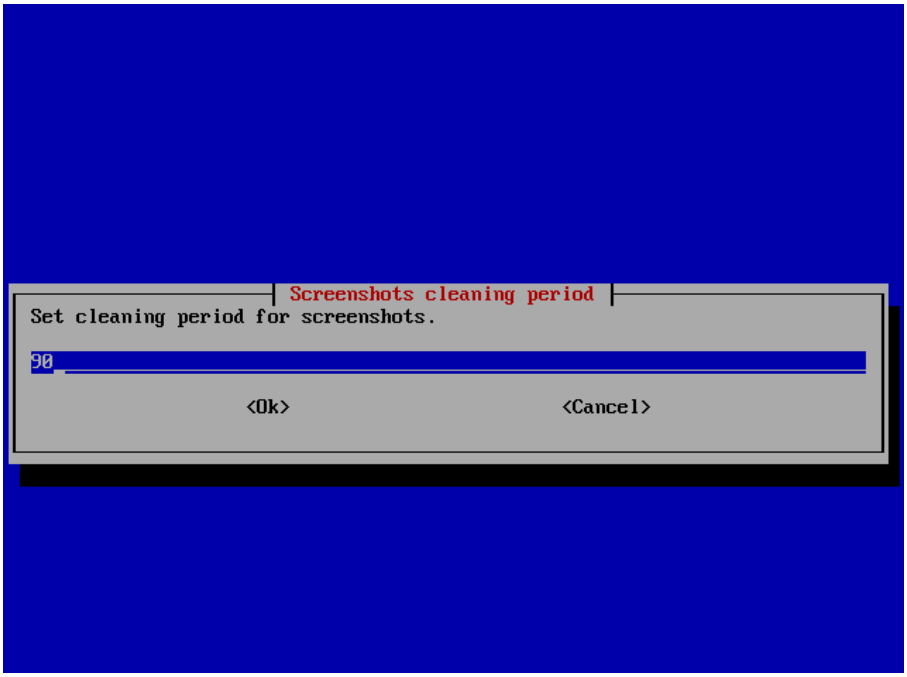


Enter the period of deletion, in days. Click **Ok**.
- **Non-violation** – sets a number of days after which the event without violations will be deleted from the DB. Default value is 45 days.



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.

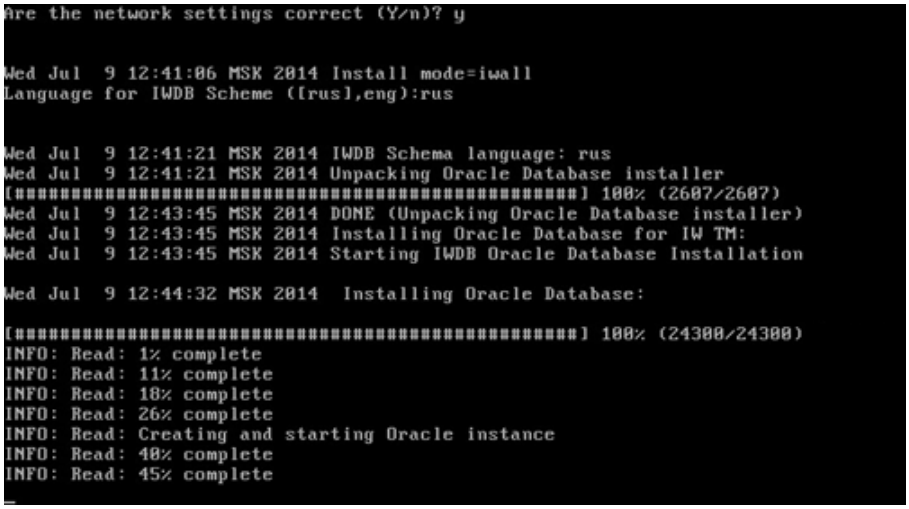


Enter the period of deletion, in days. Click **Ok**.

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".

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.

> **Warning!**
>
> 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. To log into the System, enter login and password (you should enter as a **root** user with a password created while installation).

   > **Warning!**
   >
   > Before running the installation make sure that server complies with the OS and network settings requirements.

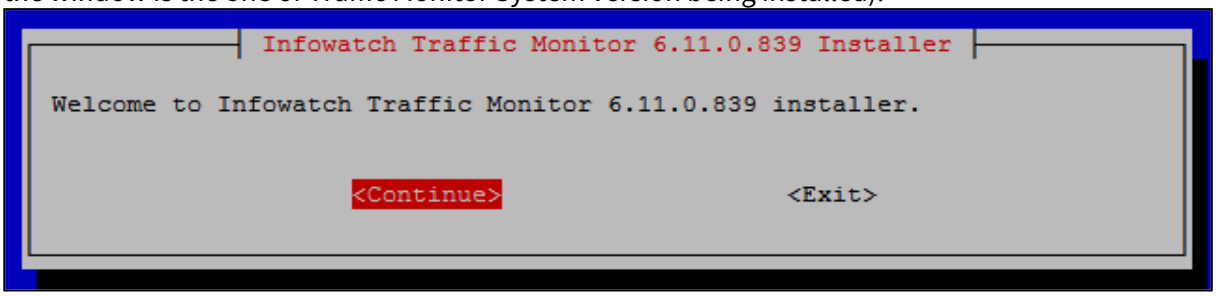
2. Create a directory to locate the InfoWatch Traffic Monitor installer. For example, to create a directory named `distr` in the root of the file system run the following command:
   `mkdir /distr`
3. Copy the files from InfoWatch Traffic Monitor distributive into the created directory.
   - **iwtm-installer-x.x.x.xxx-rhel7.run** (where x.x.x.xxx is a number of build);
   - **iwtm-postgresql-9.6.13-x.xx.x.tar.gz**;
   - **iwtm-oracle-12.2.0.1-x.xx.x.tar.gz**;
   - **iwtm-adp-x.xx.x.tar.gz**.

   As per our example:
   - **`iwtm-installer-6.11.0.839-rhel7.run`;**

- **iwtm-postgresql-9.6.13-6.11.0.tar.gz;**
- **iwtm-oracle-12.2.0.1-6.11.0.tar.gz;**
- **iwtm-adp-6.11.0.tar.gz.**

> **Note:**
>
> If you are using **Oracle DBMS** and Network File System (NFS), follow the steps below:
> - in case you are using Oracle Real Application Clusters (RAC)
>   Set mount options according to the article from official website.
> - in case you are not using RAC:
>   Check in mount point settings (by default `/etc/fstab`), that `noac` option is not used and `actimeo` parameter does not have 0 value.
>   For details, see the article on the official website.

4. Enter the command to shift to Traffic Monitor distributive directory.
   As per our example:
   `cd /distr`
5. Run the following command:
   `bash ./iwtm-installer-x.x.x.xxx-rhel7.run`
   Our example command:
   `bash ./iwtm-installer-6.11.0.839-rhel7.run`
   The unpacking of Traffic Monitor installation files will start. First, the installer will check the System and if a noncompliance found, the installer will interrupt the installation progress and display an error. In this case you should correct the noncompliance and restart the installation. After the unpacking is finished, a window to install Traffic Monitor will be displayed (the number in the window is the one of Traffic Monitor System version being installed).



   To continue, press **Continue**.
6. In the window of Traffic Monitor version selection, please choose:
   - **TM Enterprise** to install Enterprise edition;
   - **TM Standard** to install Standard edition.

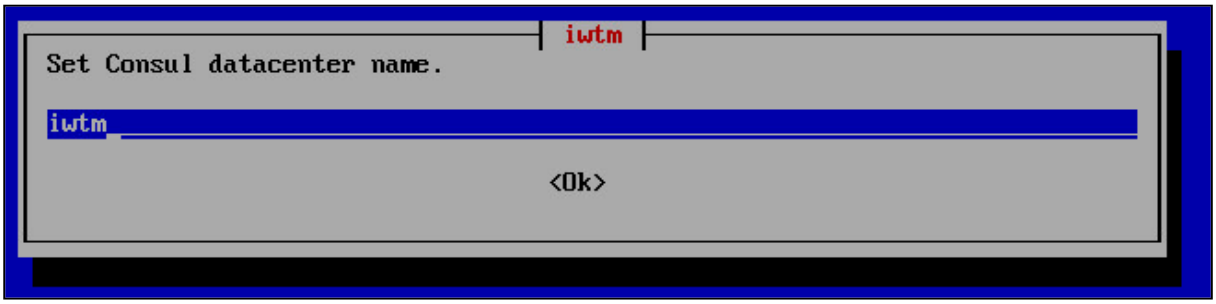
   For this, set asterisk (*) in the required field by pressing Space, then click **OK**.

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

7. In the window of the Database selection, please select the required DBMS (the option is available for **TM Enterprise** only):

- **Oracle Enterprise**
- **PostgreSQL**.
  For this, set asterisk (*) opposite to the DBMS by pressing Space, then click **OK**.

8. If **TM Enterprise** edtition was selected, in the window of installation mode selection, choose **All-in-one**. For this, set asterisk (*) opposite to the mode by pressing Space, then click **OK**.
9. Enter the name of Consul datacenter and click **OK**.



10. 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 (see the details on configuring the NTP server in "*InfoWatch Traffic Monitor. Administration Guide*», "Setting time synchronization").

11. 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.

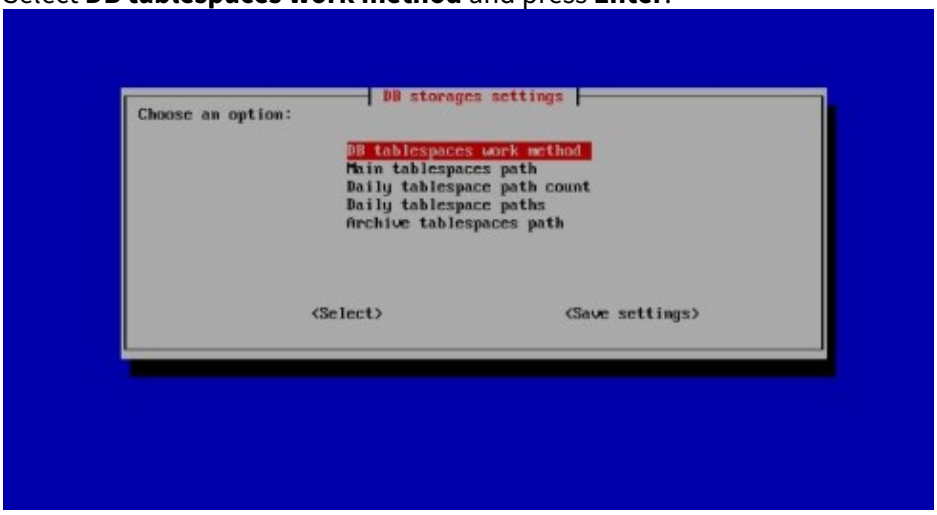
    b. Set interface language:
       i. Select **Interface**and press **Enter**.
       ii. Specify the desired language.
       The Management console will be installed in selected language.
       iii. Click **OK**.

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

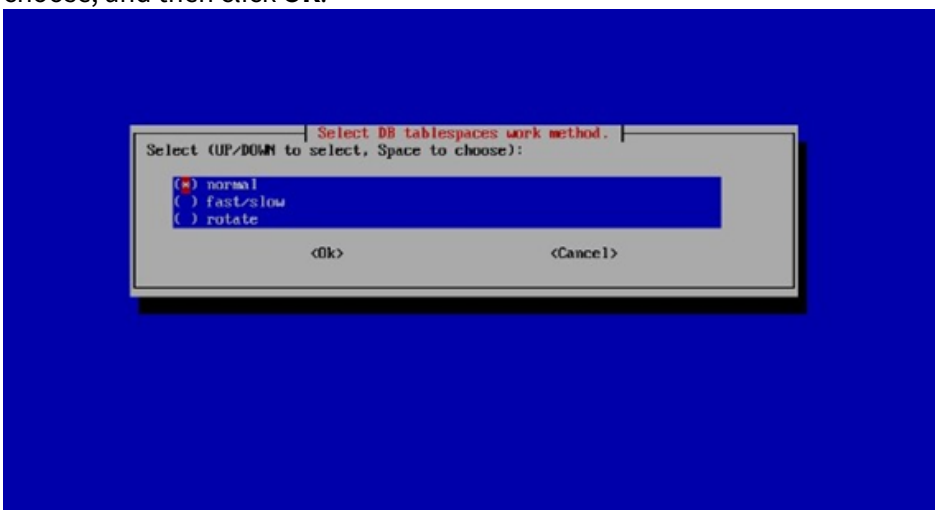
    d. Click **Accept**.
    e. In the opened window, make sure the selected languages for pre-installed settings and interface are specified correctly, then click **Yes**.

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 the mode you choose, and then click **OK**.



- **Normal** (regular) – data transfer method, when the switching to the following partition (when it is specified) happens after the previous one is overflow.
- **Fast/slow** (fast and slow disks) – 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** (daily switch) – 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 the automatic events deletion from the database (by default, the automatic events 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 the screen.

The process may take some time.

Note:

During the installation, you can get the following message:

```
--> Finished Dependency Resolution
Error: Package: iwtm-imagemagick-6.9.10.48-6.11.1.993.x86_64 (tm-6.11.1.1017-rel
          Requires: urw-base35-fonts-legacy
Error: Package: perl-utf8-all-0.011-1.el7.noarch (iwtm-adp-6.11.1)
          Requires: perl(Dist::CheckConflicts) >= 0.02
**********************************************************************
Dependency resolving failed due to missing dependencies.
Some repositories on your system are disabled, but yum can enable them
and search for missing dependencies. This will require downloading
metadata for disabled repositories and may take some time and traffic.
**********************************************************************

https://cdn.redhat.com/content/e4s/rhel/server/7/7Server/x86_64/sat-tools/6.7/os
Trying other mirror.
To address this issue please refer to the below knowledge base article

https://access.redhat.com/solutions/69319

If above article doesn't help to resolve this issue please open a ticket with Red Hat Support.
```

In this case, connect the EPEL repository and start the installation again.

You can find instructions on how to connect the EPEL repository at the Red Hat Enterprise Linux official web page.

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

Web Console is installed in an automatic mode using installation 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.

See the list of processes that should be running in a single copy only on a particular server, in the document "InfoWatch Traffic Monitor. Administration guide", the article "Check of process autostart". To learn how to enable or disable the processes autorun, check the same document, the artcile "Enabling and disabling process autorun". To see the processes description, go to "InfoWatch Traffic Monitor. Administration guide", the article "List of Traffic Monitor Server End Processes".

Installing Database

> **Warning!**
>
> This chapter contains instructions without a 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 DB, perform the following steps:

1. To log into the System, enter login and password (you will be logged in on behalf of a root user with login and password created while installation).

   > **Warning!**
   >
   > Before running the installation make sure that the server complies with the OS and network settings requirements

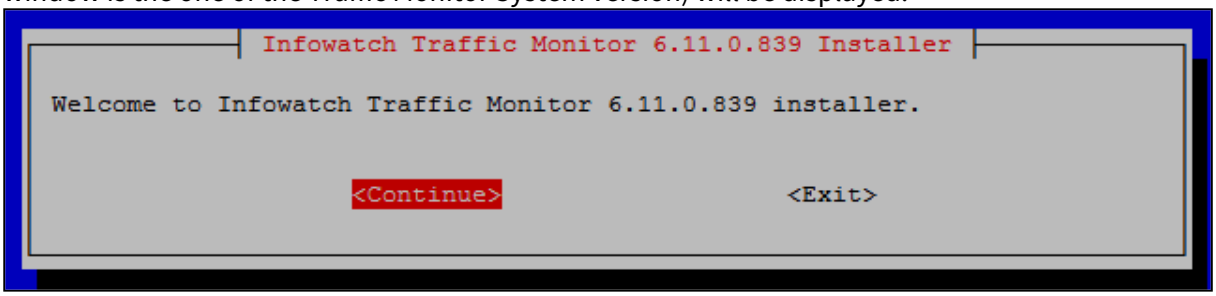
2. Create a directory to locate the InfoWatch Traffic Monitor installer. For example, to create a directory named distr in the root of the file system, run the following command:
   `mkdir /distr`
3. Copy the files from the InfoWatch Traffic Monitor distributive into the created directory.
   - **iwtm-installer-x.x.x.xxx-rhel7.run** (where x.x.x.xxx is a number of build);
   - **iwtm-postgresql-9.6.13-x.xx.x.tar.gz**;
   - **iwtm-oracle-12.2.0.1-x.xx.x.tar.gz**;
   - **iwtm-adp-x.xx.x.tar.gz**.

   Our example command:
   - **`iwtm-installer-6.11.0.839-rhel7.run`**;
   - **`iwtm-postgresql-9.6.13-6.11.0.tar.gz`**;
   - **`iwtm-oracle-12.2.0.1-6.11.0.tar.gz`**;
   - **`iwtm-adp-6.11.0.tar.gz`**.

   Note:

   If you are using **Oracle DBMS** and Network File System (NFS), follow the steps below:
   - in case you are using Oracle Real Application Clusters (RAC)
     Set mount options according to the article from official website.
   - in case you are not using RAC:
     Check in mount point settings (by default `/etc/fstab`), that `noac` option is not used and `actimeo` parameter does not have 0 value.
     For details, see the article on the official website.

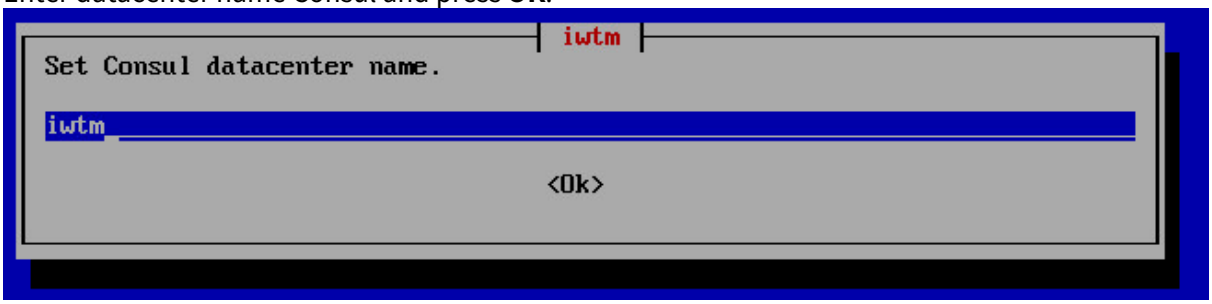
4. Run the command to shift to the Traffic Monitor distributive directory. Our example command:
   `cd /distr`
5. Run the following command:
   `bash ./iwtm-installer-x.x.x.xxx-rhel7.run`
   Our example command:
   `bash ./iwtm-installer-6.11.0.839-rhel7.run`
   The unpacking of Traffic Monitor installation files will start. First, it the installer will check the System, and if a noncompliance found, the installer will interrupt the installation progress and display an error.
   In this case, you should correct the noncompliance and restart the installation.
   After the unpacking is finished, a window asking to install the Traffic Monitor (the number in the window is the one of the Traffic Monitor System version) will be displayed.



   To continue, press **Continue**.
6. In the window of Traffic Monitor edition selection, please select **TM Enterprise**. For this, set asterisk (*) in **TM Enterprise** field by pressing Space, then click **OK**.

7. In the window of the Database selection, please select the required DBMS:
   - **Oracle;**
   - **PostgreSQL.**

   For this, set asterisk (*) in the field opposite to the mode you choose, and then click **OK**.
8. In the window of the installation mode, select **DB node**, and press **OK**.
9. Enter datacenter name Consul and press **OK**.



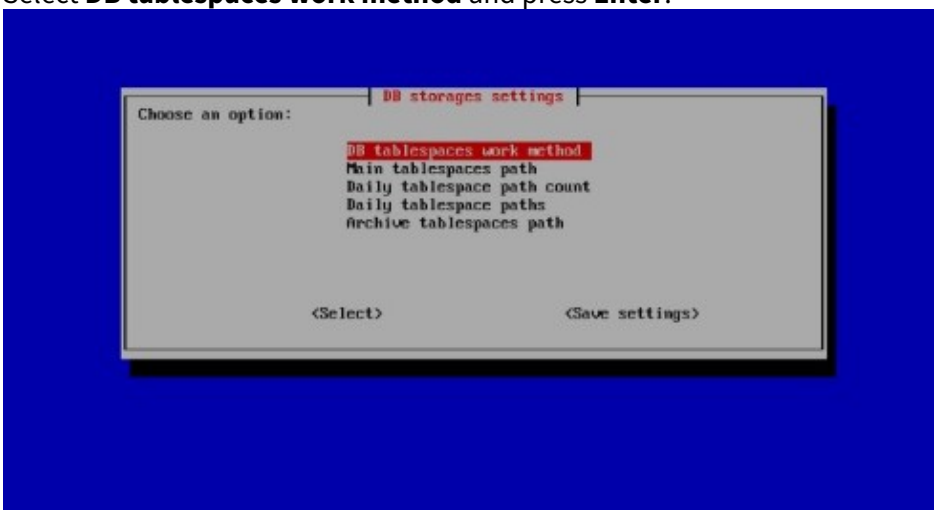
10. Specify server address for time synchronization (NTP-server). To do this, set asterisk (*) in the required field by pressing **Space**, then click **OK**.
11. Set localization settings:
    a. Set the language of pre-installed settings:
       i. Select **CFDB** and press **Enter**.
       ii. Specify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

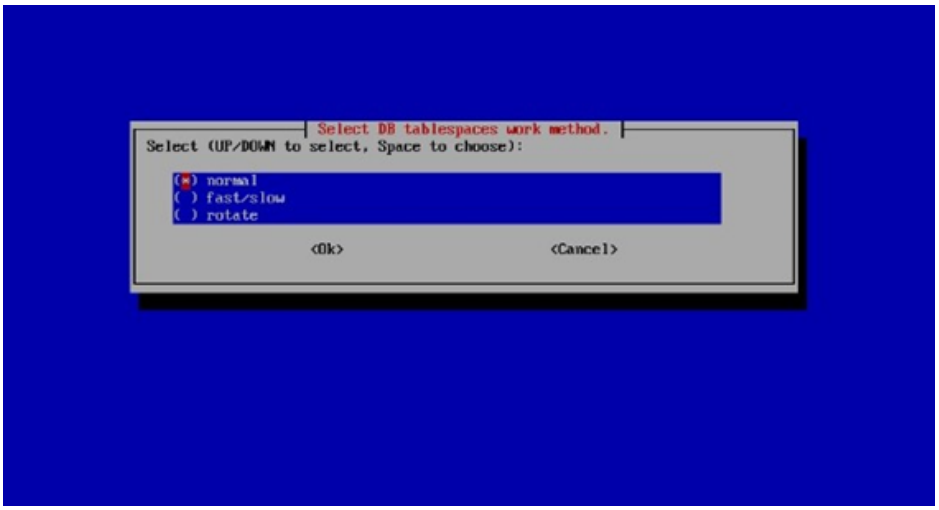
    c. Set the language for Search indexer:
       i. Select **Search indexer** and press **Enter**.
       ii. Specify one or several languages.
       iii. Press **OK**.

    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 the mode you choose and then click **OK**.



- **Normal** (regular) – data transfer method, when the switching to the following partition (when it is specified) happens after the previous one is overflow.
- **Fast/slow** (fast and slow disks) – data transfer method, dividing pools into fast and slow ones. 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** (daily switch) – 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 the 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/oradata** and for PostgreSQL database it is **/u02/pgdata**).
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). Enable automatic deletion of events that violate the security policy and/or do not violate the security policy. To select the option set the cursor opposite the **Violation** and/or **Non-violation**. Press **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, received from DM Client will be deleted from the DB.
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.

Note:

During the installation, you can get the following message:

```
--> Finished Dependency Resolution
Error: Package: iwtm-imagemagick-6.9.10.48-6.11.1.993.x86_64 (tm-6.11.1.1017-rel
|  |  |  |  |  |  Requires: urw-base35-fonts-legacy
Error: Package: perl-utf8-all-0.011-1.el7.noarch (iwtm-adp-6.11.1)
|  |  |  |  |  |  Requires: perl(Dist::CheckConflicts) >= 0.02
**********************************************************************
Dependency resolving failed due to missing dependencies.
Some repositories on your system are disabled, but yum can enable them
and search for missing dependencies. This will require downloading
metadata for disabled repositories and may take some time and traffic.
**********************************************************************

https://cdn.redhat.com/content/e4s/rhel/server/7/7Server/x86_64/sat-tools/6.7/os
Trying other mirror.
To address this issue please refer to the below knowledge base article

https://access.redhat.com/solutions/69319

If above article doesn't help to resolve this issue please open a ticket with Red Hat Support.
```

In this case, connect the EPEL repository and start the installation again.

You can find instructions on how to connect the EPEL repository at the Red Hat Enterprise Linux official web page.

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

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 a 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:

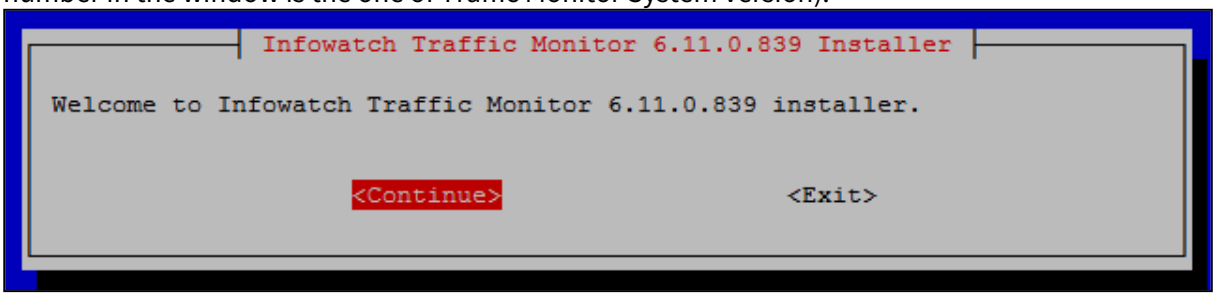
1. To log in into the System, enter login and password (you will be logged in as a root user with login and password created during installation).

   Warning

   Before running the installation, make sure that the server complies with the OS and network settings requirements

2. Create a directory to locate the InfoWatch Traffic Monitor installer. **For example**, to create a directory named `distr` in the root of the file system run the following command:
   `mkdir /distr`
3. Copy the files from InfoWatch Traffic Monitor distributive into the created directory.
   - **iwtm-installer-x.x.x.xxx-rhel7.run** (where x.x.x.xxx is a number of build);
   - **iwtm-postgresql-9.6.13-x.xx.x.tar.gz**;
   - **iwtm-oracle-12.2.0.1-x.xx.x.tar.gz**;
   - **iwtm-adp-x.xx.x.tar.gz**.

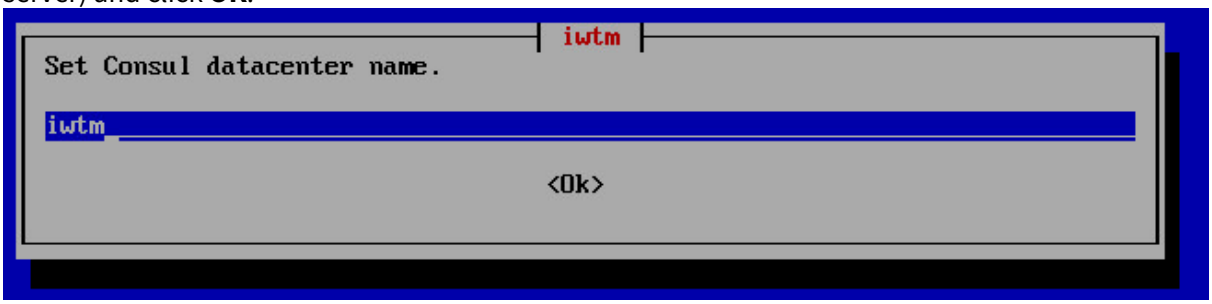
   Our example command:
   - **`iwtm-installer-6.11.0.839-rhel7.run;`**
   - **`iwtm-postgresql-9.6.13-6.11.0.tar.gz;`**
   - **`iwtm-oracle-12.2.0.1-6.11.0.tar.gz;`**
   - **`iwtm-adp-6.11.0.tar.gz.`**
4. Run the command to shift to Traffic Monitor distributive directory.
   Our example command:
   `cd /distr`
5. Run the following command:
   `bash ./iwtm-installer-x.x.x.xxx-rhel7.run`
   Our example command:
   `bash ./iwtm-installer-6.11.0.839-rhel7.run`
   The unpacking of Traffic Monitor installation file will start. First, the installer will check the System. If noncompliance found the installer will interrupt the installation progress and display an error. In this case, you should correct the noncompliance and restart the installation.
   After the unpacking is finished, a window asking to install Traffic Monitor will be displayed (the number in the window is the one of Traffic Monitor System version).



   To continue, press Continue.
6. In the window of Traffic Monitor edition selection, please select **TM Enterprise**. For this, set asterisk (*) in **TM Enterprise** field by pressing Space, then click **OK**.
7. In the window of the Database selection, select the required DBMS:
   - **Oracle**
   - **PostgreSQL**.

   For this, set asterisk (*) opposite to the mode you choose by pressing Space, then click **OK**.
8. In the window of installation mode selection, choose **TM Node**. For this, set asterisk (*) opposite to the mode by pressing Space, then click **OK**.

9. Enter the name of Consul datacenter which was specified when installing DB server (TME DB server) and click **OK**.



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

12. 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**.

> **Note:**
>
> During the installation, you can get the following message:
>
> ```
> --> Finished Dependency Resolution
> Error: Package: iwtm-imagemagick-6.9.10.48-6.11.1.993.x86_64 (tm-6.11.1.1017-rel
>        Requires: urw-base35-fonts-legacy
> Error: Package: perl-utf8-all-0.011-1.el7.noarch (iwtm-adp-6.11.1)
>        Requires: perl(Dist::CheckConflicts) >= 0.02
> ********************************************************************
> Dependency resolving failed due to missing dependencies.
> Some repositories on your system are disabled, but yum can enable them
> and search for missing dependencies. This will require downloading
> metadata for disabled repositories and may take some time and traffic.
> ********************************************************************
>
> https://cdn.redhat.com/content/e4s/rhel/server/7/7Server/x86_64/sat-tools/6.7/os
> Trying other mirror.
> To address this issue please refer to the below knowledge base article
>
> https://access.redhat.com/solutions/69319
>
> If above article doesn't help to resolve this issue please open a ticket with Red Hat Support.
> ```
>
> In this case, connect the EPEL repository and start the installation again.
>
> You can find instructions on how to connect the EPEL repository at the Red Hat Enterprise Linux official web page.

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

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.

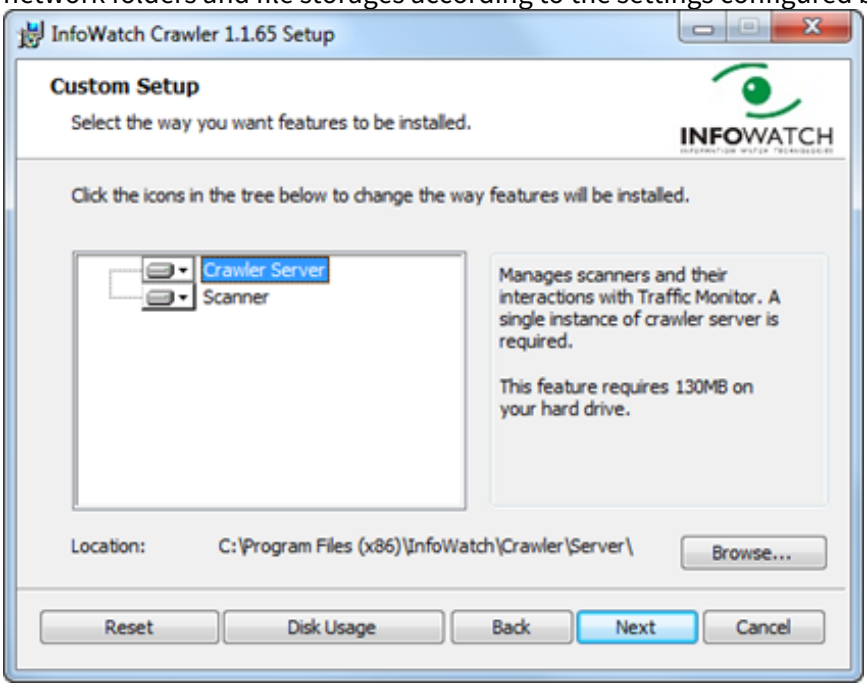
> **Warning!**
>
> Before the installation, make sure that the servers Traffic Monitor and Crawler are connected. For this, check Crawler server's availability by running the following command on Traffic Monitor server: ping <short name of Crawler server>. Otherwise, Crawler subsystem can be installed, 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.

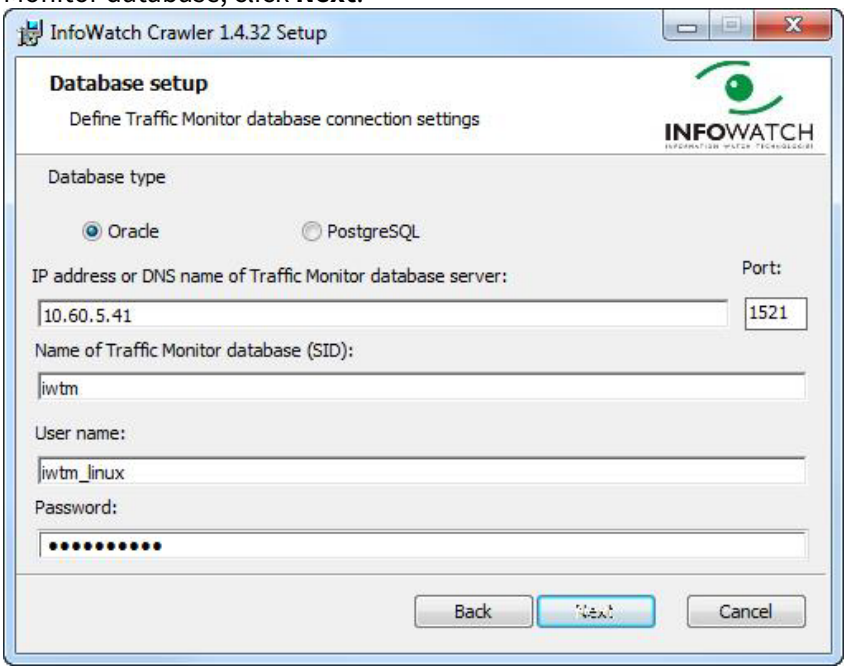
> **Note:**
>
> The language of the Installation Wizard is defined automatically and depends on the selected format (see **Start -> Control Panel -> Region and Language**, **Formats** tab).

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.Scanner` 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**:

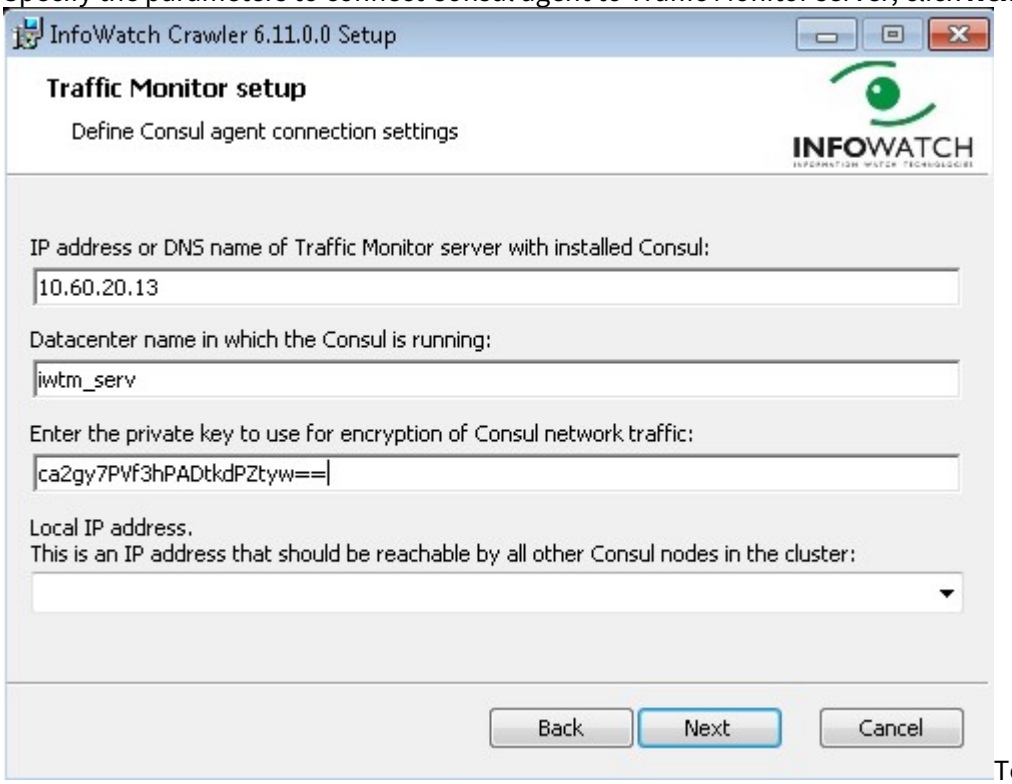
a. Specify parameters for connection of the `InfoWatch.Crawler.Server` service with Traffic Monitor database, click **Next**.



Depending on DB being used, connnection 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 the 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`.

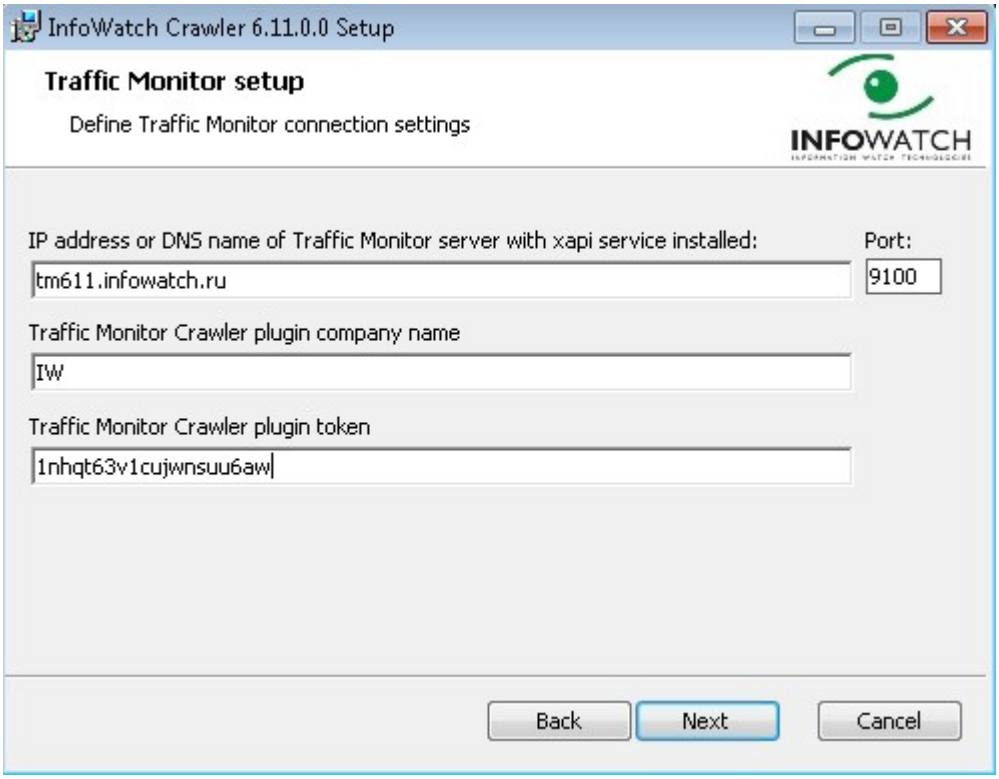
iv. The data required for installation are located in the sections:

`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**.

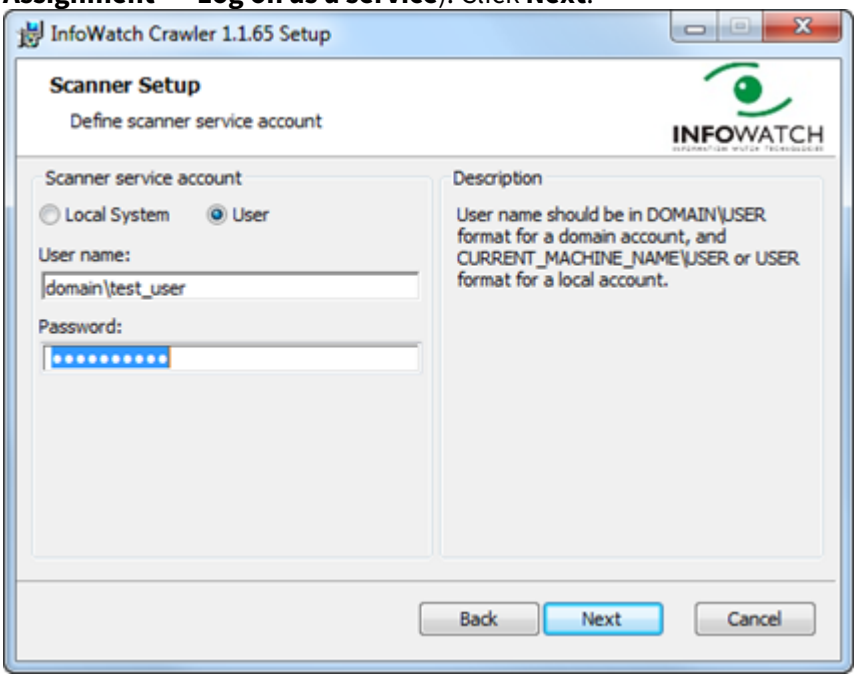


In case of distributed installation, in **IP address or DNS name of Traffic Monitor Service Manager** field specify the IP address or DNS name of TM server (TME Node Server).

d. Fill in the fields the following way:
   - **Traffic Monitor Crawler plugin company name** - always "IW",
   - **Traffic Monitor Crawler plugin token** - use data from the **Plugins** section of Traffic Monitor Management Console.

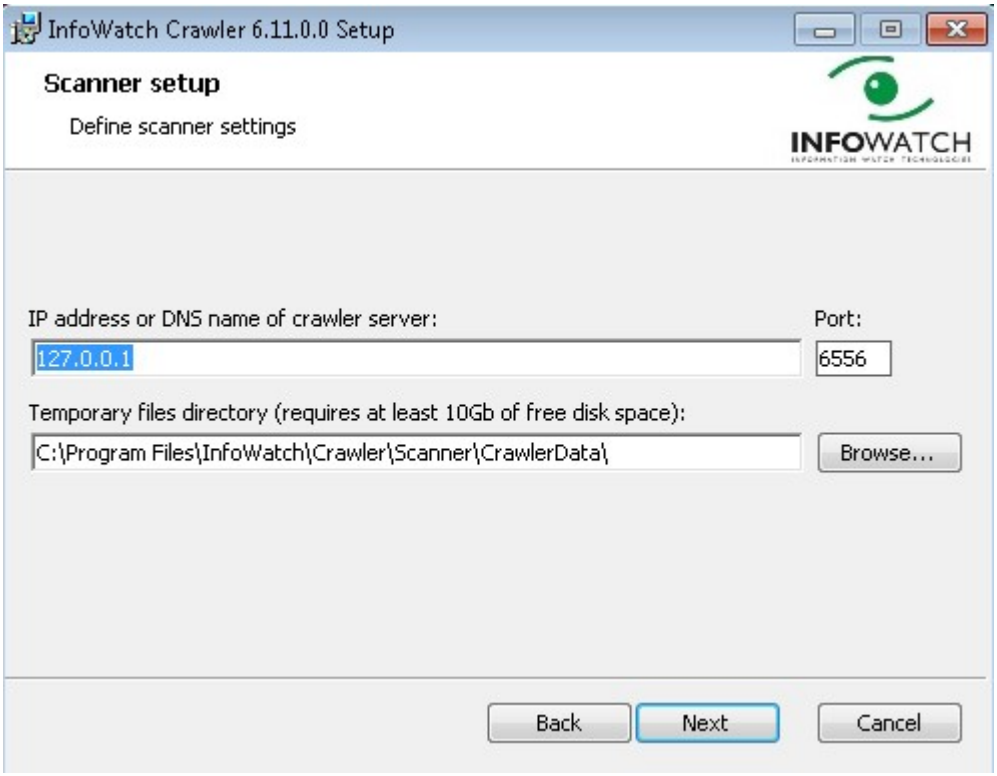
6. If on the **Custom Setup** step you have chosen the installation of **Scanner component**:
   a. specify an account that will be used to launch `InfoWatch.Crawler.Scaner` service. You can select a standard Local System account (recommended) or specify an account which has permissions for running services 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: `iwtm restart kicker`.

Important!

After 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").

> **Warning!**
>
> To operate correctly Traffic Monitor and Device Monitor should have the same versions. See more details about Device Monitor 6.11 compatibility in the InfoWatchKnowledge Base article "Compatibility among the versions of TM, DM and Agents".

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

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

- Microsoft .NET Framework 4.5 pack
- Oracle DBMS client (only after 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 specify connection options. Choose one of the two options described below.

Option 1. Configure tnsnames.ora file ([ORACLE_HOME]\network\admin)

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.

Option 2. Specify TNS string representation from tnsnames.ora file as a database server.

Example of string representation

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=iwdm.infowatch.ru)(PORT=1521))
(CONNECT_DATA=(SERVER=dedicated)(SERVICE_NAME=iwtm)))
```

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.

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 the `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

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

   Note:

   To install a 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 the 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 the **Install new Database** option.
   Click **Next**.

5. **Choosing a 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 the 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.

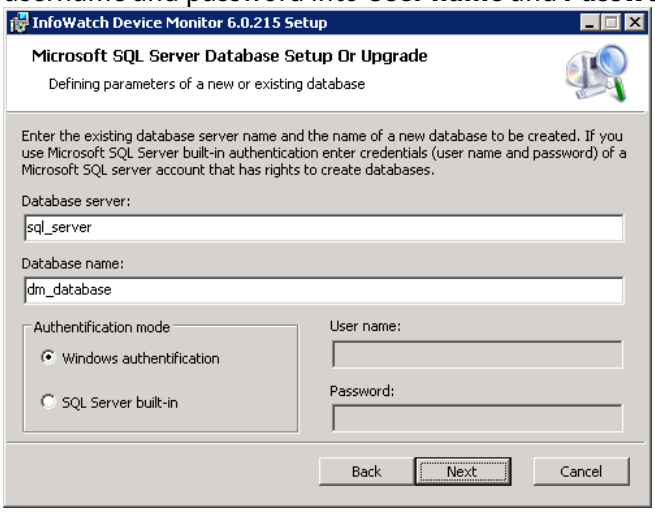
   Click **Next**. In this case, all existing settings and elements of configuration will be replaced with imported ones.

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 the 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 an IP address in the **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 the server name as follows: <server_name>\<instance_name>.
   - **Database name**. New database name.
     It may contain Latin letters, numbers, and other characters except for spaces and special characters: «*», «?», «/», «\», «|», «^», «:», «"". The name must start with a Latin letter.
     The name can 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:

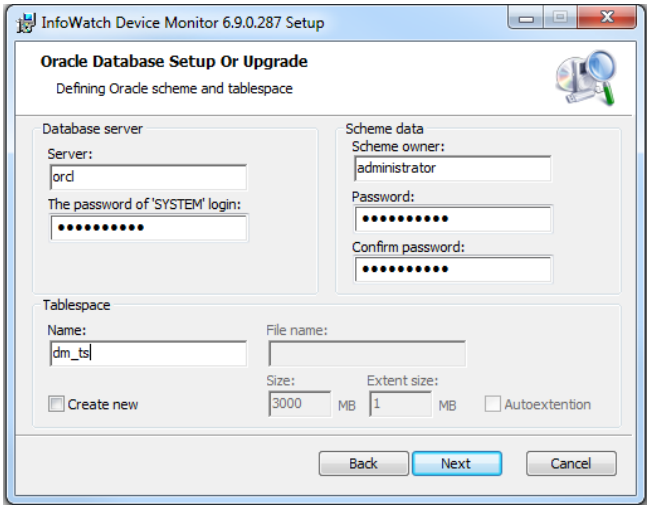
a. Set database server connection options:
- **Database server**. Database server name. For this parameter, use server alias `tns_name` from the **tnsnames.ora** file or TNS string representation.
- **The password of 'SYSTEM' login**. SYSTEM account password.

b. Specify the parameters of the database schema owner account:

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

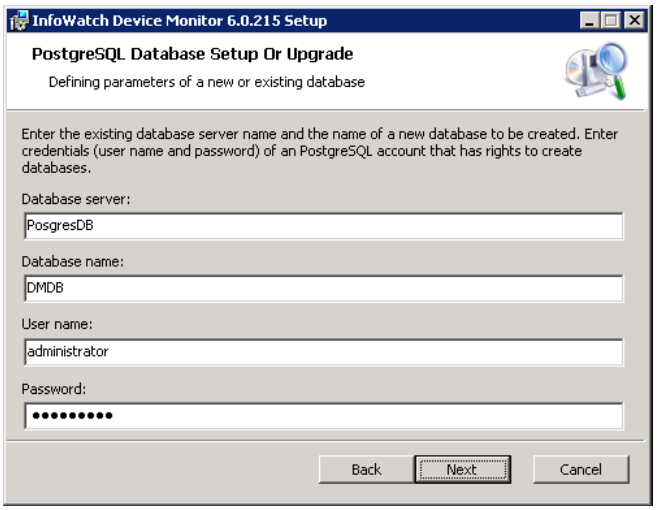
- **Scheme owner**. Database schema owner account name.
- **Password, Confirm password**. Database schema owner account password.
Password is assigned based on requirements specified in Oracle DBMS documentation.

c. Configure tablespace settings in the **Tablespace** box.
You can use an existing tablespace or create a new one. If you are using existing tablespace, enter the tablespace name in the **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 a continuous segment in a data file (the default size is 1 MB).
- **Autoextension**. Automatic file extension via Oracle DBMS. If the **Autoextension** box is selected, an 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 created database.
  It may contain Latin letters, numbers and other symbols excluding spaces and special symbols: «*», «?», «/», «\», «|», «^», «:», «"». Name must start with a Latin letter.
  The name can 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**

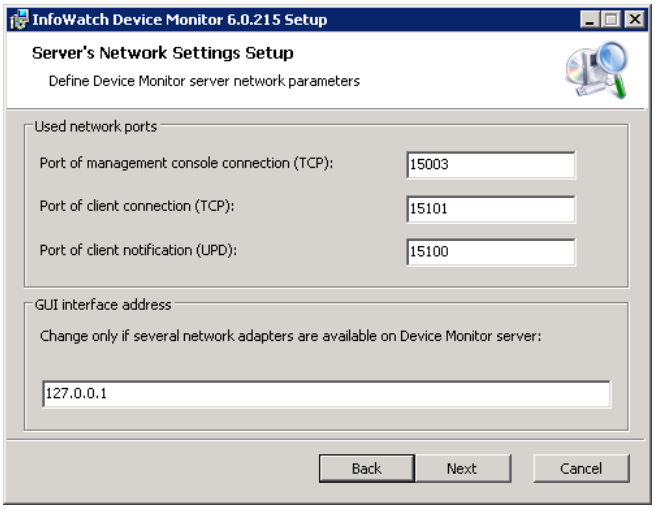
Configure Server parameters:

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 the 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 the Server, you can change this setting in the 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 a 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 the 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. The address must be entered in the following format:
      `host:port`
      Host parameter should contain the 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**. The 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 the 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 the server installation directory by selecting the **Save shadow copies** box.

    Click **Next**.
13. **Completing the installation**
Click **Install** to start Server installation.
Follow the instructions to complete the 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**.

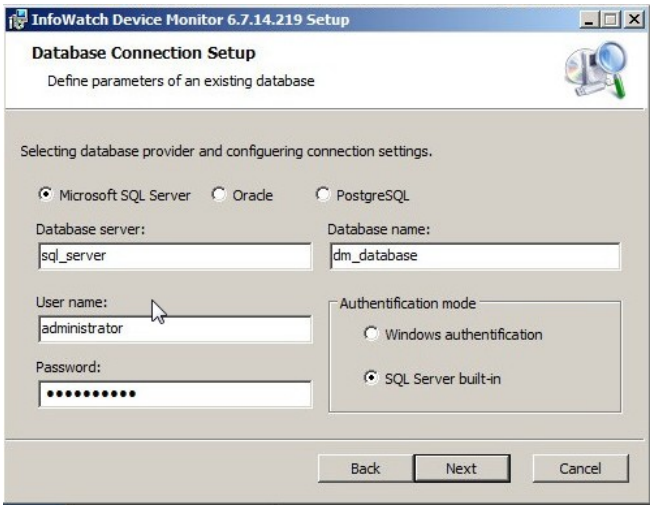
> **Note:**
>
> Signature installation may take a while (up to 30 minutes).

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 the CD-ROM drive. Then open the `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

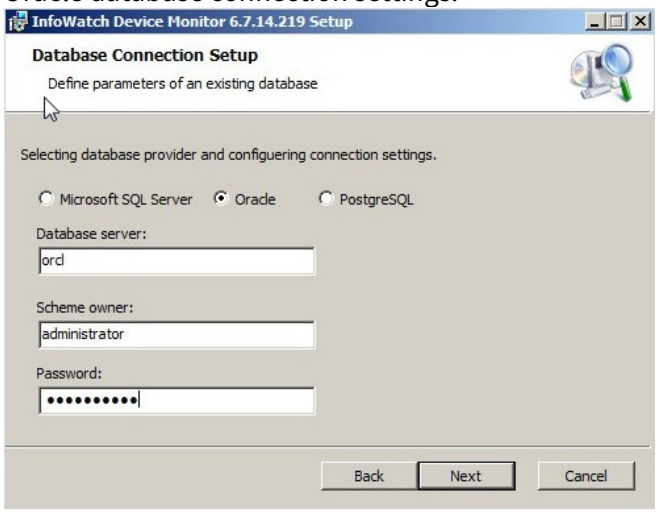
    You can change the list of components you want to install. For example, if you want to use an existing Management Console with a new Server, you do not need to install this feature: click **Management Console** and select ✕**Entire feature will be unavailable**. You can also change the folder to install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

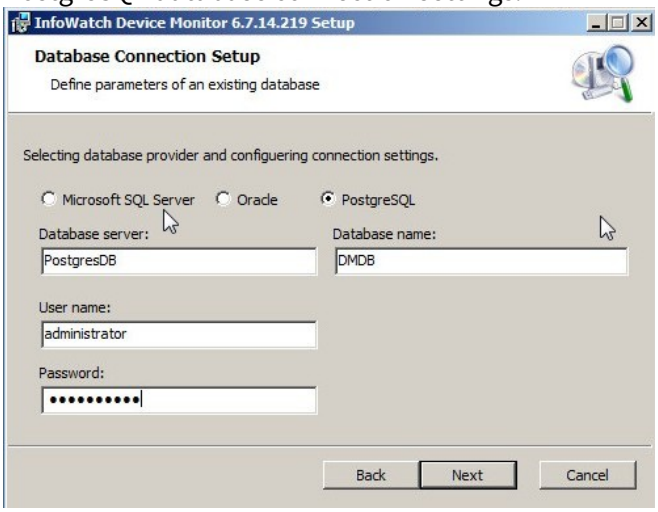
    e. Database connection setup
    Specify DBMS managing Device Monitor database and put in the rest connection parameters that were used while installing the primary server.
    Microsoft SQL Server connection settings
    If the account uses Windows authentication, and the database was created by a domain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

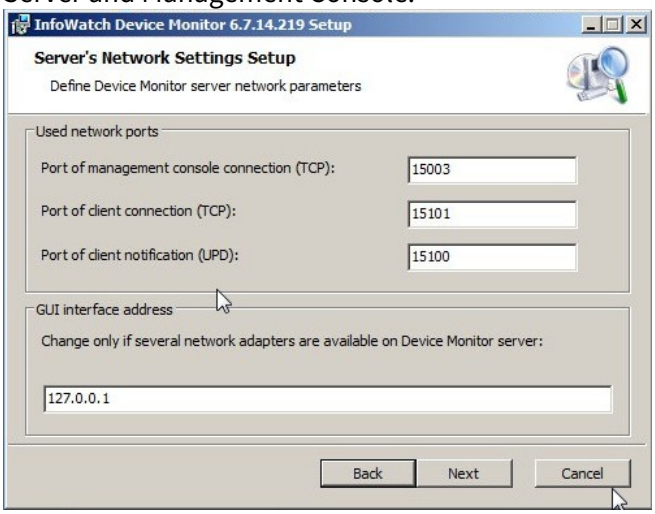
f. Server network parameters setup

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 the server;
- **Agents notification** about security scheme changes.
In **GUI interface address**, enter an 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.
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).

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:

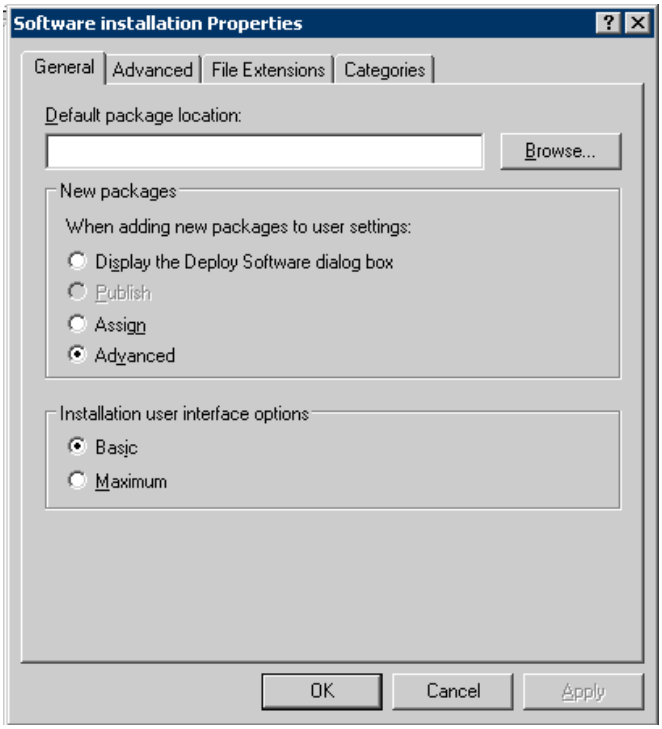
- Active Directory container that holds all target workstations
- the whole Active Directory domain, but not default domain policy. This policy should only cover the group that includes all controlled workstations.

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. **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**.

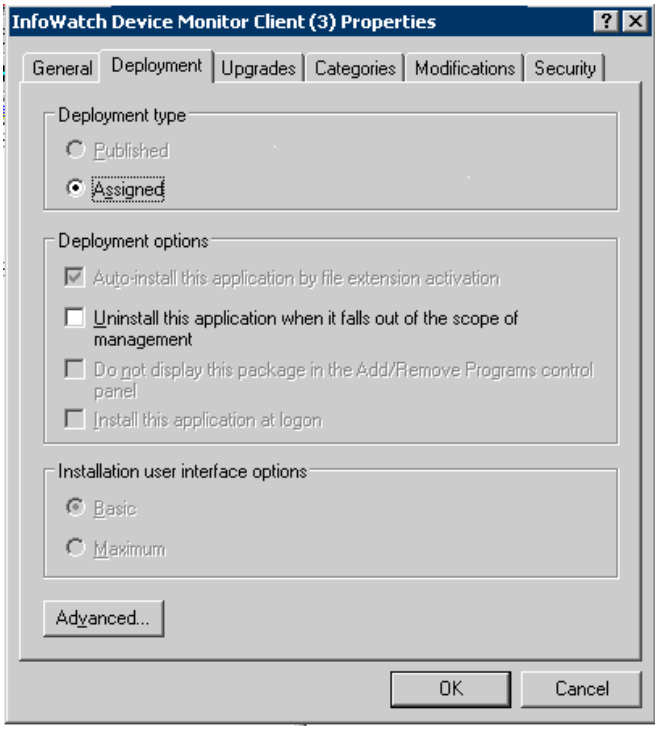


f. When the configuration is complete, click **OK**.

3. **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.

4. **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.

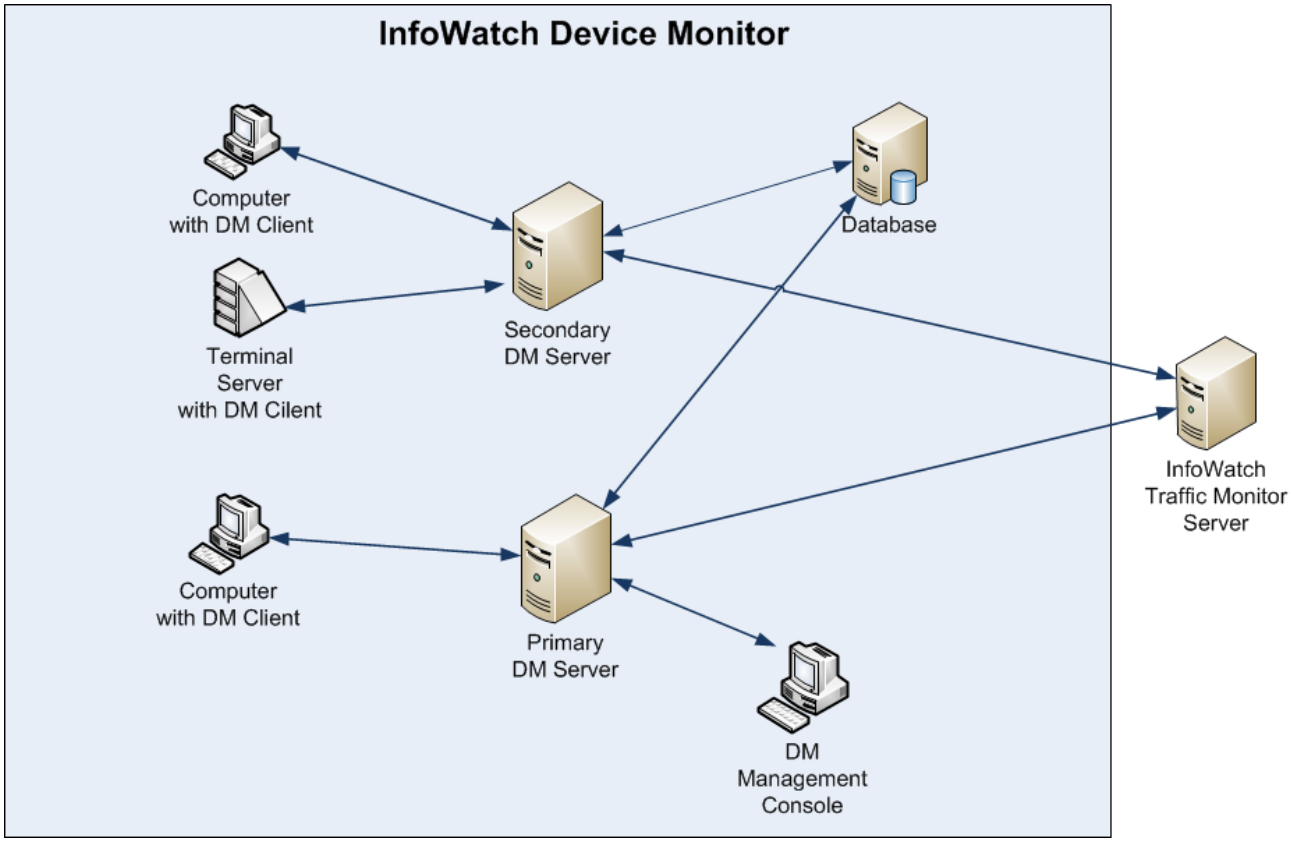
> **Important!**
>
> You can check if the Agent has been installed successfully in InfoWatch Device Monitor Management Console. All workstations the Agent has been successfully installed to must appear in the list in **Workstations** area. To view all managed workstations, click **Show all workstations**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

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
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 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 the 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**. 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. Information about events that subject to a security scheme rule and files shadow copies are sent from controlled workstations 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 no 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 no 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.

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

Warning!

Update to the required Traffic Monitor version is available from two previous releases. The update to 6.11 version can be installed from 6.10 and/or 6.9 versions. Releases history can be found in the article "Traffic Monitor: Main".

Note:

The System is updated 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 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. Guide how to work with repository you can find on Red Hat Enterprise Linux official website.

Warning!

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.

Warning!

During the update, events are neither intercepted nor analyzed.

Before the update, make sure that you have:

- Red Hat Enterprise Linux 7.x distribution disk ISO image;
- InfoWatch Traffic Monitor distributive of the current version;
- InfoWatch Traffic Monitor distributive 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;
- 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.

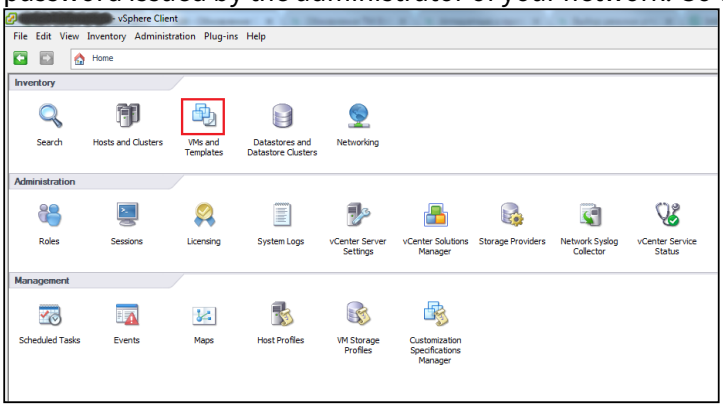
Before the update, take the following steps:

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);

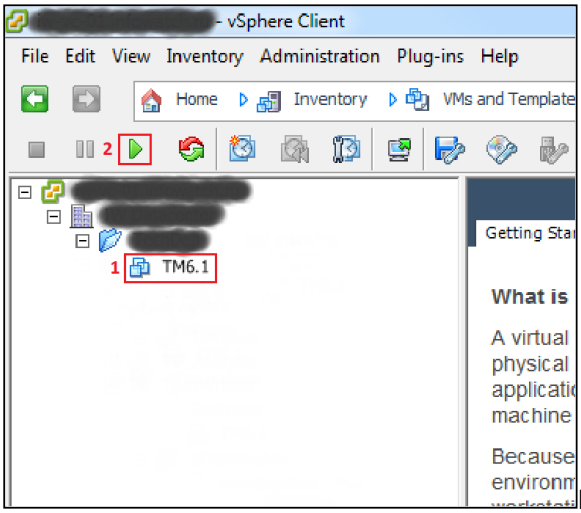
- for the virtual server - run **Power On** command (see the example below).

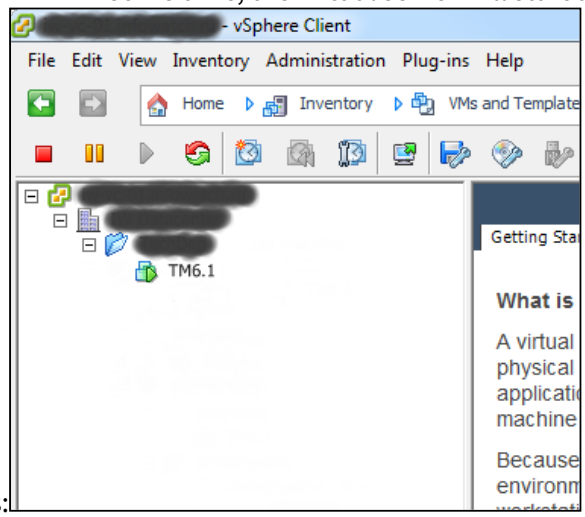
> **Note:**
>
> This instruction contains examples of working with a virtual server in the client application of one of the most common virtualization environments - VMware vSphere (VMware vSphere Client).
> In frameworks, you can see interface areas that you need to click in the specified order to achieve 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 distributive to the servers you want to update, using your OS or virtualization system resources.

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

> **Note:**
>
> After the System update, 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

> **Warning!**
>
> Before updating TM server to version 6.11 we recommend updating DM server first.

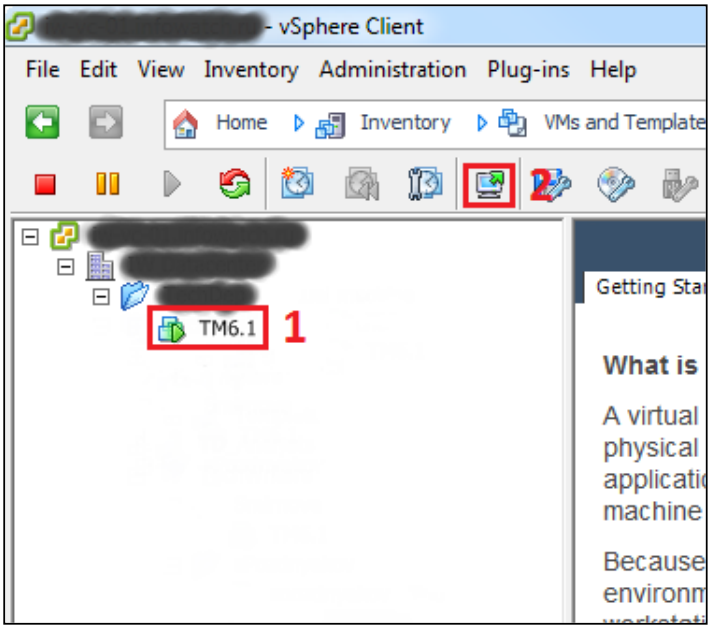
The update will be done through a console of the server being updated. A console (or a terminal) is a window of a Linux-based operating system where you can type commands in a text form - as strings. Depending on the server type, when started, the console may display general information on the server 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 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**.

```
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] ~]#
```

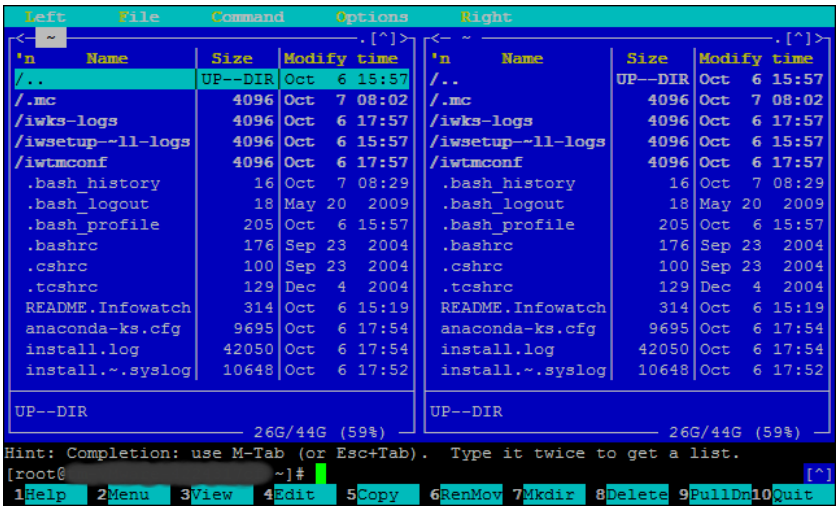
The screen will display the service information and (in the last line) an invitation to enter the command (command line).

> **Tip:**
>
> 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.
> 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 processes started are not to be interrupted and you may safely continue the System update.
Warning! 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 a specific screen with «name»;
- `exit` - exit screen (to be input within the screen window).

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

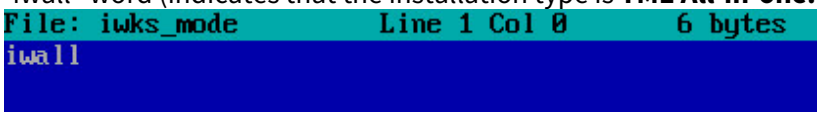


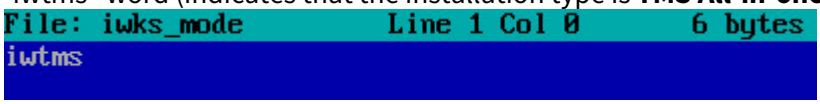
The screen will display a window of *Midnight Commander* file manager where you can view files. You can navigate in the file manager using keyboard arrows and the **Enter** key or with a mouse. Besides, you can enter commands at the command line which is displayed in the lower part of the screen (for 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.

     Press **F3**.
7. To see the number of Traffic Monitor version go to `/opt/iw/tm5/version`.
   Depending on Traffic Monitor version that will be updated together with the System, further steps can differ.
8. To exit the file manager (it is necessary for better commands executing) enter the command:
   `exit`

> **Warning!**
>
> Before running the installation make sure that the server complies with the OS and network settings requirements.

Depending on how you are going to update the System, choose the instruction:

- Updating the System over the installed one;

- The following instruction is **recommended** when updating the System from a version lower than 6.11:
  Updating system by reinstalling and restoring data from backup copy;
- Updating the System from version 6.11.xx to 6.11.yy.

Updating the System over the installed one

> **Warning**
>
> The OS Red Hat Enterprise Linux will be updated up to the 7.x version together with the System. To update the OS, please check the official instruction.
> We strongly recommend to back up the System, clone it and update on this particular testing computer.
> If Oracle DBMS is used in the System, before processing the update you should perform a database backup. When Oracle DBMS update is running, changes cannot be rollback.

To update the System, take the following steps:

1. Copy files into the `/root` directory:
   a. The files from InfoWatch Traffic Monitor distributive:
      - **`iwtm-installer-x.x.x.xxx-rhel7.run`** (where x.x.x.xxx is a number of build);
      - **`iwtm-postgresql-9.6.13-x.xx.x.tar.gz`**;
      - **`iwtm-oracle-12.2.0.1-x.xx.x.tar.gz`**;
      - **`iwtm-adp-x.xx.x.tar.gz`**.

   b. ISO-image of distributive disc of OS Red Hat Enterprise Linux 7.x.

   > **Note:**
   >
   > To make sure the ISO-image version of OS Red Hat Enterprise Linux 7.x distributive kit is correct, please check on official website the version number the System to be updated.

   Our example:
   - **`iwtm-installer-6.11.0.839-rhel7.run`** ;
   - **`iwtm-postgresql-9.6.13-6.11.0.tar.gz`** ;
   - **`iwtm-oracle-12.2.0.1-6.11.0.tar.gz`** ;
   - **`iwtm-adp-6.11.0.tar.gz`** ;
   - **`rhel-server-7.6-x86_64-dvd.iso`** .

2. To make the file **`iwtm-installer-x.x.x.xxx-rhel7.run`** executable, enter the command:
   `chmod u+x /root/iwtm-installer-x.x.x.xxx-rhel7.run`
   Our example command:
   `chmod u+x /root/iwtm-installer-6.11.0.839-rhel7.run`

Note:

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

3. Enter commands to stop interceptors:
```
service iwtm stopwait icap
service iwtm stopwait smtpd
service iwtm stopwait expressd
service iwtm stopwait sniffer
service iwtm stopwait xapi_xapi
service iwtm stopwait xapi_puppy
```
4. Enter the command to call the file manager:
```
mc
```
5. 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/
/opt/iw/tm5/queue/x2x/.db/
/opt/iw/tm5/queue/x2x/.in/
/opt/iw/tm5/queue/x2x/.out/
```
When all the events are processed, these directories should be empty.

Warning!

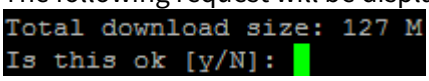
To continue the update, make sure that all specified directories are empty. Otherwise, we cannot guarantee that the System will be updated correctly and will operate properly after the update.
If for some reason, you cannot wait until the processing is complete, you can delete events from the queue; these 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.

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

7. To stop services of Traffic Monitor server, enter the command:
   `service iwtm stop && chkconfig iwtm off`
8. Depending on DBMS being used and Traffic Monitor version installed, enter the command to stop the DB:
   - For **Oracle DBMS**:
     - `service oracle stop && chkconfig oracle off`
   - For **PostgreSQL DBMS**:
     - `service postgresql-9.4 stop && chkconfig postgresql-9.4 off` (Traffic Monitor **6.9.x** version)
     - `service postgresql-9.6 stop && chkconfig postgresql-9.6 off` (Traffic Monitor **6.10.x** version)
9. Depending on Traffic Monitor version installed, enter the command:
   - `service php-fpm stop && chkconfig php-fpm off` (Traffic Monitor **6.9.x** version)
   - `service iwtm-php-fpm stop && chkconfig iwtm-php-fpm off` (Traffic Monitor **6.10.x** version)
10. Enter commands to stop services:
    ```
    service redis stop && chkconfig redis off
    service nginx stop && chkconfig nginx off
    service gearmand stop && chkconfig gearmand off
    service nagios stop && chkconfig nagios off
    ```
11. If you have Traffic Monitor **6.10.x** version installed, enter the command to stop the service:
    `service iwtm-consul stop && chkconfig iwtm-consul off`
12. To update packages enter the command:
    `yum upgrade --exclude=nagios`

    > **Warning!**
    >
    > To run the command at this step you should connect Red Hat Enterprise Linux 6 repositories having the latest updates installed.
    > Find how to work with repository in the guide on Red Hat Enterprise Linux official website.

    The following request will be displayed:

    To continue type **Y** and press **Enter**.
13. After packages updating is completed, enter the command to reboot the server:
    `reboot`
    Wait until the server is loaded and log in again. For this, take the steps 1-3 of the instruction before updating.
14. To install assistive utilities for updating, enter the command:
    ```
    yum -y install yum-utils redhat-upgrade-tool preupgrade-assistant
    preupgrade-assistant-ui preupgrade-assistant-el6toel7
    ```
    Wait until the installation is completed.
15. To disconnect repositories run the command:
    `yum-config-manager --disable \*`
16. Enter the command to clear the cash of package manager:
    `yum clean all`

17. Delete or disconnect Red Hat Enterprise Linux 6 repositories:
    - To delete repositories:
        a. Enter the command to call file manager:
           `mc`
        b. Go to directory `/etc/yum.repos.d/`;
        c. Open configuration files of the Red Hat Enterprise Linux 6 repositories;
           The `baseurl` parameters contain the addresses of directories of local repositories;
        d. Delete these directories and their content, then delete the configuration files in the directory `/etc/yum.repos.d/`;
        e. To exit the file manager enter the command:
           `exit`
    - To disconnect the repository, take one of the following steps:
        - Open for editing the repository configuration file stored in `/etc/yum.repos.d/`, in enabled parameter change 1 for 0 and save changes;
        - Delete repository configuration file from the directory `/etc/yum.repos.d/`.

18. To run the utility, checking the System before the update, enter the command:
    `preupg -v`
    The following request will be displayed:
    ```
    The Preupgrade Assistant is a diagnostics tool
    and does not perform the actual upgrade.
    Do you want to continue? [Y/n]
    ```
19. To continue, type **Y** and press **Enter**.
20. Wait until the utility completes the job. The results of checking appear in the report `/root/preupgrade/`**`result.html`** , created by the utility. Follow the recommendations from the report. For this, check the paragraph 1.1.3.3 of official instruction.
21. Delete the **dkms** package by running the command:
    `rpm -ev --nodeps dkms`

> **Warning!**
>
> Non_compliance may cause the OS updating error.

22. To run the updating utility, enter the command:
    `redhat-upgrade-tool --iso /root/rhel-server-7.x-x86_64-dvd.iso` (where 7.x is an edition of the OS Red Hat Enterprise Linux, up to which the System will be updated)
    Our example command:
    `redhat-upgrade-tool --iso /root/rhel-server-7.6-x86_64-dvd.iso`
    The following request will be displayed: `Continue with the upgrade [Y/N]?`
    To continue, type **Y** and press **Enter**.
    The following message will be displayed:
    ```
    HOOK-pkgdowngrades: INFO: done
    Finished. Reboot to start upgrade.
    ```

Warning!

In case OS Red Hat Enterprise Linux is updated to version **following after 7.6**, the message as follows can be displayed:

```
[            ~]# redhat-upgrade-tool --iso /root/rhel-server-7.7-x86_64-dvd.iso
setting up repos...
upgradeiso
upgradeiso/primary
The installed version of Preupgrade Assistant allows upgrade only to the system version 7.6.
```

The message is aimed to inform you about inability of operating system to be updated to the specified version. In this case, use ISO image of OS Red Hat Enterprise Linux distributive kit of the version which was specified in the message final part.

23. Enter the command to restart server:
    `reboot`
    The updating continues after server is rebooted.
24. Wait until the updated System is loaded and log in again. For this, take the steps 1-3 of the instruction before updating.
25. To update the configuration of Postfix mail server, enter the command:
    `postfix upgrade-configuration`
26. Enter the command to find and display the list of files with **.rpmnew** extension at the console:
    `find / -name "*rpmnew*" -print`
    If the files have been found, they should be correctly merged with configuration files (see "Merging configuration files").

Note:

To merge successfully the configuration files you should read the following articles on official site:

- "What are rpmnew & rpmsave files?";
- "Recommendations on handling of rpmnew and rpmsave files following Red Hat Enterpries Linux system update".

Warning!

Do not change **`web.conf`**, **`database.conf`**, **`consul.json`** files. It is also recommended not to change the file `/etc/nagios/`**`nagios.cfg`**.

27. Before continuing the update, connect the external and internal repositories Red Hat Enterprise Linux 7.
    You can check the instruction of the local repository setting on Red Hat Enterprise Linux official website.
28. Enter the command to go to the directory containing Traffic Monitor distributives:
    `cd /root`
29. If you are using **Oracle DBMS**, take the following steps:

a. Enter the command to stop DBMS Oracle:
`service oracle start`
b. Enter the command to run the Oracle update:
`bash ./iwtm-installer-x.x.x.xxx-rhel7.run -- --oracle-upgrade`
Our example command:
`bash ./iwtm-installer-6.11.0.839-rhel7.run -- --oracle-upgrade`
After Oracle successful update the following message appears:

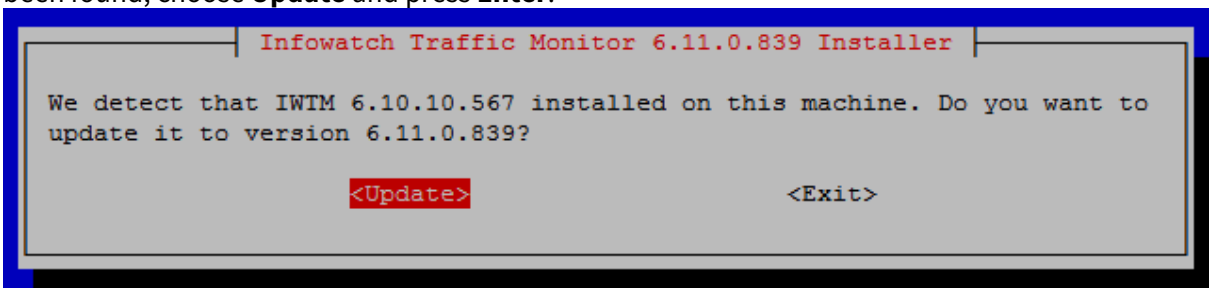
```
Tue Mar 19 17:53:12 MSK 2019 INFO: Oracle DB upgrades successfuly.
Tue Mar 19 17:53:12 MSK 2019 INFO: You can cleanup old Oracle installation with the folowing
 commands (Only after IWTM upgrade and checks!!!):
su - "oracle" -c "/u01/app/oracle/product/db_1/oui/bin/runInstaller -ignoreSysPrereqs -detac
hHome ORACLE_HOME=/u01/app/oracle/product/db_1"
su - "oracle" -c "rm -rf /u01/app/oracle/product/db_1 /u01/app/oracle/product/db_2/OPatch.ba
ckup"
su - "oracle" -c "rm -rf /home/oracle/oracle12c_distr"
```

> **Note:**
>
> Oracle DBMS upgrade may take a long time.
> **Approximate** timing to update 1 TB Oracle database:
> - DBMS Oracle will be updated in 60 minutes;
> - Oracle database scheme will be updated in 50 minutes.
>
> To perform the update, make sure there is 11 GB of free space in `ORACLE_HOME`, the default directory of which is `/u01/app/oracle`.
> The message saying that Oracle has been successfully upgraded also says that you can remove the previous Oracle version.
> You can remove it **only after** the System has been upgraded and all checks are completed.
> Before the removal, **be sure to check** that:
> - a new version is **not** installed in the `/u01/app/oracle/product/db_1` directory;
> - all services of the System are started and running;
> - the **System condition** tab of the TM Console does not contain errors;
> - the DB contains old events. To check this, create a query on the **Events** tab and specify the required interception date;
> - the DB receives new events.
>
> To remove the old version, follow commands from the message.

c. To convert password file to Oracle 12 format, please enter the command:
`su - oracle -c "orapwd file=${ORACLE_HOME}/dbs/orapwiwtm force=y format=12 input_file=${ORACLE_HOME}/dbs/orapwiwtm"`

30. Enter the command to update Traffic Monitor packages:
`bash ./iwtm-installer-x.x.x.xxx-rhel7.run`
Our example command:
`bash ./iwtm-installer-6.11.0.839-rhel7.run`
The installer will check the System before running and in case of non-compliance with requirements, it will interrupt the installation and display an error message. In this case, you need to correct the error and restart the update.

In the window that opens informing that an early version of the InfoWatch Traffic Monitor has been found, choose **Update** and press **Enter**:



31. If you are using **PostgreSQL DBMS**, and Traffic Monitor has been updated from the version **6.9.x**, do the following:
    a. Update PostgreSQL DBMS.
    b. Enter the command to switch to *postgres* user:
    `su - postgres`
    c. Enter the command to run the script (scenario) of the DB update:
    `bash /opt/iw/tm5/csw/postgres/update.sh`

    > **Note:**
    >
    > Database scheme update may take a long time.
    > **Example**: a database of size 1 TB will be updated in 95 minutes.
    > To perform the update, make sure there is 12 GB of free space in the root directory.

    d. Enter the command:
    `exit`
32. Enter the command to search and display the list of files with**.rpmnew** extension:
    `find / -name "*rpmnew*" -print`
    If mentioned files have been found, they should be correctly merged with configuration files (see "Merging Configuration Files").

    > **Warning!**
    >
    > Do not change **`web.conf`**, **`database.conf`**, **`consul.json`** files. It is also recommended not to change the file `/etc/nagios/`**`nagios.cfg`**.

33. Enter the command to call file manager again:
    `mc`
34. Go to the directory `/opt/iw/tm5/etc/scripts/` and make sure that there is a file **`iwssid.lua.upgrade`**. The System does not use the file **`iwssid.lua.update`**, as it is a backup in case the System is to be customised.
35. The file **`iwssid.lua`** should be `opt/iw/tm5/etc/scripts/` as well. We recommend to keep it as it is if it has not been edited before update.
    Otherwise, it should be correctly merged with the configuration file **`iwssid.lua.rpmnew`** (see "Merging configuration files").
36. To exit the file manager:
    `exit`

37. Enter the command to reboot server:
`reboot`
Wait until the server is loaded and log in again. For this, take the steps 1-3 of the instruction before the updating.

Warning!

After the start, Traffic Monitor connects to the database and loads the configuration file `cas_config.xml` from there. Depending on configuration size, file loading may take some time.
During this loading period, the System may record error messages in log files:

- /opt/iw/tm5/log/cas_config_compiler.log

Запись об ошибке вида

```
1 2019-10-07 17:00:57.351489 (3936:0x00007f4008de8880) [ERROR  ] : <Root>
Exception:.
Diagnostic information..
/sandbox/src/cas3/config/details/cas_factory.cpp(233): Throw in function bool
cas::CasConfigFactory::LoadXmlConfig(cas::ConfigCreator::Ptr&, const
boost::filesystem::path&) const
Dynamic exception type:
boost::exception_detail::clone_impl<cas::ExceptionCasConfig>
```

- /opt/iw/tm5/log/cas.log

Запись об ошибке вида

```
1 2019-10-03 17:39:13.348146 (14262:0x00007fe83892ba80) [WARNING] : <Root>
Prometheus server is off, therefore the statistics is unavailable. That's
what you wanted, isn't it?
2 2019-10-03 17:39:14.364655 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
Error when loading config of tech: Cannot open xml file with cas
configuration: etc/config/cas/cas_config.xml
3 2019-10-03 17:39:14.364856 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
failed to initialize thrift server
Diagnostic information.
/sandbox/src/cas3/handler.cpp(682): Throw in function
 cas::Handler::LoadedConfigData cas::Handler::GetLoadedConfigData(const
prop::Property&, const Ptr&)
Dynamic exception type:
boost::exception_detail::clone_impl<tech::ExceptionTechLoadConfig>
std::exception::what: Cannot open xml file with cas configuration: etc/
config/cas/cas_config.xml
```

After the configuration file has been successfully loaded, the System will stop recording error messages and will work in standard mode.

If the System continues to record error messages for a long time, check connection with the database.

38. Enter the command to delete Red Hat Enterprise Linux 6 packages:
`yum remove *.el6*`

> **Warning!**
>
> Before the deletion processing on display, you will see the list of packages to be removed and a query for removal. Please carefully check the list for packages starting with "**`iwtm-`**". Once you see any package, **cancel the deletion and miss this action**.

To delete the displayed list of packages, press **Y** on the keyboard and press **Enter**.

39. Enter the command to clear cash of packages manager.
`yum clean all`
40. Enter the command to clear cash:
`redis-cli flushall`
41. Enter the command to check start of processes:
`iwtm status`
The processes and their statuses will be displayed. Usually, the services `iw_qmover_client, iw_qmover_server` and `iw_image2text_fre_batch` are stopped, the rest of services are running. Thereby the strings should have the following endings: **"inactive (dead)"** for the services `iw_qmover_client,iw_qmover_server` and `iw_image2text_fre_batch` and **"active (running)"** for other services:

```
Service iw_bookworm.service is active (running); enabled state: loaded (enabled)
Service iw_x2db.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_x2x.service is active (running); enabled state: loaded (enabled)
Service iw_deliver.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_warpd.service is active (running); enabled state: loaded (enabled)
Service iw_licensed.service is active (running); enabled state: loaded (enabled)
Service iw_luaengined.service is active (running); enabled state: loaded (enabled)
Service iw_cas.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_analysis.service is active (running); enabled state: loaded (enabled)
Service iw_tech_tools.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_pas.service is active (running); enabled state: loaded (enabled)
Service iw_adlibitum.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_blackboard.service is active (running); enabled state: loaded (enabled)
Service iw_icap.service is active (running); enabled state: loaded (enabled)
Service iw_image2text_fre_batch.service is inactive (dead); enabled state: masked (bad)
Service iw_messed.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_http.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_icq.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_smtp.service is active (running); enabled state: loaded (enabled)
Service iw_sample_compiler.service is active (running); enabled state: loaded (enabled)
Service iw_smtpd.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_puppy.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_xapi.service is active (running); enabled state: loaded (enabled)
Service iw_system_check.service is active (running); enabled state: loaded (enabled)
Service iw_sniffer.service is active (running); enabled state: loaded (enabled)
Service iw_agent.service is active (running); enabled state: loaded (enabled)
Service iw_capstack.service is active (running); enabled state: loaded (enabled)
Service iw_configerator.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_indexer.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_kicker.service is active (running); enabled state: loaded (enabled)
Service iw_qmover_client.service is inactive (dead); enabled state: masked (bad)
Service iw_qmover_server.service is inactive (dead); enabled state: masked (bad)
Service iw_updater.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_is.service is active (running); enabled state: loaded (enabled)
```

Note:

If Crawler subsystem is a part of System, it is required to run the services of this subsystem (on Crawler server): `InfoWatch.Crawler.Scanner`, `InfoWatch.Crawler.Server`, `Consul Agent`. 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.

Traffic Monitor All-in-one server is updated. The System version shown in the management Console window **About the System** should be changed accordingly. If you have other systems or subsystems to be updated, check the instructions of the chapter.

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:

Clear the cash before starting, so the Console can be displayed correctly. Use your browser standard functionalities to perform the action.

Updating system by reinstalling and restoring data from backup copy

Warning!

We strongly recommend to back up the System, clone it and update on this particular testing machine. If Oracle DBMS is used in the System, before processing the update you should perform a database backup. When Oracle DBMS update is running, changes cannot be rollback.

The OS Red Hat Enterprise Linux 7.x will be installed during the System updating.

After installing OS Red Hat Enterprise Linux 7.x version, Traffic monitor configuration files should be set up again. We recommend saving them to perform additional configuration after the update.

During the System update, the following steps will be performed:

i. DB, indexes and configuration of iw_adlibitum service backup (Preparing for update).
ii. Installation of the OS Red Hat Enterprise Linux 7.x (The user follows the official instruction to install the OS).
iii. InfoWatch Traffic Monitor 6.11 installation.
iv. Data backup and DBMS update.

Note:

If Crawler subsystem is a part of System, it is required to run the services of this subsystem (on Crawler server): `InfoWatch.Crawler.Scanner, InfoWatch.Crawler.Server, Consul Agent`. 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**.

1. Enter commands to stop interceptors and `iw_indexer`:
```
service iwtm stopwait icap
service iwtm stopwait smtpd
service iwtm stopwait expressd
service iwtm stopwait sniffer
service iwtm stopwait xapi_xapi
service iwtm stopwait xapi_puppy
service iwtm stopwait indexer
```
2. Again, enter the command to call the file manager:
```
mc
```

3. 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/`
   `/opt/iw/tm5/queue/x2x/.db/`
   `/opt/iw/tm5/queue/x2x/.in/`
   `/opt/iw/tm5/queue/x2x/.out/`
   When all the events are processed, these directories should be empty.

   > **Warning!**
   >
   > 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; these 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.

4. To exit the file manager (is required to better control command execution), enter the command:
   `exit`
5. To stop services of Traffic Monitor server, enter the command:
   `service iwtm stop && chkconfig iwtm off`
6. Depending on Traffic Monitor version, enter the command:
   - `service php-fpm stop && chkconfig php-fpm off` (Traffic Monitor **6.9.x** version)
   - `service iwtm-php-fpm stop && chkconfig iwtm-php-fpm off` (Traffic Monitor **6.10.x** version)
7. Connect to DB and check the number of events it contains:
   a. For Oracle DBMS
      i. To connect to DB server, enter the commands using a console:
         `su - oracle`
         `sqlplus <scheme_owner_data> where <scheme_owner_data>` - login and password of DB scheme owner. Default data are available on the Accounts page.
         Example:
         `su - oracle`
         `sqlplus iwtm/xxXX1234`
      ii. Then enter the command:
         `select count(1) from object;`

iii. To disconnect from DB, enter the command:
exit
iv. To switch to other user, enter the command:
`exit`

b. For PostgreSQL DBMS
i. To connect to DB server, enter the commands using a console:
```
su - iwtm
psql postgres iwtm -p 5433
```
ii. Then enter the command:
```
select count(1) from object;
```
iii. To exit, enter the command:
`\q`
iv. Enter the command:
`exit`

8. To stop `searchd` processes enter the command:
`killall searchd`
To verify, enter the command:
`ps -ef | grep searchd | grep -v grep`
The command should not respond with running processes.
9. Run backup:

> **Warning!**
>
> To back up successfully, you should copy the files with their **rights**, **users** and **groups** saved.
> To do this, copy files into the **Linux file system** (ex., Ext4 or XFS).
> Store backup copies either on a separate section of server or on another server, or on external device.
> Make sure that the data will not be lost when installing the OS Red Hat Enterprise Linux 7.x.
> After installation, backup copies should be copied into their **original directories**, and **rights**, **users** and **groups** should not be changed.

a. Depending on DBMS being used and the Traffic Monitor version installed, enter the command to stop the DB:
- For **Oracle DBMS**:
  - `service oracle stop && chkconfig oracle off`
- For **PostgreSQL DBMS**:
  - `service postgresql-9.4 stop && chkconfig postgresql-9.4 off` (Traffic Monitor **6.9.x** version)
  - `service postgresql-9.6 stop && chkconfig postgresql-9.6 off` (Traffic Monitor **6.10.x** version)

b. Make DB backup. By default, DB is stored in the directories **`/u01, /u02`** etc. Copy DB into another section of sever or on another server, or on an external device.

> **Note:**
>
> To specify directories keeping DB, check the file:
> - /opt/iw/tm5/csw/oracle/database.conf (**DBMS Oracle**)
> - /opt/iw/tm5/csw/postgres/database.conf (**DBMS PostgreSQL**)

c. Make indexes backup. To do this:
   i. Enter the command to call the file manager:
   `sudo mc`
   ii. Go to `/opt/iw/tm5/etc directory` and open file **`indexer.conf`** in view mode.
   iii. The path to indexes directory is defined in `"SphinxBaseDir"` parameter. A relative path to indexes archive is defined in `"ArchiveDir"` parameter. Archive path is defined relatively to content of `"NookDir"` parameter.
   Copy indexes directories and indexes archive into either other section of server, or other server, or external device.

d. Make `iw_adlibitum` service configuration backup. To do this, take the following steps:
   i. Go to `/opt/iw/tm5/etc` directory and open file **`adlibitum.conf`** in view mode.
   ii. A relative path to the directory containing `iw_adlibitum` service configuration is defined in `"ConfigDir"` parameter. The path is defined relatively to the content of `"NookDir"` parameter.
   Copy configuration directory into either other section of the server, or another server, or external device.
   iii. To exit the file manager (is required to better control command execution), enter the command:
   `exit`

10. Install the OS Red Hat Enterprise Linux 7.x on server. To do this, check official instruction.
11. Install Traffic Monitor version 6.11.

> **Warning!**
>
> If backup copies are kept on external storages, do not connect them during the installation.
> It should be done right before DB backup and update.

12. To stop service enter the commands:
    `iwtm stop`
    `service iwtm-php-fpm stop service nagios stop`
13. Depending on DBMS you are using, enter the command to stop the DB:
    - `service oracle stop` (**Oracle DBMS)**
    - `service postgresql-9.6 stop` **(PostgreSQL DBMS)**
14. To stop `searchd` processes, enter the command:
    `killall searchd`
    To verify, enter the command:

```
ps -ef | grep searchd | grep -v grep
```
Command response should not have running processes.

15. Copy DB backup copy that was created at step 9b into the original directory.
16. When using Oracle DBMS, please make sure the **uid** ID (**oracle** user) and **gid** ID (**oinstall** group) have the value equal to 1001:
    a. To find out the **uid** and **gid** ID values, please run the command:
    ```
    id oracle
    ```
    b. Check the rights as per /u01 and /u02 directories:
    ```
    ls -l /u01
    ls -l /u02
    ```
    c. In case the rights are incorrect, search all these rights as per this owner in files and directories and replace it as follows:
    ```
    find /u01 -uid 501 -exec chown -v -h 1001 '{}' \;
    find /u01 -gid 501 -exec chgrp -v 1001 '{}' \;
    find /u02 -uid 501 -exec chown -v -h 1001 '{}' \;
    find /u02 -gid 501 -exec chgrp -v 1001 '{}' \;
    ```
17. Enter command to shift to Traffic Monitor distributive's directory:
    ```
    cd /root
    ```
18. Update DBMS:
    a. For Oracle DBMS
        i. Enter command to start Oracle:
        ```
        service oracle start
        ```
        ii. Enter command to start Oracle update:
        ```
        bash ./iwtm-installer-x.x.x.xxx-rhel7.run -- --oracle-upgrade
        ```
        Our example command:
        ```
        bash ./iwtm-installer-6.11.0.630-rhel7.run -- --oracle-upgrade
        ```
        In case of successful update the following message will be displayed:

```
Tue Mar 19 17:53:12 MSK 2019 INFO: Oracle DB upgrades successfuly.
Tue Mar 19 17:53:12 MSK 2019 INFO: You can cleanup old Oracle installation with the folowing
 commands (Only after IWTM upgrade and checks!!!):
su - "oracle" -c "/u01/app/oracle/product/db_1/oui/bin/runInstaller -ignoreSysPrereqs -detac
hHome ORACLE_HOME=/u01/app/oracle/product/db_1"
su - "oracle" -c "rm -rf /u01/app/oracle/product/db_1 /u01/app/oracle/product/db_2/OPatch.ba
ckup"
su - "oracle" -c "rm -rf /home/oracle/oracle12c_distr"
```

> **Note:**
>
> Oracle DBMS upgrade may take a long time.
> **Approximate** timing to update 1 TB Oracle database:
> - DBMS Oracle will be updated in 60 minutes;
> - The Oracle database scheme will be updated in 50 minutes.
>
> To perform the update, make sure there is 11 GB of free space in `ORACLE_HOME`, the default directory of which is `/u01/app/oracle`.
> The message saying that Oracle has been successfully upgraded also says that you can remove the previous Oracle version.
> You can remove it **only after** the System has been upgraded and all checks are completed.
> Before the removal, **be sure to check** that:

- a new version is **not** installed in the `/u01/app/oracle/product/db_1` directory;
- all services of the System are started and running;
- the **System condition** tab of the TM Console does not contain errors;
- the DB contains old events. To check this, create a query on the **Events** tab and specify the required interception date;
- the DB receives new events.

To remove the old version, follow commands from the message.

iii. Enter the command to shift to directory, containing the script (scenario) of DB scheme update.
```
cd /opt/iw/tm5/csw/oracle
```
iv. Enter the command to run the script:
```
su --command "/opt/iw/tm5/csw/oracle/update.sh" oracle
```
v. To convert password file to Oracle 12 format, please enter the command:
```
su - oracle -c "orapwd file=${ORACLE_HOME}/dbs/orapwiwtm force=y
format=12 input_file=${ORACLE_HOME}/dbs/orapwiwtm"
```

b. For PostgreSQL DBMS

i. If System updates from version **6.9.x**:
1. Run PostgreSQL DBMS update.
2. Enter command to run script (scenario) of the DB scheme update:
```
su --command "/opt/iw/tm5/csw/postgres/update.sh" postgres
```

ii. If System updates from version **6.10.x**:
1. Enter command to run **PostgreSQL**:
```
service postgresql-9.6 start
```
2. Run command:
```
su --command "/usr/pgsql-9.6/bin/psql -d postgres -p 5433 -
f /opt/iw/tm5/etc/update_psql_commands" postgres
```
3. Enter command to shift to directory containing the script (scenario) of DB scheme update:
```
cd /opt/iw/tm5/csw/postgres
```
4. Enter the command to run the script:
```
su --command "/opt/iw/tm5/csw/postgres/update.sh" postgres
```

Note:

The database scheme update may take a long time.
Example: a database of size 1 TB will be updated in 95 minutes.
To perform the update, make sure there is 12 GB of free space in the root directory.

19. Perform step 7 of the instruction to compare the number of events in DB before and after update.
20. Copy backup copies that were created at step 9b and 9c, into original directories and files.
If original directory is not a default one, it needs to be indicated in the appropriate sections of configuration files (see steps 10b and 10c).
21. Run the commands:

```
sudo -u iwtm touch /opt/iw/tm5/www/backend/protected/runtime/
first_run
iwtm restart kicker
```

22. Enter command to reboot server:
    `reboot`
    Wait until server loading is completed and log in again by performing steps 1-3 of the instruction before updating.
23. Enter command to clear cash:
    `redis-cli flushall`
24. Enter the command to test processes' start:
    `iwtm status`
    List of processes and their statuses will be displayed. Usually, the services `iw_qmover_client`, `iw_qmover_server` and `iw_image2text_fre_batch` are stopped, the rest of services are running. Thereby the strings should have the following endings: **"inactive (dead)"** for the services `iw_qmover_client`,`iw_qmover_server` and `iw_image2text_fre_batch` and **"active (running)"** for other services:

```
Service iw_bookworm.service is active (running); enabled state: loaded (enabled)
Service iw_x2db.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_x2x.service is active (running); enabled state: loaded (enabled)
Service iw_deliver.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_warpd.service is active (running); enabled state: loaded (enabled)
Service iw_licensed.service is active (running); enabled state: loaded (enabled)
Service iw_luaengined.service is active (running); enabled state: loaded (enabled)
Service iw_cas.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_analysis.service is active (running); enabled state: loaded (enabled)
Service iw_tech_tools.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_pas.service is active (running); enabled state: loaded (enabled)
Service iw_adlibitum.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_blackboard.service is active (running); enabled state: loaded (enabled)
Service iw_icap.service is active (running); enabled state: loaded (enabled)
Service iw_image2text_fre_batch.service is inactive (dead); enabled state: masked (bad)
Service iw_messed.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_http.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_icq.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_smtp.service is active (running); enabled state: loaded (enabled)
Service iw_sample_compiler.service is active (running); enabled state: loaded (enabled)
Service iw_smtpd.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_puppy.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_xapi.service is active (running); enabled state: loaded (enabled)
Service iw_system_check.service is active (running); enabled state: loaded (enabled)
Service iw_sniffer.service is active (running); enabled state: loaded (enabled)
Service iw_agent.service is active (running); enabled state: loaded (enabled)
Service iw_capstack.service is active (running); enabled state: loaded (enabled)
Service iw_configerator.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_indexer.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_kicker.service is active (running); enabled state: loaded (enabled)
Service iw_qmover_client.service is inactive (dead); enabled state: masked (bad)
Service iw_qmover_server.service is inactive (dead); enabled state: masked (bad)
Service iw_updater.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_is.service is active (running); enabled state: loaded (enabled)
```

Note:

If the Crawler subsystem is a part of the System, it is required to run 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. The System version in the **About the System** 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.

Updating the System from version 6.11.xx to 6.11.yy

Warning

We strongly recommend to back up the System, clone it and update on this particular testing computer.

To update the System, take the following steps:

1. Copy the files from InfoWatch Traffic Monitor distributive into the `/root` directory:
   - **`iwtm-installer-x.x.x.xxx-rhel7.run`** (where x.x.x.xxx is a number of build);
   - **`iwtm-postgresql-9.6.13-x.xx.x.tar.gz`**;
   - **`iwtm-oracle-12.2.0.1-x.xx.x.tar.gz`**;
   - **`iwtm-adp-x.xx.x.tar.gz`**.

   Our example:
   - **`iwtm-installer-6.11.2.1032-rhel7.run`**;
   - **`iwtm-postgresql-9.6.13-6.11.2.tar.gz`**;
   - **`iwtm-oracle-12.2.0.1-6.11.2.tar.gz`**;
   - **`iwtm-adp-6.11.2.tar.gz`**.

   Note:

   If Crawler subsystem is a part of the System, it is required to stop the services of this subsystem (on Crawler server): `InfoWatch.Crawler.Scanner`,

`InfoWatch.Crawler.Server, Consul Agent`. This is to be done on the server, where the subsystem is installed using Windows standard tools: **Start** - **Control Panel** - **Administrative Tools** - **Services**, then select the service in the list and click **Stop service**.

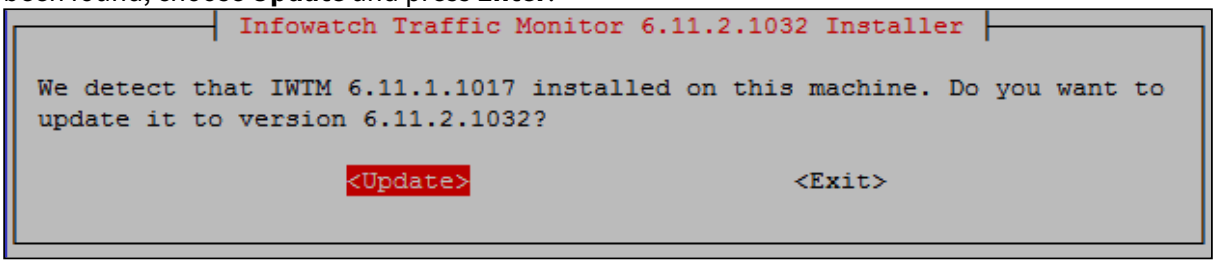
2. Enter commands to stop interceptors:
   ```
   iwtm stop icap
   iwtm stop smtpd
   iwtm stop sniffer
   iwtm stop xapi_xapi
   iwtm stop xapi_puppy
   ```
3. Enter command to call the file manager:
   ```
   mc
   ```
4. Wait until all events which are in the queue for processing are processed. Events 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/
   /opt/iw/tm5/queue/x2x/.db/
   /opt/iw/tm5/queue/x2x/.in/
   /opt/iw/tm5/queue/x2x/.out/
   ```
   When all the events are processed, these directories should be empty.

   Warning!

   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; these 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.

5. To exit the file manager (is required to better control command execution), enter the command:
   ```
   exit
   ```
6. To stop services of Traffic Monitor server, enter the command:
   ```
   iwtm stop
   ```
7. Depending on DBMS being used enter the command to stop the DB:
   - For **Oracle DBMS**:
     ```
     service oracle stop
     ```
   - For **PostgreSQL DBMS**:
     ```
     service postgresql-9.6 stop
     ```

8. Enter commands to stop services:
   ```
   systemctl stop iwtm-php-fpm
   systemctl stop nginx
   systemctl stop nagios
   systemctl stop iwtm-consul
   ```
9. Connect the external and internal repositories Red Hat Enterprise Linux 7.
   You can check the instruction of local repository setting on Red Hat Enterprise Linux official website.
10. To update packages enter the command:
    ```
    yum upgrade
    ```
    The following request will be displayed:
    ```
    Total download size: 127 M
    Is this ok [y/N]:
    ```
    To continue type **Y** and press **Enter**.
11. Enter the command to go to the directory containing Traffic Monitor distributives:
    ```
    cd /root
    ```
12. Enter the command to update Traffic Monitor packages:
    ```
    bash ./iwtm-installer-x.x.x.xxx-rhel7.run
    ```
    Our example command:
    ```
    bash ./iwtm-installer-6.11.0.839-rhel7.run
    ```
    The installer will check the System before running and in case of non-compliance with requirements, it will interrupt the installation and display an error message. In this case you need to correct the error and restart the update.
    In the window that opens informing that an early version of the InfoWatch Traffic Monitor has been found, choose **Update** and press **Enter**:



Please wait until the packages update is complete.

> **Note:**
>
> The database scheme update may take a long time.
> **Example**: for database of size 1 TB - above 30 minutes.
> To perform the update, make sure:
> - There is 11 GB of free space in `ORACLE_HOME`, the default directory of which is `/u01/app/oracle` - for **Oracle DBMS**;
> - There is 12 GB of free space in the root directory - for **PostgreSQL DBMS**.
>
> The message saying that Oracle has been successfully upgraded also says that you can remove the previous Oracle version.
> You can remove it **only after** the System has been upgraded and all checks are completed.
> Before the removal, **be sure to check** that:
> - a new version is **not** installed in the `/u01/app/oracle/product/db_1` directory;

- all services of the System are started and running;
- the **System condition** tab of the TM Console does not contain errors;
- the DB contains old events. To check this, create a query on the **Events** tab and specify the required interception date;
- the DB receives new events.

To remove the old version, follow commands from the message.

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

> **Note:**
>
> To merge successfully the configuration files you should read the following articles on official site:
> - "What are rpmnew & rpmsave files?";
> - "Recommendations on handling of rpmnew and rpmsave files following Red Hat Enterpries Linux system update".

14. Enter the command to call the file manager again:
`mc`
15. Go to directory `/opt/iw/tm5/etc/scripts/` and make sure that there is a file **`iwssid.lua.upgrade`**. The System does not use the file **`iwssid.lua.update`**, as it is a backup in case the System is to be customised.
16. The file **`iwssid.lua`** should be `opt/iw/tm5/etc/scripts/` as well. We recommend to keep it as it is, if it has not been edited before update.
Otherwise, it should be correctly merged with configuration file **`iwssid.lua.rpmnew`** (see "Merging configuration files").
17. To exit the file manager:
`exit`
18. Enter the command to reboot the server:
`reboot`
Wait until server is loaded and log in again. For this, take the steps 1-3 of the instruction before the updating.

> **Warning!**
>
> After the start, Traffic Monitor connects to the database and loads the configuration file `cas_config.xml` from there. Depending on configuration size, file loading may take some time.
> During this loading period, the System may record error messages in log files:
> - /opt/iw/tm5/log/cas_config_compiler.log

Запись об ошибке вида

```
1 2019-10-07 17:00:57.351489 (3936:0x00007f4008de8880) [ERROR  ] : <Root>
Exception:.
Diagnostic information..
/sandbox/src/cas3/config/details/cas_factory.cpp(233): Throw in function bool
cas::CasConfigFactory::LoadXmlConfig(cas::ConfigCreator::Ptr&, const
boost::filesystem::path&) const
Dynamic exception type:
boost::exception_detail::clone_impl<cas::ExceptionCasConfig>
```

- /opt/iw/tm5/log/cas.log

Запись об ошибке вида

```
1 2019-10-03 17:39:13.348146 (14262:0x00007fe83892ba80) [WARNING] : <Root>
Prometheus server is off, therefore the statistics is unavailable. That's
what you wanted, isn't it?
2 2019-10-03 17:39:14.364655 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
Error when loading config of tech: Cannot open xml file with cas
configuration: etc/config/cas/cas_config.xml
3 2019-10-03 17:39:14.364856 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
failed to initialize thrift server
Diagnostic information.
/sandbox/src/cas3/handler.cpp(682): Throw in function
 cas::Handler::LoadedConfigData cas::Handler::GetLoadedConfigData(const
prop::Property&, const Ptr&)
Dynamic exception type:
boost::exception_detail::clone_impl<tech::ExceptionTechLoadConfig>
std::exception::what: Cannot open xml file with cas configuration: etc/
config/cas/cas_config.xml
```

After the configuration file has been successfully loaded, the System will stop recording error messages and will work in standard mode.
If the System continues to record error messages for a long time, check connection with the database.

19. Enter the command to clear cash of packages manager.
    `yum clean all`
20. Enter the command to clear cash:
    `redis-cli flushall`
21. Enter the command to check start of processes:
    `iwtm status`
    The processes and their statuses will be displayed. Usually, the services `iw_qmover_client, iw_qmover_server` and `iw_image2text_fre_batch` are stopped, the rest of services are running. Thereby the strings should have the following endings: **"inactive (dead)"** for the
    services `iw_qmover_client`,`iw_qmover_server` and `iw_image2text_fre_batch` and **"active (running)"** for other services:

```
Service iw_bookworm.service is active (running); enabled state: loaded (enabled)
Service iw_x2db.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_x2x.service is active (running); enabled state: loaded (enabled)
Service iw_deliver.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_warpd.service is active (running); enabled state: loaded (enabled)
Service iw_licensed.service is active (running); enabled state: loaded (enabled)
Service iw_luaengined.service is active (running); enabled state: loaded (enabled)
Service iw_cas.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_analysis.service is active (running); enabled state: loaded (enabled)
Service iw_tech_tools.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_pas.service is active (running); enabled state: loaded (enabled)
Service iw_adlibitum.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_blackboard.service is active (running); enabled state: loaded (enabled)
Service iw_icap.service is active (running); enabled state: loaded (enabled)
Service iw_image2text_fre_batch.service is inactive (dead); enabled state: masked (bad)
Service iw_messed.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_http.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_icq.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_smtp.service is active (running); enabled state: loaded (enabled)
Service iw_sample_compiler.service is active (running); enabled state: loaded (enabled)
Service iw_smtpd.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_puppy.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_xapi.service is active (running); enabled state: loaded (enabled)
Service iw_system_check.service is active (running); enabled state: loaded (enabled)
Service iw_sniffer.service is active (running); enabled state: loaded (enabled)
Service iw_agent.service is active (running); enabled state: loaded (enabled)
Service iw_capstack.service is active (running); enabled state: loaded (enabled)
Service iw_configerator.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_indexer.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_kicker.service is active (running); enabled state: loaded (enabled)
Service iw_qmover_client.service is inactive (dead); enabled state: masked (bad)
Service iw_qmover_server.service is inactive (dead); enabled state: masked (bad)
Service iw_updater.service is activating (auto-restart); enabled state: loaded (enabled)
Service iw_is.service is active (running); enabled state: loaded (enabled)
```

Note:

If Crawler subsystem is a part of System, it is required to run the services of this subsystem (on Crawler server): `InfoWatch.Crawler.Scanner`, `InfoWatch.Crawler.Server`, `Consul Agent`. 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.

Traffic Monitor All-in-one server is updated. The System version shown in the management Console window **About the System** should be changed accordingly. If you have other systems or subsystems to be updated, check the instructions of the chapter.

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:

Clear the cash before starting, so the Console can be displayed correctly. Use your browser standard functionalities to perform the action.

4.2 Updating TM in case of Distributed Installation

Warning!

Before updating Traffic Monitor server to version 6.11 it is strongly recommended to update DM server first.

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 in 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 processes started are not to be interrupted and you may safely continue the System update.

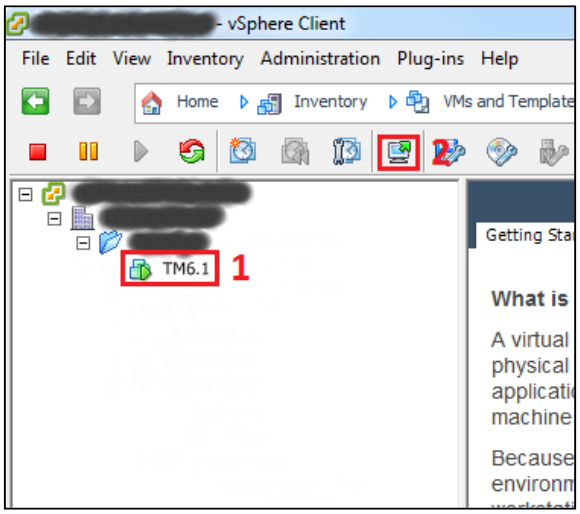
Warning! Using Screen is highly recommended when working with DB and updating DBMS.

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).

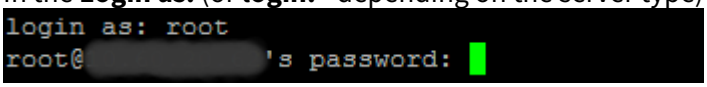
Before updating the System, take the following steps on each server to be updated:

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).

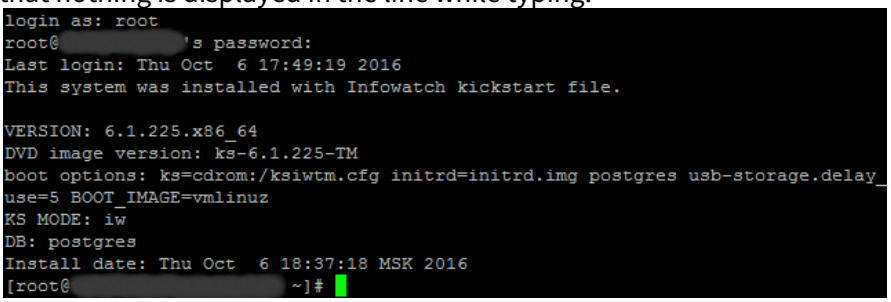


   A window with the server console will open.

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



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.



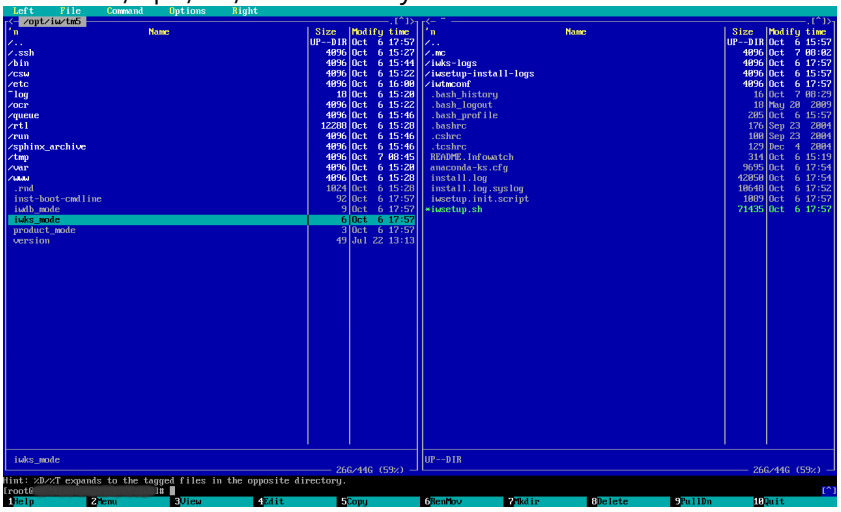
   The screen will display the service information and, in the last line, an invitation to enter the command (command line).

> **Tip:**
>
> 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* the 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 that will differ depending on a server type:
   - "`iwtm`" word (defines the installation type **TME Node server**);
   - "`iwdb`" (defines the installation type **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:
> `iwtm` for Traffic Monitor server (**TME Node server**);
> `iwdb` for DBMS server (**TME DB server**).
> 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.

   Press **F3**.
7. To see the number of Traffic Monitor version installed go to /opt/iw/tm5/**version.**
   Depending on Traffic Monitor version that will be updated together with the System, further actions can differ.
8. If you have a Traffic monitor **6.9.x** installed, take the following steps to prepare for the update of the System over the installed one:
   a. On **DBMS server (TME DB Server)**:
      i. Go to `/opt/iw/tm5/etc` directory, position the cursor on **serman.conf** file and press **F3**.
      ii. 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_client.conf** file and press **F4**.
      ii. Find `SermanHost` block.
      Compare its value with the 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 servers (TME Node Server)** with the 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 close viewing file **serman.conf**.

9. To exit the file manager (it is necessary for better commands executing) enter the command:

```
exit
```

> **Warning!**
>
> Before running the installation make sure that the server complies with the OS and network settings requirements

Depending on the System update's type, choose the instruction:

- Updating the System over the installed one;
- The following instruction is **recommended** when updating the System from a version lower than 6.11:
  Updating system by reinstalling and restoring data from backup copy;
- Updating the System from version 6.11.xx to 6.11.yy.

Updating the System over the installed one

> **Warning!**
>
> The OS Red Hat Enterprise Linux will be updated up to version 7.x together with the System. To update the OS, please check the official instruction.
>
> We strongly recommend to back up the System, clone it and update on this particular testing machine. If Oracle DBMS is used in the System, before processing the update you should perform a database backup. When Oracle DBMS update is running, changes cannot be rollback.

Updating steps look as follows:

Step 1. Upgating all TM servers (TME Node Server)
Step 2. DBMS server update (TME DB Server)
Step 3. Checking Consul cluster
Step 4. Healthckeck of internal services of System
Step 5. Finishing update on DBMS server (TME DB Server)
Step 6. Restart all TM servers (TME Node Server)

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

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

1. Copy into `/root` directory:
   a. The files from the InfoWatch Traffic Monitor distributive:
      - **iwtm-installer-x.x.x.xxx-rhel7.run** (where x.x.x.xxx is a number of build);
      - **iwtm-postgresql-9.6.13-x.xx.x.tar.gz**;
      - **iwtm-oracle-12.2.0.1-x.xx.x.tar.gz**;
      - **iwtm-adp-x.xx.x.tar.gz**.

   b. ISO- image of distributive disc of OS Red Hat Enterprise Linux 7.x.

> **Note:**
>
> To make sure the ISO-image version of OS Red Hat Enterprise Linux 7.x distributive kit is correct, please check on the official website the version number the System to be updated.

Example:

- **iwtm-installer-6.11.0.839-rhel7.run**;
- **iwtm-postgresql-9.6.13-6.11.0.tar.gz**;
- **iwtm-oracle-12.2.0.1-6.11.0.tar.gz**;
- **iwtm-adp-6.11.0.tar.gz;**
- **rhel-server-7.6-x86_64-dvd.iso**.

2. To make the **iwtm-installer-x.x.x.xxx-rhel7.run** file executable, enter the command:
`chmod u+x /root/iwtm-installer-x.x.x.xxx-rhel7.run`
Our example command:
`chmod u+x /root/iwtm-installer-6.11.0.839-rhel7.run`
3. > **Note:**
>
> If Crawler subsystem is a part of System, it is required to stop the services of this subsystem (on Crawler server): `InfoWatch.Crawler.Scanner`, `InfoWatch.Crawler.Server`, `Consul Agent`. 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**.

If updating from the 6.9.x version, run the commands:

a. Run the command:
`mkdir -p /mnt/rhel-dvd`
Directory `/mnt/rhel-dvd` will be created
b. Connect the disk with a **current version** of Traffic Monitor distributive to the server (see "Updating System", step 2).
c. Enter command:
`mount /dev/cdrom /mnt/rhel-dvd`

> **Note:**
>
> There is a space between parts "/dev/cdrom" and "/mnt/rhel-dvd" of the command.

Distributive disk located in `/dev/cdrom` will be connected to the `/mnt/rhel-dvd` directory as a repository.

d. Go to `/mnt/rhel-dvd` directory and make sure that files and folders are there. If the directory is empty, repeat steps b and c.
e. Enter command:
`yum install iwtm-qatools`

Before loading packages needed for installation, the following request will be displayed

```
================================================================================
================================================
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**.

f. After the package is installed, enter the command:
`umount /mnt/rhel-dvd`

g. Disconnect disk with a **current version** of Traffic Monitor distributive from the server.

h. To update, it is necessary to get a file with node IP-addresses (file name - **sd_nodes.out**). For this, run installer .run with a parameter:

If there are 2 nodes (TM server and DBMS):	`bash /root/iwtm-installer-x.x.x.xxx-rhel7.run -- --before-upgrade`
If there are more than 2 nodes:	`bash /root/iwtm-installer-x.x.x.xxx-rhel7.run -- --before-upgrade --tm_nodes_count=<nodes number>`

where `<nodes_number>` - the number of all servers, including the DBMS server.
Our example command:
`bash /root/iwtm-installer-6.11.0.839-rhel7.run -- --before-upgrade`
Example of console entry:

```
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
```

i. Copy file **sd_nodes.out** into all the nodes that were indicated, excluding the particular one it was created in.
Run command:
`scp /opt/iw/tm5/tmp/sd_nodes.out <node_address>:/opt/iw/tm5/tmp/sd_nodes.out`

where `<node_address>` is the IP-address or domain name of the node, which the **sd_nodes.out** file should be copied into.
Check the previous step and find that the console displays commands to copy the **sd_nodes.out** file to all necessary IP-addresses.
Our example command:
`scp /opt/iw/tm5/tmp/sd_nodes.out 10.20.30.40:/opt/iw/tm5/tmp/sd_nodes.out`

As copy command is entered, the following request will be displayed:

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

To continue type **yes** and press **Enter**.
Then enter the password of the target node and press **Enter**.

> **Warning!**
>
> Make sure that file **sd_nodes.out** is located in `/opt/iw/tm5/tmp` directory on all servers to be updated, including DBMS. Otherwise, move the file there.

> **Note:**
>
> Perform steps a-h on one node only. You can choose any node.

4. Enter commands to stop interceptors:
```
service iwtm stopwait icap
service iwtm stopwait smtpd
service iwtm stopwait expressd
service iwtm stopwait sniffer
service iwtm stopwait xapi_xapi
service iwtm stopwait xapi_puppy
```
5. Again, enter the command to call the file manager:
```
mc
```

6. 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/`
   `/opt/iw/tm5/queue/x2x/.db/`
   `/opt/iw/tm5/queue/x2x/.in/`
   `/opt/iw/tm5/queue/x2x/.out/`
   When all the events are processed, these directories should be empty.

   > **Warning!**
   >
   > Before continuing 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.

7. To exit the file manager (is required to better control command execution), enter the command:
   `exit`
8. To stop Traffic Monitor services enter the command:
   `service iwtm stop && chkconfig iwtm off`
9. Depending on Traffic Monitor version installed, enter the command:
   - `service php-fpm stop && chkconfig php-fpm off` (Traffic Monitor **6.9.x** version)
   - `service iwtm-php-fpm stop && chkconfig iwtm-php-fpm off` (Traffic Monitor **6.10.x** version)
10. Enter commands to stop the services:
    `service redis stop && chkconfig redis off`
    `service nginx stop && chkconfig nginx off`
    `service gearmand stop && chkconfig gearmand off`
    `service nagios stop && chkconfig nagios off`
11. In the case of Traffic Monitor **6.10.x** version installed, enter the command to stop the service:
    `service iwtm-consul stop && chkconfig iwtm-consul off`
12. To update packages enter the command:
    `yum upgrade --exclude=nagios`

> **Warning!**
>
> Red Hat Enterprise Linux 6 repositories with the latest updates should be connected to run the command at this step.
> Find how to work with the repository in the guide on Red Hat Enterprise Linux official website.

The following request will be displayed:

```
Total download size: 127 M
Is this ok [y/N]:
```

To continue, type **Y** and press **Enter**.

13. After packages are updated, enter the command to reboot the server:
    `reboot`
    Wait until the server is loaded and log in again by taking steps 1-3 of the instruction before updating.
14. To install assistive installation utilities, enter the command:
    `yum -y install yum-utils redhat-upgrade-tool preupgrade-assistant preupgrade-assistant-ui preupgrade-assistant-el6toel7`
    Wait until utilities are installed.
15. To disconnect repositories enter the command:
    `yum-config-manager --disable \*`
16. Enter the command to clear cash of packages manager:
    `yum clean all`
17. Delete or disconnect Red Hat Enterprise Linux 6 repositories:
    - To delete repositories:
        a. Enter the command to call the file manager:
           `mc`
        b. Go to `/etc/yum.repos.d/` directory;
        c. Open configuration files of Red Hat Enterprise Linux 6 repositories;
           `baseurl parameter` contains directories' addresses of local repositories;
        d. Delete the directories and their content, then delete configuration files in `/etc/yum.repos.d/` directory;
        e. To exit the file manager, enter the command:
           `exit`
    - To disconnect repository perform one of the following steps:
        - Open repository configuration file located in `/etc/yum.repos.d/` directory in editing mode, in enabled parameter, change 1 for 0 and save changes;
        - Delete repository configuration file in `/etc/yum.repos.d/` directory.

18. To run utility, checking system before the update, enter the command:
    `preupg -v`
    The following request will be displayed:

```
The Preupgrade Assistant is a diagnostics tool
and does not perform the actual upgrade.
Do you want to continue? [Y/n]
```

    To continue, type **Y** and press **Enter**.
19. Wait until utility completes the job. It will create a report `/root/preupgrade/result.html` containing checking results.
    Follow the report recommendations. For this, check paragraph 1.1.3.3 of the official instruction.
20. Delete the **dkms** package by running the command:
    `rpm -ev --nodeps dkms`

> **Warning!**
>
> The command is used on TM servers only (TME Node Server).
> Non_compliance may cause the OS updating error.

21. To run update utility, enter the command:
    `redhat-upgrade-tool --iso /root/rhel-server-7.x-x86_64-dvd.iso` (where 7.x is a version of Red Hat Enterprise Linux OS, up to which the System will be updated)
    Our example command:
    `redhat-upgrade-tool --iso /root/rhel-server-7.6-x86_64-dvd.iso`
    The following request will be displayed:
    `Continue with the upgrade [Y/N]?` To continue, type **Y** and press **Enter**.
    The following request will be displayed:

    ```
    HOOK-pkgdowngrades: INFO: done
    Finished. Reboot to start upgrade.
    ```

    > **Warning!**
    >
    > In case OS Red Hat Enterprise Linux is updated to version **following after 7.6**, the message as follows can be displayed:
    > ```
    > [            ~]# redhat-upgrade-tool --iso /root/rhel-server-7.7-x86_64-dvd.iso
    > setting up repos...
    > upgradeiso
    > upgradeiso/primary
    > The installed version of Preupgrade Assistant allows upgrade only to the system version 7.6.
    > ```
    > The message is aimed to inform you about the inability of the operating system to be updated to the specified version. In this case, use ISO image of OS Red Hat Enterprise Linux distributive kit of the version which was specified in the message final part.

22. Enter the command to reboot the server:
    `reboot`
    Updating will continue automatically after the server reboot.
23. Wait until the updated System is loaded and log in again. For this, take the steps 1-3 of the instruction before updating.
24. To update the configuration of the Postfix mail server, enter the command:
    `postfix upgrade-configuration`
25. Enter the command to find and display the list of files with **`.rpmnew`** extension at the console:
    `find / -name "*rpmnew*" -print`
    If the files have been found, they should be correctly merged with configuration files (see " Merging configuration files").

Note:

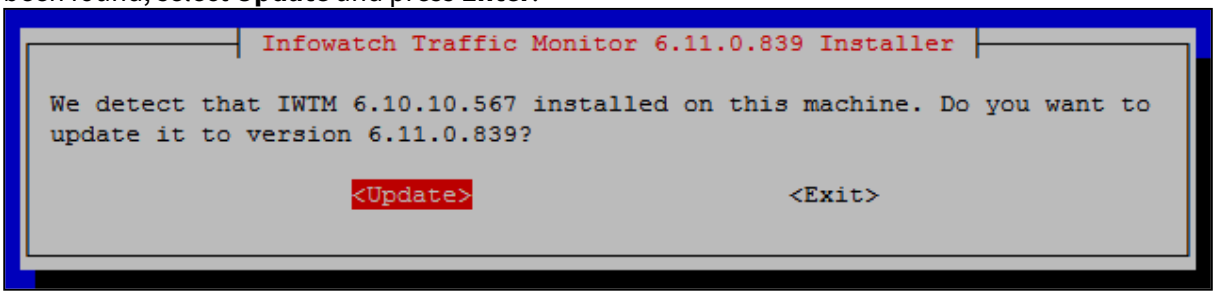
To merge successfully the configuration files, you should read the following articles on the official site:

- "What are rpmnew & rpmsave files?";
- "Recommendations on handling of rpmnew and rpmsave files following Red Hat Enterpries Linux system update".

Warning!

Do not change **web.conf**, **database.conf**, **consul.json** files. It is also recommended not to change the file /etc/nagios/**nagios.cfg**.

26. Before continuing the update, connect the external and internal Red Hat Enterprise Linux 7 repositories. You can check the instruction of the local repository setting on the Red Hat Enterprise Linux official website.
27. Enter the command to go to the directory containing Traffic Monitor distributives:
    `cd /root`
28. To start updating Traffic Monitor packages enter the command:
    `bash ./iwtm-installer-x.x.x.xxx-rhel7.run`
    Our example command:
    `bash ./iwtm-installer-6.11.0.839-rhel7.run`
    The installer will check the System before running and in case of non-compliance with requirements, it will interrupt the installation and display an error message. In this case, you need to correct the error and restart the update.
    In the window that opens informing that an early version of the InfoWatch Traffic Monitor has been found, select **Update** and press **Enter**:



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

> **Warning!**
>
> After the files have been merged, you should take the following action on TM server (TME Node Server): specify the DBMS server IP address (TME DB Server) within `hostname` parameter of `search_meta` block **`web.conf`** file.
> Do not change **`database.conf`**, **`consul.json`** files. It is also recommended not to change the file `/etc/nagios/`**`nagios.cfg`**.

30. Again, enter the command to call the file manager:
    `mc`
31. Go to directory `opt/iw/tm5/etc/scripts/` and make sure that file **`iwssid.lua.upgrade`** is there.
    The System does not use the file **`iwssid.lua.upgrade`**, as this is a backup in case the System needs to be customized.
32. Directory `/opt/iw/tm5/etc/scripts/` should contain the file **`iwssid.lua`** as well. We recommend to keep it as it is if it has not been edited before the update.
    Otherwise, it should be correctly merged with the configuration file **`iwssid.lua.rpmnew`** (see "Merging configuration files").
33. To exit the file manager:
    `exit`
34. Update server DBMS (TME DB Server) - see description below.

STEP 2. UPDATING DBMS SERVER (TME DB Server)

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

1. Complete steps 1, 2, of Step 1 of the instruction.
2. To stop Traffic Monitor services enter the command:
   `service iwtm stop && chkconfig iwtm off`
3. If you have Traffic Monitor **6.10.x** version installed, enter the command to stop service:
   `service iwtm-consul stop && chkconfig iwtm-consul off`
4. Depending on DBMS being used and Traffic Monitor version installed, enter the command to stop DB:
   - For **Oracle DBMS**:
     - `service oracle stop && chkconfig oracle off`
   - For **PostgreSQL DBMS**:
     - `service postgresql-9.4 stop && chkconfig postgresql-9.4 off` (Traffic Monitor **6.9.x** version)
     - `service postgresql-9.6 stop && chkconfig postgresql-9.6 off` (Traffic Monitor **6.10.x** version)
5. Complete steps 12-19, 21-27 of Step 1 of the instruction.
6. For **DBMS Oracle**:
   a. Enter the command to start Oracle:
      `service oracle start`
   b. Enter the command to start Oracle update:
      `bash ./iwtm-installer-x.x.x.xxx-rhel7.run -- --oracle-upgrade`
      Our example command:

```
bash ./iwtm-installer-6.11.0.630-rhel7.run -- --oracle-upgrade
```

As Oracle updates successfully, the following message appears:

```
Tue Mar 19 17:53:12 MSK 2019 INFO: Oracle DB upgrades successfuly.
Tue Mar 19 17:53:12 MSK 2019 INFO: You can cleanup old Oracle installation with the folowing
 commands (Only after IWTM upgrade and checks!!!):
su - "oracle" -c "/u01/app/oracle/product/db_1/oui/bin/runInstaller -ignoreSysPrereqs -detac
hHome ORACLE_HOME=/u01/app/oracle/product/db_1"
su - "oracle" -c "rm -rf /u01/app/oracle/product/db_1 /u01/app/oracle/product/db_2/OPatch.ba
ckup"
su - "oracle" -c "rm -rf /home/oracle/oracle12c_distr"
```

Note:

Oracle DBMS upgrade may take a long time.
Approximate timing to update 1 TB Oracle database:

- DBMS Oracle will be updated in 60 minutes;
- The Oracle database scheme will be updated in 50 minutes.

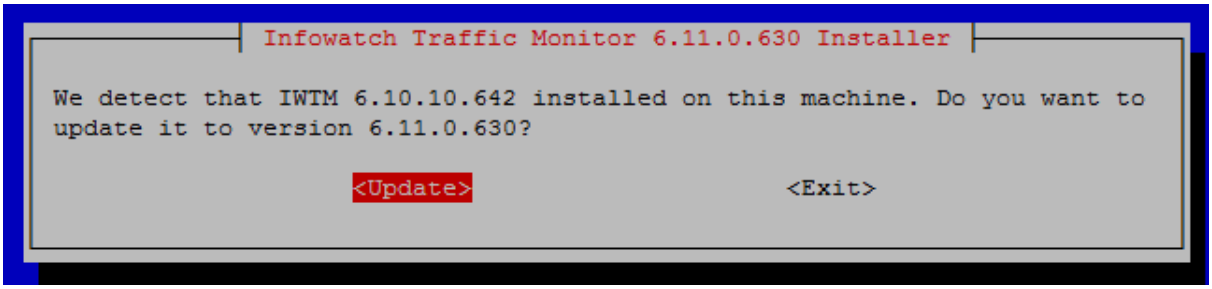
To perform the update, make sure there is 11 GB of free space in `ORACLE_HOME`, the default directory of which is `/u01/app/oracle`.
The message saying that Oracle has been successfully upgraded also says that you can remove the previous Oracle version.
You can remove it **only after** the System has been upgraded and all checks are completed.
Before the removal, **be sure to check** that:

- a new version is **not** installed in the `/u01/app/oracle/product/db_1` directory;
- all services of the System are started and running;
- the **System condition** tab of the TM Console does not contain errors;
- the DB contains old events. To check this, create a query on the **Events** tab and specify the required interception date;
- the DB receives new events.

To remove the old version, follow commands from the message.

c. To convert password file to Oracle 12 format, please enter the command: su - oracle -c "orapwd file=${ORACLE_HOME}/dbs/orapwiwtm force=y format=12 input_file=${ORACLE_HOME}/dbs/orapwiwtm"

7. To run an update of Traffic Monitor packages, enter the command:
`bash ./iwtm-installer-x.x.x.xxx-rhel7.run`
Our example command:
`bash ./iwtm-installer-6.11.0.630-rhel7.run`
The installer will check the System before running and in case of non-compliance with requirements, it will interrupt the installation and display an error message. In this case, you need to correct the error and restart the update.
In the window that opens informing that an early version of the InfoWatch Traffic Monitor has been found, choose **Update** and press **Enter**:



8. If you are using **PostgreSQL DBMS**, and Traffic Monitor has been updated from the version **6.9.x**, do the following:

1. Update PostgreSQL DBMS.
2. To switch to *postgres* user enter the command:
   `su - postgres`
3. To run the script (scenario) and update the DB enter command:
   `bash /opt/iw/tm5/csw/postgres/update.sh`

> **Note:**
>
> The database scheme update may take a long time.
> **Example**: a database of size 1 TB will be updated in 95 minutes.
> To perform the update, make sure there is 12 GB of free space in the root directory.

4. Enter command:
   `exit`

- Complete steps 29-33 of Step 1 of the instruction.
- Check Consul cluster - see the description below.

STEP 3. CHECKING CONSUL CLUSTER

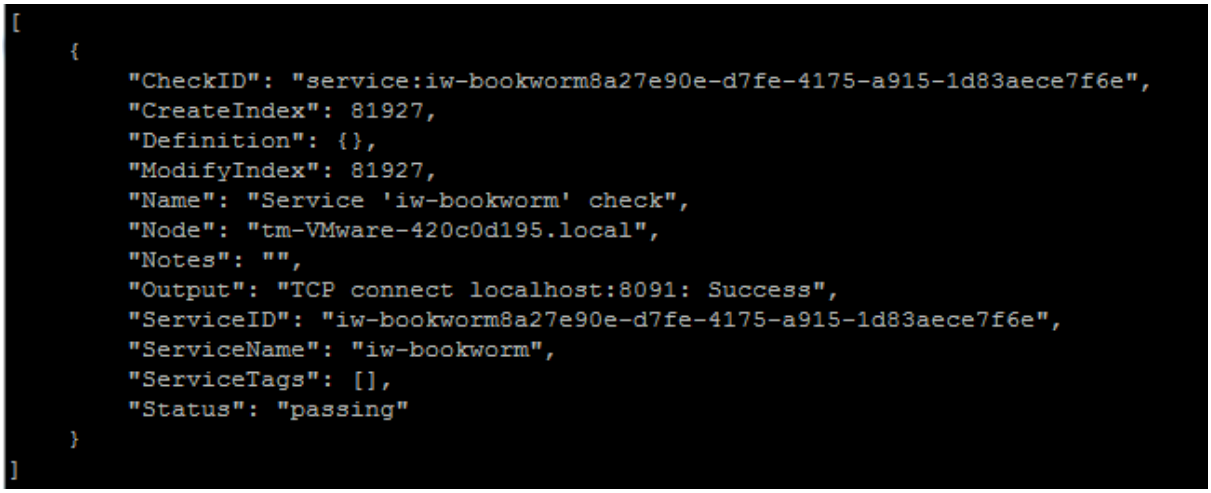
To check Consul cluster take the following steps:

1. Start Consul on all servers to be updated by running the command:
   `service iwtm-consul start`
   Enter the command to check status:
   `service iwtm-consul status`
2. To check Consul on DBMS server (TME DB Server), enter command:
   a. To get the IP-address of the primary server in the cluster (leader):
      `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   b. To get the information about cluster members:
      `consul members`
3. If no response with the IP-address of cluster leader, or not all servers are listed as cluster members, configure Consul cluster.
   Recheck after configuration. (step 2).
4. Perform health check of the System internal services - see description below.

STEP 4. PERFORMING HEALTHCHECK OF SYSTEM INTERNAL SERVICES
Start services `iw_bookworm`, `iw_licensed`, `iw_updater` и `iw_kicker` , check the status of the services.

1. Run command to start `iw_bookworm` service**:**
   `iwtm start bookworm`

2. Service may need some time to start. Enter the command to check the service status:
   `curl -s http://localhost:8500/v1/health/checks/iw-bookworm | python -mjson.tool`
   The following information will be displayed as a result of command execution:



3. Check "Node" and "Status" blocks:
   a. "Node" block should contain node's name (that has a service being checked) in Consul cluster;
   b. "Status" block should be "passing".
4. There should be only one `iw_licensed` service running on cluster. Start `iw_licensed` service using the command:
   `iwtm start licensed`
5. The service may need some time to start. Enter the command to check the status of `iw_licensed` service:
   `curl -s http://localhost:8500/v1/health/checks/iw-licensed | python -mjson.tool`
   Complete action 3 of the current step.
6. Run command to start `iw_updater service:`
   `iwtm start updater`
7. The service may need some time to start. Enter the command to check the status of `iw_updater` service:
   `curl -s http://localhost:8500/v1/health/checks/iw-updater | python -mjson.tool`
   Complete action 3 of the current step.
8. To check `iw_kicker` service you need to start `iw_blackboard:`
   `iwtm start blackboard`
9. There should be only one `iw_kicker` service running on cluster. Start `iw_kicker` service using the command:
   `iwtm start kicker`
10. The service may need some time to start. Check `/opt/iw/tm5/log/web-console-error.log file to` check the status of `iw_kicker` service and find if any errors occurred during the update. Enter command:
    `grep -r 'error' /opt/iw/tm5/log/web-console-error.log || echo "All good"`
    Make sure the command address is correct. If no errors found, the `All good` message will be displayed.

11. Run command to stop services:
    `iwtm stop`
12. Finish update of DBMS server - see description below.

> **Note:**
>
> In case a service has not started successfully, check if the appropriate log file had errors during the update. And contact InfoWatch technical service at support@infowatch.com. Also, you can check the support section on our site: www.infowatch.com/support.
> Log files for checking:
> - /opt/iw/tm5/log/bookworm.log - `iw_bookworm` service
> - /opt/iw/tm5/log/updater.log - `iw_updater` service
> - /opt/iw/tm5/log/licserv.log - `iw_licensed` service
> - /opt/iw/tm5/log/web-console-error.log - `iw_kicker` service
>
> To exclude errors appearing, we recommend to check log files if services has started successfully.
> Recommended login level - not lower than INFO. A log file can be missing if no errors registered.

STEP 5. COMPLETING DBMS SERVER UPDATE (TME DB Server)

Take the following steps to complete update of DBMS server (TME DB Server):

1. Enter the command to reboot the server:
   `reboot`
   Wait until the updating System is loaded and log in again. For this, take steps 1-3 of the instruction before updating.
2. Enter the command to delete packages from Red Hat Enterprise Linux 6:
   `yum remove *.el6*`

> **Warning!**
>
> Before the deletion processing on display, you will see the list of packages to be removed and a query for removal. Please carefully check the list for packages started with "**`iwtm-`**". Once you see any package, **cancel the deletion and miss this action**.

   To delete the displayed list of packages, press **Y** on the keyboard and press **Enter**.
3. Enter the command to clear cash of package manager:
   `yum clean all`
4. Enter the command to check the start of processes:
   `iwtm status`
   List of processes and their statuses will be displayed. The services should be started, the strings should have the following endings: **"active (running)"**.

```
Service iw_system_check.service is active (running); enabled state: loaded (enabled)
Service iw_agent.service is active (running); enabled state: loaded (enabled)
Service iw_indexer.service is active (running); enabled state: loaded (enabled)
Service iw_is.service is active (running); enabled state: loaded (enabled)
```

5. Run all TM servers (TME Node Server) - see the description below.

STEP 6. TM SERVERS RESTART (TME Node Server)

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

1. Enter the command to reboot the server:
   `reboot`
   Wait until server loading is completed and log in again by performing steps 1-3 of the instruction before updating.

Warning!

After the start, Traffic Monitor connects to the database and loads the configuration file `cas_config.xml` from there. Depending on configuration size, file loading may take some time.
During this loading period, the System may record error messages in log files:

- /opt/iw/tm5/log/cas_config_compiler.log

Запись об ошибке вида

```
1 2019-10-07 17:00:57.351489 (3936:0x00007f4008de8880) [ERROR  ] : <Root>
Exception:.
Diagnostic information..
/sandbox/src/cas3/config/details/cas_factory.cpp(233): Throw in function bool
cas::CasConfigFactory::LoadXmlConfig(cas::ConfigCreator::Ptr&, const
boost::filesystem::path&) const
Dynamic exception type:
boost::exception_detail::clone_impl<cas::ExceptionCasConfig>
```

- /opt/iw/tm5/log/cas.log

Запись об ошибке вида

```
1 2019-10-03 17:39:13.348146 (14262:0x00007fe83892ba80) [WARNING] : <Root>
Prometheus server is off, therefore the statistics is unavailable. That's
what you wanted, isn't it?
2 2019-10-03 17:39:14.364655 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
Error when loading config of tech: Cannot open xml file with cas
configuration: etc/config/cas/cas_config.xml
3 2019-10-03 17:39:14.364856 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
failed to initialize thrift server
Diagnostic information.
/sandbox/src/cas3/handler.cpp(682): Throw in function
 cas::Handler::LoadedConfigData cas::Handler::GetLoadedConfigData(const
prop::Property&, const Ptr&)
Dynamic exception type:
boost::exception_detail::clone_impl<tech::ExceptionTechLoadConfig>
```

```
std::exception::what: Cannot open xml file with cas configuration: etc/
config/cas/cas_config.xml
```

After the configuration file cas_config.xml has been successfully loaded, the System will stop recording error messages and will work in standard mode.
If the System continues to record error messages for a long time, check the connection with the database.

2. Enter the command to clear cash on TM server (TME Node Server), that has `web-gui` package functioning:
   `redis-cli flushall`
3. Complete actions 2 and 3 of Step 5 of the instruction.
4. Enter the command to check processes starting:
   `iwtm status`
   List of processes and their statuses will be displayed. Usually services `iw_qmover_client, iw_qmover_server and iw_image2text_fre_batch` are stopped, the rest of the services are running. Thereby the strings should have the following endings: **"inactive (dead)"** for services iw_qmover_client,iw_qmover_server and iw_image2text_fre_batch; and **"active (running)"** for other services:

```
Service iw_bookworm.service is active (running); enabled state: loaded (enabled)
Service iw_x2db.service is active (running); enabled state: loaded (enabled)
Service iw_x2x.service is active (running); enabled state: loaded (enabled)
Service iw_deliver.service is active (running); enabled state: loaded (enabled)
Service iw_warpd.service is active (running); enabled state: loaded (enabled)
Service iw_licensed.service is active (running); enabled state: loaded (enabled)
Service iw_luaengined.service is active (running); enabled state: loaded (enabled)
Service iw_cas.service is active (running); enabled state: loaded (enabled)
Service iw_analysis.service is active (running); enabled state: loaded (enabled)
Service iw_tech_tools.service is active (running); enabled state: loaded (enabled)
Service iw_pas.service is active (running); enabled state: loaded (enabled)
Service iw_adlibitum.service is active (running); enabled state: loaded (enabled)
Service iw_blackboard.service is active (running); enabled state: loaded (enabled)
Service iw_icap.service is active (running); enabled state: loaded (enabled)
Service iw_image2text_fre_batch.service is inactive (dead); enabled state: masked (bad)
Service iw_messed.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_http.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_icq.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_smtp.service is active (running); enabled state: loaded (enabled)
Service iw_sample_compiler.service is active (running); enabled state: loaded (enabled)
Service iw_smtpd.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_puppy.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_xapi.service is active (running); enabled state: loaded (enabled)
Service iw_system_check.service is active (running); enabled state: loaded (enabled)
Service iw_sniffer.service is active (running); enabled state: loaded (enabled)
Service iw_agent.service is active (running); enabled state: loaded (enabled)
Service iw_capstack.service is active (running); enabled state: loaded (enabled)
Service iw_configerator.service is active (running); enabled state: loaded (enabled)
Service iw_kicker.service is active (running); enabled state: loaded (enabled)
Service iw_qmover_client.service is inactive (dead); enabled state: masked (bad)
Service iw_qmover_server.service is inactive (dead); enabled state: masked (bad)
Service iw_updater.service is active (running); enabled state: loaded (enabled)
```

Note:

If Crawler subsystem is a part of System, it is required to run the services of this subsystem (on Crawler server): `InfoWatch.Crawler.Scanner, InfoWatch.Crawler.Server, Consul Agent`. 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 server in case of Distributed Installation is complete. The System version 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 the update, perform synchronizations manually to guarantee load of entities (see "*Infowatch Traffic Monitor. User Guide*", "Running Synchronization with Server Manually").

Note:

Clear the cash before starting, so the Console can be displayed correctly. Use your browser standard functionalities to perform the action.

Updating system by reinstalling and restoring data from backup copy

Warning!

We strongly recommend to back up the System, clone it and update on this particular testing computer. If Oracle DBMS is used in the System, before processing the update you should perform a database backup. When Oracle DBMS update is running, changes cannot be rollback.

During the update, the OS Red Hat Enterprise Linux 7.x version will be installed.

After installing the OS Red Hat Enterprise Linux 7.x version, Traffic monitor configuration files should be set up again. We recommend saving them to perform additional configuration after the update.

The following steps will be completed during the update:

i. Backing up DB, indexes, the configuration of iw_adlibitum service (Preparing for update).
ii. Installing OS Red Hat Enterprise Linux 7.x (The user follows the official instruction to install the OS).
iii. Installing InfoWatch Traffic Monitor 6.11.
iv. Restoring data from backup copies and DBMS update.

Updating steps look as follows:

Step 1. Preparing system for update and OS installing
Step 2. Updating DBMS server (TME DB Server)
Step 3. Updating all TM servers (TME Node Server)

Note:

If Crawler subsystem is a part of System, it is required to stop the services of this subsystem (on Crawler server): `InfoWatch.Crawler.Scanner, InfoWatch.Crawler.Server, Consul Agent`. 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**.

STEP 1. PREPARING SYSTEM FOR UPDATE AND INSTALLING OS

To prepare the system for the update, perform the following steps:

1. On all **TM servers (TME Node Server)**:
   a. Enter commands to stop interceptors:
   ```
   service iwtm stopwait icap
   service iwtm stopwait smtpd
   service iwtm stopwait expressd
   service iwtm stopwait sniffer
   service iwtm stopwait xapi_xapi
   service iwtm stopwait xapi_puppy
   ```
   b. Again, enter the command to call the file manager:
   ```
   mc
   ```
   c. 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/
   /opt/iw/tm5/queue/x2x/.db/
   /opt/iw/tm5/queue/x2x/.in/
   /opt/iw/tm5/queue/x2x/.out/
   ```
   When all the events are processed, these directories should be empty.

   Warning!

   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; these 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.

d. To exit the file manager (is required to better control command execution), enter the command:
`exit`
e. To stop services of Traffic Monitor server, enter the command:
`service iwtm stop && chkconfig iwtm off`
f. Depending on Traffic Monitor version installed, enter the command:
   - `service php-fpm stop && chkconfig php-fpm off` (Traffic Monitor **6.9.x** version)
   - `service iwtm-php-fpm stop && chkconfig iwtm-php-fpm off` (Traffic Monitor **6.10.x** version)

g. Back up `iw_adlibitum` service. For this:
   i. Go to `/opt/iw/tm5/etc` directory and open **`adlibitum.conf`** file to view.
   ii. "ConfigDir" parameter has a relative path to directory with `iw_adlibitum` configuration. The path is defined relatively to the content of "`NookDir`" parameter.
   Copy configuration directory into either other section of the server, or another server, or external device.

> **Warning!**
>
> To back up successfully, **files of all backup copies** must be copied altogether with their **rights**, **users** and **groups**.
> To do this, copy files into the **Linux file system** (ex., Ext4 or XFS).
> Store backup copies either on a separate section of the server or on another server or on an external device. Make sure that the data will not be lost when installing the OS Red Hat Enterprise Linux 7.x.
> After installation, backup copies should be copied into their **original directories**, and **rights**, **users** and **groups** should not be changed.

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

2. On **DBMS server (TME DB Server)**:
   a. Enter the command to stop `iw_indexer` service:
   `service iwtm stopwait indexer`
   b. To stop Traffic Monitor services enter the command:
   `service iwtm stop && chkconfig iwtm off`
   c. Connect to DB and check the number of events it contains:
      i. Oracle DBMS
         1. To connect to DB server, enter the commands using a console:
         `su - oracle`
         `sqlplus <scheme_owner_data>`
         where `<scheme_owner_data>` - login and pasword of the DB scheme owner. The default data are available on User accounts page.
         Example:

```
su - oracle
sqlplus iwtm/xxXX1234
```

2. Enter command:
   ```
   select count(1) from object;
   ```
3. To disconnect from the DB enter:
   exit
4. To switch to a required user enter the command:
   ```
   exit
   ```

PostgreSQL DBMS

1. To connect to DB server, enter the commands using a console:
   ```
   su - iwtm
   psql postgres iwtm -p 5433
   ```
2. Enter command:
   ```
   select count(1) from object;
   ```
3. To exit enter command:
   ```
   \q
   ```
4. Enter command:
   ```
   exit
   ```

d. To stop `searchd` processes enter the command:
   ```
   killall searchd
   ```
   To check, enter the command:
   ```
   ps -ef | grep searchd | grep -v grep
   ```
   Command response should not have processes running.

e. Run backup in accordance with the **requirements**:

   i. Depending on DBMS being used and the Traffic Monitor version installed, enter the command to stop DB:

      For **Oracle DBMS**:

      - `service oracle stop && chkconfig oracle off`

      For **PostgreSQL DBMS**:

      - `service postgresql-9.4 stop && chkconfig postgresql-9.4 off` (Traffic Monitor **6.9.x** version)
      - `service postgresql-9.6 stop && chkconfig postgresql-9.6 off` (Traffic Monitor **6.10.x** version)

   ii. Make DB backup. By default, DB is stored in directories **`/u01, /u02`**, etc.
   Copy DB into another section of the server or on another server or on an external device.

   > **Note:**
   >
   > To specify directories storing DB, check the file:
   > - /opt/iw/tm5/csw/oracle/database.conf (for **Oracle DBMS**);
   > - /opt/iw/tm5/csw/postgres/database.conf (for **PostgreSQL DBMS**).

   iii. Make indexes backup. To do this:

1. Enter the command to call the file manager:
   `sudo mc`
2. Go to `/opt/iw/tm5/etc` directory and open file **`indexer.conf`** to view.
3. The path to indexes directory is defined in "`SphinxBaseDir`" parameter. A relative path to indexes archives is defined in "`ArchiveDir`" parameter. Path to archives is defined relatively to the content of "`NookDir`" parameter. Copy indexes directories and indexes archive into another section of the server, or another server, or external device.
4. Install OS Red Hat Enterprise Linux 7.x on all servers. To do this, check the official instruction.
5. Update TM DBMS server (TME DB Server) - see description below.

STEP 2. UPDATING DBMS SERVER (TME DB Server)

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

1. Install Traffic Monitor version 6.11 in **DB node** mode on the **DBMS** server **(TME DB Server)**.

   > **Warning!**
   >
   > If backup copies are kept on external storage, do not connect them during the installation. You should do it right before DB backup and update.

2. To stop services enter the command:
   `iwtm stop`
3. Depending on DBMS being used, enter the command to stop DB:
   - `service oracle stop` (**Oracle DBMS**)
   - `service postgresql-9.6 stop` (**PostgreSQL DBMS**)
4. To stop `searchd` processes enter the command:
   `killall searchd`
   To check enter command:
   `ps -ef | grep searchd | grep -v grep`
   Command response should not have processes running.
5. Copy backup copy of DB that was created at action 2, step 1 into the original directory.

   > **Note:**
   >
   > The article gives an example, in your case, there may be more directories and files. Make sure you have all data restored.

6. When using Oracle DBMS, please make sure the **uid** ID (**oracle** user) and **gid** ID (**oinstall** group) have the value equal to 1001:
   a. To find out the **uid** and **gid** ID values, please run the command:
   `id oracle`
   b. Check the rights as per /u01 and /u02 directories:
   `ls -l /u01`
   `ls -l /u02`
   c. In case the rights are incorrect, search all these rights as per this owner in files and directories

and replace it as follows:

```
find /u01 -uid 501 -exec chown -v -h 1001 '{}' \;
find /u01 -gid 501 -exec chgrp -v 1001 '{}' \;
find /u02 -uid 501 -exec chown -v -h 1001 '{}' \;
find /u02 -gid 501 -exec chgrp -v 1001 '{}' \;
```

7. Enter command to shift to Traffic Monitor distributive's directory.
   Example:
   `cd /root`
8. Update DBMS:
   a. Oracle DBMS
      i. Enter the command to start Oracle:
      `service oracle start`
      ii. Enter the command to start Oracle update:
      `bash ./iwtm-installer-x.x.x.xxx-rhel7.run -- --oracle-upgrade`
      Our example command:
      `bash ./iwtm-installer-6.11.0.630-rhel7.run -- --oracle-upgrade`
      The following message will be displayed after a successful update of Oracle:

```
Tue Mar 19 17:53:12 MSK 2019 INFO: Oracle DB upgrades successfuly.
Tue Mar 19 17:53:12 MSK 2019 INFO: You can cleanup old Oracle installation with the folowing
 commands (Only after IWTM upgrade and checks!!!):
su - "oracle" -c "/u01/app/oracle/product/db_1/oui/bin/runInstaller -ignoreSysPrereqs -detac
hHome ORACLE_HOME=/u01/app/oracle/product/db_1"
su - "oracle" -c "rm -rf /u01/app/oracle/product/db_1 /u01/app/oracle/product/db_2/OPatch.ba
ckup"
su - "oracle" -c "rm -rf /home/oracle/oracle12c_distr"
```

> **Note:**
>
> Oracle DBMS upgrade may take a long time.
> **Approximate** timing to update 1 TB Oracle database:
> - DBMS Oracle will be updated in 60 minutes;
> - The Oracle database scheme will be updated in 50 minutes.
>
> To perform the update, make sure there is 11 GB of free space in `ORACLE_HOME`, the default directory of which is `/u01/app/oracle`.
> The message saying that Oracle has been successfully upgraded also says that you can remove the previous Oracle version.
> You can remove it **only after** the System has been upgraded and all checks are completed.
> Before the removal, **be sure to check** that:
> - a new version is **not** installed in the `/u01/app/oracle/product/db_1` directory;
> - all services of the System are started and running;
> - the **System condition** tab of the TM Console does not contain errors;
> - the DB contains old events. To check this, create a query on the **Events** tab and specify the required interception date;
> - the DB receives new events.
>
> To remove the old version, follow commands from the message.

iii. Enter the command to shift to the directory containing the script (scenario) of DB scheme upgrade:
`cd /opt/iw/tm5/csw/oracle`

iv. Enter the command to run the script:
`su --command "/opt/iw/tm5/csw/oracle/update.sh" oracle`

v. To convert password file to Oracle 12 format, please enter the command: `su - oracle -c "orapwd file=${ORACLE_HOME}/dbs/orapwiwtm force=y format=12 input_file=${ORACLE_HOME}/dbs/orapwiwtm"`

PostgreSQL DBMS

i. If System upgrades from version **6.9.x**:
   1. Complete PostgreSQL DBMS update.
   2. Enter the command to run script (scenario) of DB scheme upgrade:
      `su --command "/opt/iw/tm5/csw/postgres/update.sh" postgres`

ii. If System upgrades from version **6.10.x**:
   1. Enter the command to start **PostgreSQL**:
      `service postgresql-9.6 start`
   2. Enter command:
      `su --command "/usr/pgsql-9.6/bin/psql -d postgres -p 5433 -f /opt/iw/tm5/etc/update_psql_commands" postgres`
   3. Enter command to shift to directory containing the script (scenario) of DB scheme upgrade:
      `cd /opt/iw/tm5/csw/postgres`
   4. Enter command to run script:
      `su --command "/opt/iw/tm5/csw/postgres/update.sh" postgres`

> **Note:**
>
> The database scheme update may take a long time.
> **Example**: a database of size 1 TB will be updated in 95 minutes.
> To perform the update, make sure there is 12 GB of free space in the root directory.

9. Perform action 2c, Step 1 of the instruction to compare the number of events in DB before and after the update.
10. Copy **indexes backup** that was created at action 2e, Step 1 that way, so the directory is up with the original files and directories.
    If the original directory is not a default one, it needs to be indicated in the appropriate sections of configuration files (see steps 2e, Section 1).
11. Enter the command to reboot the server:
    `reboot`
    Wait until the loading of the server is completed and log in again by performing steps 1-3 of the instruction before updating.
12. Enter the command to test the start of processes:
    `iwtm status`
    List of processes and their statuses will be displayed. Services should be running, strings should

have the following endings: "**active (running)**".

```
Service iw_system_check.service is active (running); enabled state: loaded (enabled)
Service iw_agent.service is active (running); enabled state: loaded (enabled)
Service iw_indexer.service is active (running); enabled state: loaded (enabled)
Service iw_is.service is active (running); enabled state: loaded (enabled)
```

13. Update all TM servers (TME Node Server) - see the description below.

STEP 3. UPDATING ALL TM SERVERS (TME Node Server)

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

1. Install Traffic Monitor version 6.11 in **TM node mode** on all **TM servers (TME Node Server)**.
2. To stop services, enter the command:
   `iwtm stop`
   `service iwtm-php-fpm stop`
   `service nagios stop`
3. On a server that has `iw_adlibitum` service installed and added in autorun, copy configuration copy that was created at step 1g, Section 1 that way, so the directory is up with the original files and directories.
   If the original directory is not a default one, it needs to be indicated in the appropriate sections of configuration files (see action 1g, Step 1).
4. Run the commands:
   `sudo -u iwtm touch /opt/iw/tm5/www/backend/protected/runtime/first_run`
   `iwtm restart kicker`
5. Enter the command to reboot the server:
   `reboot`
   Wait until server loading is completed and log in again by performing steps 1-3 of the instruction before updating.
6. Enter the command to clear cash on TM server (TME Node Server) with `web-gui` package functioning on it:
   `redis-cli flushall`
7. Enter the command to test the start of processes:
   `iwtm status`
   List of processes and their statuses will be displayed. Usually,
   services `iw_qmover_client, iw_qmover_server и iw_image2text_fre_batch` are stopped, the rest of the services are running. Thereby the strings should have the following endings: **"inactive (dead)"** for the
   services `iw_qmover_client, iw_qmover_server and iw_image2text_fre_batch` and "**acti**

ve (running)" for other services:

```
Service iw_bookworm.service is active (running); enabled state: loaded (enabled)
Service iw_x2db.service is active (running); enabled state: loaded (enabled)
Service iw_x2x.service is active (running); enabled state: loaded (enabled)
Service iw_deliver.service is active (running); enabled state: loaded (enabled)
Service iw_warpd.service is active (running); enabled state: loaded (enabled)
Service iw_licensed.service is active (running); enabled state: loaded (enabled)
Service iw_luaengined.service is active (running); enabled state: loaded (enabled)
Service iw_cas.service is active (running); enabled state: loaded (enabled)
Service iw_analysis.service is active (running); enabled state: loaded (enabled)
Service iw_tech_tools.service is active (running); enabled state: loaded (enabled)
Service iw_pas.service is active (running); enabled state: loaded (enabled)
Service iw_adlibitum.service is active (running); enabled state: loaded (enabled)
Service iw_blackboard.service is active (running); enabled state: loaded (enabled)
Service iw_icap.service is active (running); enabled state: loaded (enabled)
Service iw_image2text_fre_batch.service is inactive (dead); enabled state: masked (bad)
Service iw_messed.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_http.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_icq.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_smtp.service is active (running); enabled state: loaded (enabled)
Service iw_sample_compiler.service is active (running); enabled state: loaded (enabled)
Service iw_smtpd.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_puppy.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_xapi.service is active (running); enabled state: loaded (enabled)
Service iw_system_check.service is active (running); enabled state: loaded (enabled)
Service iw_sniffer.service is active (running); enabled state: loaded (enabled)
Service iw_agent.service is active (running); enabled state: loaded (enabled)
Service iw_capstack.service is active (running); enabled state: loaded (enabled)
Service iw_configerator.service is active (running); enabled state: loaded (enabled)
Service iw_kicker.service is active (running); enabled state: loaded (enabled)
Service iw_qmover_client.service is inactive (dead); enabled state: masked (bad)
Service iw_qmover_server.service is inactive (dead); enabled state: masked (bad)
Service iw_updater.service is active (running); enabled state: loaded (enabled)
```

Note:

If Crawler subsystem is a part of System, it is required to run the services of this subsystem (on Crawler server): `InfoWatch.Crawler.Scanner, InfoWatch.Crawler.Server, Consul Agent`. 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 server in case of Distributed installation is complete. The System version 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 the 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.

Warning!

We strongly recommend to back up the System, clone it and update on this particular testing machine.

Updating steps look as follows:

Step 1. Upgating all TM servers (TME Node Server)
Step 2. DBMS server update (TME DB Server)
Step 3. Checking Consul cluster
Step 4. Healthckeck of internal services of System
Step 5. Finishing update on DBMS server (TME DB Server)
Step 6. Restart all TM servers (TME Node Server)

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

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

1. Copy the files from InfoWatch Traffic Monitor distributive into the `/root` directory:
   - **iwtm-installer-x.x.x.xxx-rhel7.run** (where x.x.x.xxx is a number of build);
   - **iwtm-postgresql-9.6.13-x.xx.x.tar.gz**;
   - **iwtm-oracle-12.2.0.1-x.xx.x.tar.gz**;
   - **iwtm-adp-x.xx.x.tar.gz**.

   Example:
   - **`iwtm-installer-6.11.2.1032-rhel7.run`**;
   - **`iwtm-postgresql-9.6.13-6.11.2.tar.gz`**;
   - **`iwtm-oracle-12.2.0.1-6.11.2.tar.gz`**;
   - **`iwtm-adp-6.11.2.tar.gz`**.

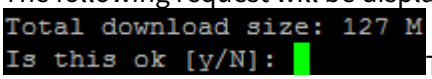
   Note:

   If Crawler subsystem is a part of System, it is required to stop the services of this subsystem (on Crawler server): `InfoWatch.Crawler.Scanner`, `InfoWatch.Crawler.Server`, `Consul Agent`. 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**.

2. Enter commands to stop interceptors:
   ```
   iwtm stop icap
   iwtm stop smtpd
   iwtm stop sniffer
   iwtm stop xapi_xapi
   iwtm stop xapi_puppy
   ```
3. Again, enter the command to call the file manager:
   ```
   mc
   ```
4. 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/
   ```

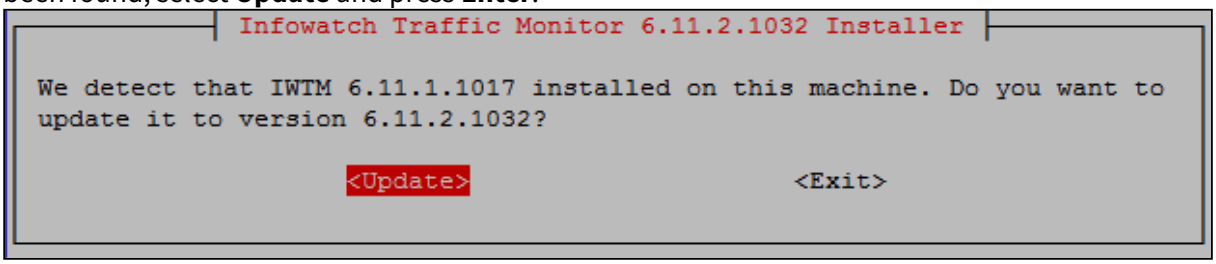
```
/opt/iw/tm5/queue/analysis/.out/
/opt/iw/tm5/queue/db/.db/
/opt/iw/tm5/queue/db/.in/
/opt/iw/tm5/queue/db/.out/
/opt/iw/tm5/queue/smtp/.db/
/opt/iw/tm5/queue/smtp/.in/
/opt/iw/tm5/queue/smtp/.out/
/opt/iw/tm5/queue/x2x/.db/
/opt/iw/tm5/queue/x2x/.in/
/opt/iw/tm5/queue/x2x/.out/
```
When all the events are processed, these directories should be empty.

> **Warning!**
>
> Before continuing 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.

5. To exit the file manager (is required to better control command execution), enter the command:
   `exit`
6. To stop Traffic Monitor services enter the command:
   `iwtm stop`
7. Enter commands to stop the services:
   ```
   systemctl stop iwtm-php-fpm
   systemctl stop nginx
   systemctl stop nagios
   systemctl stop iwtm-consul
   ```
8. Connect the external and internal repositories Red Hat Enterprise Linux 7.
   You can check the instruction of the local repository setting on Red Hat Enterprise Linux official website.
9. To update packages enter the command:
   `yum upgrade`
   The following request will be displayed:
   

   To continue, type **Y** and press **Enter**.
10. Enter the command to go to the directory containing Traffic Monitor distributives:
    `cd /root`
11. To start updating Traffic Monitor packages enter the command:
    `bash ./iwtm-installer-x.x.x.xxx-rhel7.run`
    Our example command:
    `bash ./iwtm-installer-6.11.2.1032-rhel7.run`
    The installer will check the System before running and in case of non-compliance with requirements, it will interrupt the installation and display an error message. In this case, you need to correct the error and restart the update.

In the window that opens informing that an early version of the InfoWatch Traffic Monitor has been found, select **Update** and press **Enter**:



Please wait until the packages update is complete.

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

> **Note:**
>
> To merge successfully the configuration files you should read the following articles on official site:
> - "What are rpmnew & rpmsave files?";
> - "Recommendations on handling of rpmnew and rpmsave files following Red Hat Enterpries Linux system update".

13. Again, enter the command to call the file manager:
    `mc`
14. Go to directory `/opt/iw/tm5/etc/scripts/` and make sure that there is a file **`iwssid.lua.upgrade`**. The System does not use the file **`iwssid.lua.update`**, as it is a backup in case the System is to be customized.
15. Directory `/opt/iw/tm5/etc/scripts/` should contain the file **`iwssid.lua`** as well. We recommend to keep it as it is if it has not been edited before the update.
    Otherwise, it should be correctly merged with the configuration file **`iwssid.lua.rpmnew`** (see "Merging configuration files").
16. To exit the file manager:
    `exit`
17. Update server DBMS (TME DB Server) - see description below.

STEP 2. UPDATING DBMS SERVER (TME DB Server)

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

1. Complete action 1 of Step 1 of the instruction.
2. To stop Traffic Monitor services enter the command:
   `iwtm stop`
3. Enter the command to stop service:
   `systemctl stop iwtm-consul`
4. Depending on DBMS being used enter the command to stop the DB:
   - For **Oracle DBMS**:
     `service oracle stop`

- For **PostgreSQL DBMS**:
  `service postgresql-9.6 stop && chkconfig postgresql-9.6 off` (Traffic Monitor **6.10.x** version)

5. Complete actions 8-16 of Step 1 of the instruction.

> **Note:**
>
> The database scheme update may take a long time.
> **Example**: for a database of size 1 TB - above 30 minutes.
> To perform the update, make sure:
> - There is 11 GB of free space in `ORACLE_HOME`, the default directory of which is `/u01/app/oracle` - for **Oracle DBMS**;
> - There is 12 GB of free space in the root directory - for **PostgreSQL DBMS**.
>
> The message saying that Oracle has been successfully upgraded may also say that you can remove the previous Oracle version.
> You can remove it **only after** the System has been upgraded and all checks are completed.
> Before the removal, **be sure to check** that:
> - a new version is **not** installed in the `/u01/app/oracle/product/db_1` directory;
> - all services of the System are started and running;
> - the **System condition** tab of the TM Console does not contain errors;
> - the DB contains old events. To check this, create a query on the **Events** tab and specify the required interception date;
> - the DB receives new events.
>
> To remove the old version, follow commands from the message.

6. Check the Consul cluster - see the description below.

STEP 3. CHECKING CONSUL CLUSTER

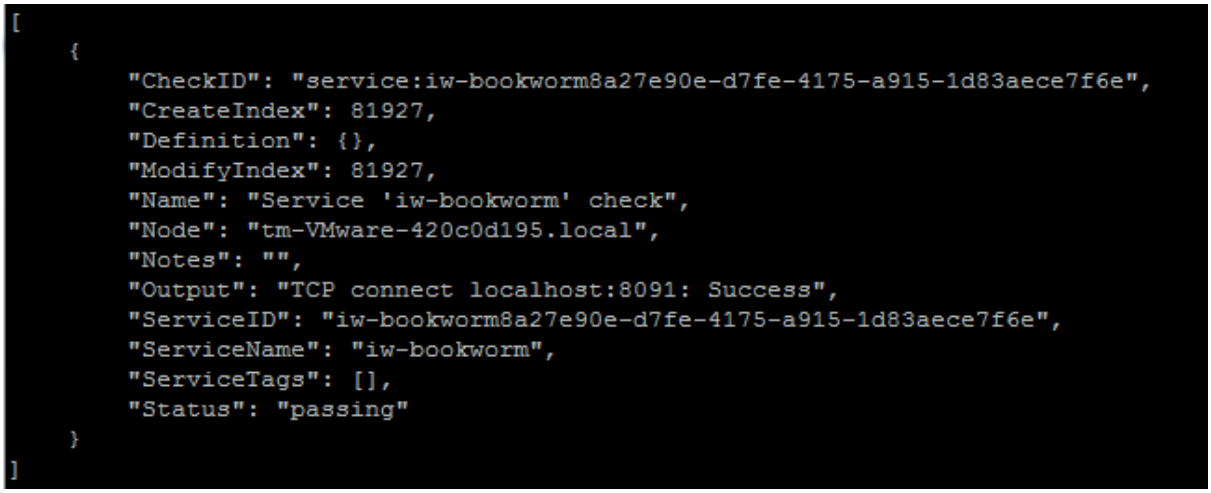
To check Consul cluster take the following steps:

1. Start Consul on all servers to be updated by running the command:
   `systemctl start iwtm-consul`
   Enter the command to check status:
   `systemctl status iwtm-consul`
2. To check Consul on DBMS server (TME DB Server), enter the command:
   a. To get the IP-address of the primary server in the cluster (leader):
      `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   b. To get the information about cluster members:
      `consul members`
3. If no response with the IP-address of cluster leader, or not all servers are listed as cluster members, configure Consul cluster.
   Recheck after configuration. (step 2).
4. Perform health check of System internal services - see description below.

STEP 4. PERFORMING HEALTHCHECK OF SYSTEM INTERNAL SERVICES
Start services `iw_bookworm`, `iw_licensed`, `iw_updater` и `iw_kicker` , check the status of the services:

1. Run command to start `iw_bookworm` service:
   `iwtm start bookworm`

2. Service may need some time to start. Enter the command to check the status of service:
   `curl -s http://localhost:8500/v1/health/checks/iw-bookworm | python -mjson.tool`
   The following information will be displayed as a result of command execution:



3. Check "Node" and "Status" blocks:
   a. "Node" block should contain node's name (that has a service being checked) in Consul cluster;
   b. "Status" block should be "passing".
4. There should be only one `iw_licensed` service running on cluster. Start `iw_licensed` service using the command:
   `iwtm start licensed`
5. The service may need some time to start. Enter the command to check the status of `iw_licensed` service:
   `curl -s http://localhost:8500/v1/health/checks/iw-licensed | python -mjson.tool`
   Complete action 3 of the current step.
6. Run command to start `iw_updater service:`
   `iwtm start updater`
7. The service may need some time to start. Enter the command to check the status of `iw_updater` service:
   `curl -s http://localhost:8500/v1/health/checks/iw-updater | python -mjson.tool`
   Complete action 3 of the current step.
8. To check `iw_kicker` service you need to start `iw_blackboard:`
   `iwtm start blackboard`
9. There should be only one `iw_kicker` service running on cluster. Start `iw_kicker` service using the command:
   `iwtm start kicker`
10. The service may need some time to start. Check `/opt/iw/tm5/log/web-console-error.log file to` check status of `iw_kicker` service and find if any errors occurred during the update. Enter command:
    `grep -r 'error' /opt/iw/tm5/log/web-console-error.log || echo "All good"`
    Make sure the command address is correct. If no errors found, the `All good` message will be displayed.

11. Run the command to stop services:
    `iwtm stop`
12. Finish update of DBMS server - see description below.

> **Note:**
>
> In case a service has not started successfully, check if the appropriate log file had errors during the update. And contact InfoWatch technical service at support@infowatch.com. Also, you can check the support section on our site: www.infowatch.com/support.
> Log files for checking:
> - `/opt/iw/tm5/log/bookworm.log` - `iw_bookworm` service
> - `/opt/iw/tm5/log/updater.log` - `iw_updater` service
> - `/opt/iw/tm5/log/licserv.log` - `iw_licensed` service
> - `/opt/iw/tm5/log/web-console-error.log` - `iw_kicker service`
>
> To exclude errors appearing, we recommend to check log files if services has started successfully.
> Recommended login level - not lower than INFO. A log file can be missing if no errors registered.

STEP 5. COMPLETING DBMS SERVER UPDATE (TME DB Server)

Take the following steps to complete update of DBMS server (TME DB Server):

1. Enter the command to reboot the server:
   `reboot`
   Wait until the updating System is loaded and log in again. For this, take steps 1-3 of the instruction before updating.
2. Enter the command to clear cash of package manager:
   `yum clean all`
3. Enter the command to check the start of processes:
   `iwtm status`
   List of processes and their statuses will be displayed. The services should be started, the strings should have the following endings: **"active (running)"**.
   ```
   Service iw_system_check.service is active (running); enabled state: loaded (enabled)
   Service iw_agent.service is active (running); enabled state: loaded (enabled)
   Service iw_indexer.service is active (running); enabled state: loaded (enabled)
   Service iw_is.service is active (running); enabled state: loaded (enabled)
   ```
4. Run all TM servers (TME Node Server) - see the description below.

STEP 6. TM SERVERS RESTART (TME Node Server)

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

1. Enter the command to reboot the server:
   `reboot`
   Wait until server loading is completed and log in again by performing steps 1-3 of the instruction before updating.

Warning!

After the start, Traffic Monitor connects to the database and loads the configuration file `cas_config.xml` from there. Depending on configuration size, file loading may take some time.
During this loading period, the System may record error messages in log files:

- /opt/iw/tm5/log/cas_config_compiler.log

Запись об ошибке вида

```
1 2019-10-07 17:00:57.351489 (3936:0x00007f4008de8880) [ERROR  ] : <Root>
Exception:.
Diagnostic information..
/sandbox/src/cas3/config/details/cas_factory.cpp(233): Throw in function bool
cas::CasConfigFactory::LoadXmlConfig(cas::ConfigCreator::Ptr&, const
boost::filesystem::path&) const
Dynamic exception type:
boost::exception_detail::clone_impl<cas::ExceptionCasConfig>
```

- /opt/iw/tm5/log/cas.log

Запись об ошибке вида

```
1 2019-10-03 17:39:13.348146 (14262:0x00007fe83892ba80) [WARNING] : <Root>
Prometheus server is off, therefore the statistics is unavailable. That's
what you wanted, isn't it?
2 2019-10-03 17:39:14.364655 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
Error when loading config of tech: Cannot open xml file with cas
configuration: etc/config/cas/cas_config.xml
3 2019-10-03 17:39:14.364856 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
failed to initialize thrift server
Diagnostic information.
/sandbox/src/cas3/handler.cpp(682): Throw in function
 cas::Handler::LoadedConfigData cas::Handler::GetLoadedConfigData(const
prop::Property&, const Ptr&)
Dynamic exception type:
boost::exception_detail::clone_impl<tech::ExceptionTechLoadConfig>
std::exception::what: Cannot open xml file with cas configuration: etc/
config/cas/cas_config.xml
```

After the configuration file cas_config.xml has been successfully loaded, the System will stop recording error messages and will work in standard mode.
If the System continues to record error messages for a long time, check the connection with the database.

2. Enter the command to clear cash on TM server (TME Node Server), that has `web-gui` package functioning:
   `redis-cli flushall`

3. Enter the command to check processes starting:
   `iwtm status`
   List of processes and their statuses will be displayed. Usually services `iw_qmover_client, iw_qmover_server and iw_image2text_fre_batch` are stopped, the rest of the services are running. Thereby the strings should have the following endings: **"inactive (dead)"** for services iw_qmover_client,iw_qmover_server and iw_image2text_fre_batch; and **"active (running)"** for other services:

```
Service iw_bookworm.service is active (running); enabled state: loaded (enabled)
Service iw_x2db.service is active (running); enabled state: loaded (enabled)
Service iw_x2x.service is active (running); enabled state: loaded (enabled)
Service iw_deliver.service is active (running); enabled state: loaded (enabled)
Service iw_warpd.service is active (running); enabled state: loaded (enabled)
Service iw_licensed.service is active (running); enabled state: loaded (enabled)
Service iw_luaengined.service is active (running); enabled state: loaded (enabled)
Service iw_cas.service is active (running); enabled state: loaded (enabled)
Service iw_analysis.service is active (running); enabled state: loaded (enabled)
Service iw_tech_tools.service is active (running); enabled state: loaded (enabled)
Service iw_pas.service is active (running); enabled state: loaded (enabled)
Service iw_adlibitum.service is active (running); enabled state: loaded (enabled)
Service iw_blackboard.service is active (running); enabled state: loaded (enabled)
Service iw_icap.service is active (running); enabled state: loaded (enabled)
Service iw_image2text_fre_batch.service is inactive (dead); enabled state: masked (bad)
Service iw_messed.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_http.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_icq.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_smtp.service is active (running); enabled state: loaded (enabled)
Service iw_sample_compiler.service is active (running); enabled state: loaded (enabled)
Service iw_smtpd.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_puppy.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_xapi.service is active (running); enabled state: loaded (enabled)
Service iw_system_check.service is active (running); enabled state: loaded (enabled)
Service iw_sniffer.service is active (running); enabled state: loaded (enabled)
Service iw_agent.service is active (running); enabled state: loaded (enabled)
Service iw_capstack.service is active (running); enabled state: loaded (enabled)
Service iw_configerator.service is active (running); enabled state: loaded (enabled)
Service iw_kicker.service is active (running); enabled state: loaded (enabled)
Service iw_qmover_client.service is inactive (dead); enabled state: masked (bad)
Service iw_qmover_server.service is inactive (dead); enabled state: masked (bad)
Service iw_updater.service is active (running); enabled state: loaded (enabled)
```

Note:

If Crawler subsystem is a part of System, it is required to run the services of this subsystem (on Crawler server): `InfoWatch.Crawler.Scanner, InfoWatch.Crawler.Server, Consul Agent`. 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 server in case of Distributed Installation is complete. The System version 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 the update, perform synchronizations manually to guarantee load of entities (see "*Infowatch Traffic Monitor. User Guide*", "Running Synchronization with Server Manually").

Note:

Clear the cash before starting, so the Console can be displayed correctly. Use your browser standard functionalities to perform the action.

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.

Warning!

To operate correctly Traffic Monitor and Device Monitor should have the same versions. See more details about Device Monitor 6.11 compatibility in the InfoWatchKnowledge Base article "Compatibility among the versions of TM, DM and Agents".

System update is similar to its installation:

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

   Warning!

   When updating the System from early versions to version 6.11 follow the procedure:
   Device Monitor server should be updated first, then update Traffic Monitor Server and after this DM Agents should be updated on workstations.
   If it is required to update IW Device Monitor to version 6.11 this should be done in sequence - first you should update to intermediate version. For example, updating Device Monitor 6.9 up to 6.10 version, first update to 6.10 and only after this you can update Device Monitor to 6.11 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.

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

> **Warning!**
>
> 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.

Важно!

Do not change **`web.conf`**, **`database.conf`**, **`consul.json`** files.

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:

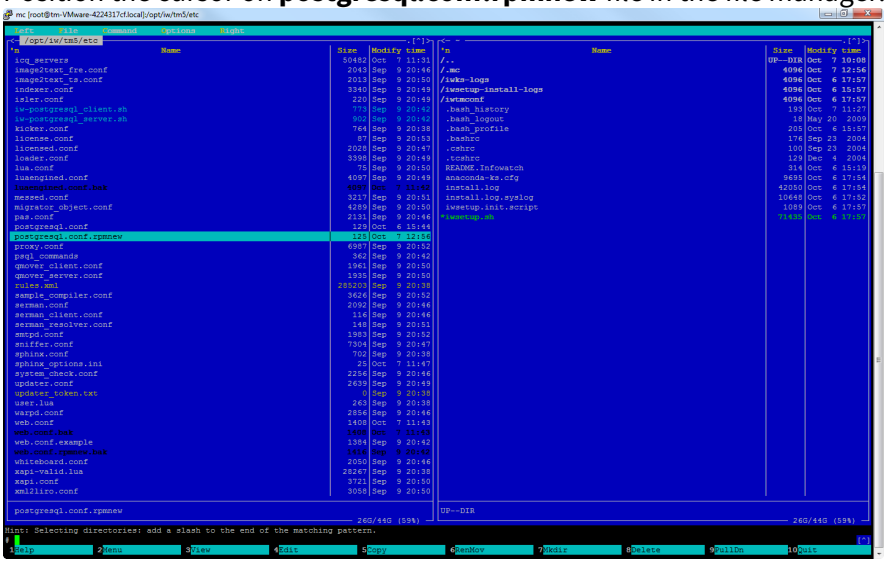
```
{
    "DB": "postgres",
    "Host": "localhost",
    "Password": "xxXX1234",
    "Port": 5433,
    "Username": "iwtm_linux"
}
```


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:

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

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 http://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.

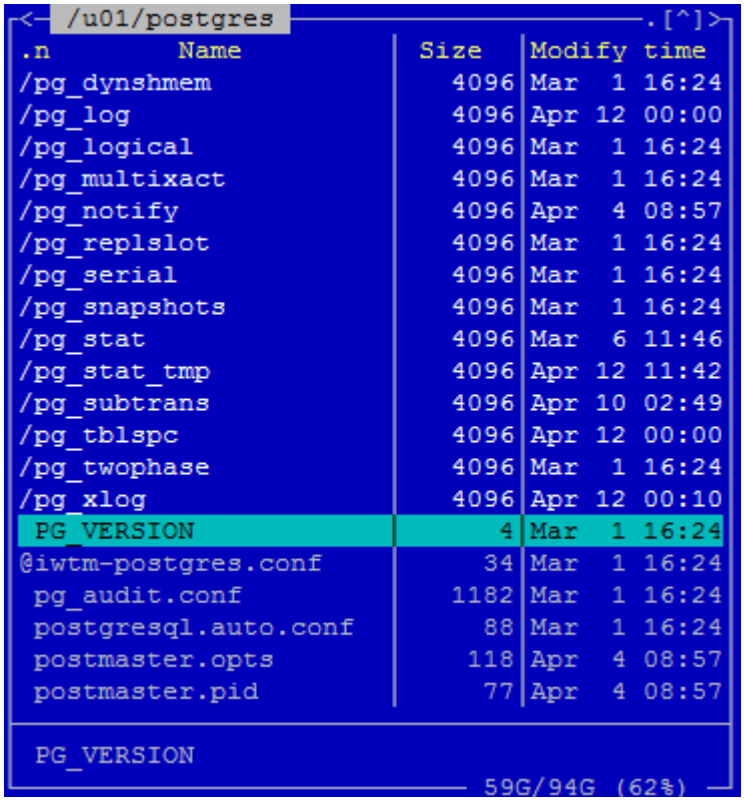
Important! Using Screen is highly recommended when working with DB and updating DBMS.

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:

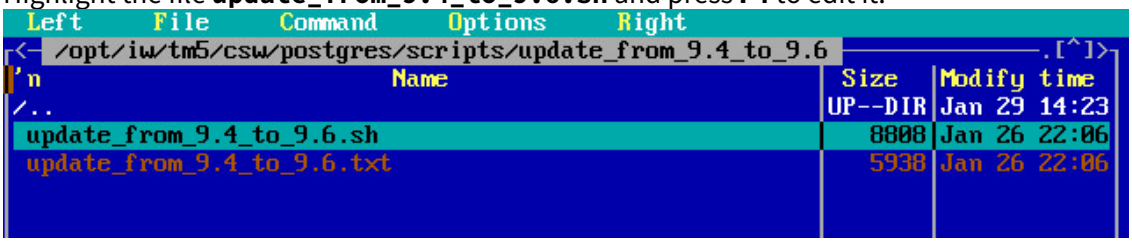


   d. Press **F3** to close the file.
   If version **9.6** is already installed in the System, then do not run DBMS update and follow the instruction on updating the System.

> **Important!**
>
> If you are updating DBMS as a part of Traffic Monitor version 6.9 which is being reinstalled, then the `PG_VERSION` file version is 9.6. Follow the instruction to update the DBMS.

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:
   ```
   iwtm stop
   service iwtm-php-fpm stop
   service nagios stop
   service iwtm-gearmand stop
   service iwtm-consul stop
   ```
   b. For Traffic Monitor distributed installation:
      i. On Traffic Monitor server:
      ```
      iwtm stop
      service iwtm-php-fpm stop
      service nagios stop
      service iwtm-gearmand stop
      service iwtm-consul stop
      ```
      ii. On DB server:
      ```
      iwtm stop
      service nagios stop
      service iwtm-consul stop
      ```

4.6.2 Update

1. Enter the command to install packages that are required for installation:
   ```
   yum install postgresql94-server
   ```
2. Enter the command to go to the required directory:
   ```
   cd /opt/iw/tm5/csw/postgres/scripts/update_from_9.4_to_9.6
   ```
3. 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.`
4. 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).

5. 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. The 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 occurred.

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 the 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 the 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 the log 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.`

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".

> **Note:**
>
> In case you require deleting the whole System, you may miss separate DB scheme deletion, since this process is to be performed in accordance with "Uninstalling Traffic Monitor'.

- 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.
- See details on Traffic Monitor removal in "Uninstalling Traffic Monitor" (all components which were installed on the server: web console, interception modules, DBMS containing DB data and others).

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.

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:
   `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:
   `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").

   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.

4. 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.

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.

5.4 Uninstalling Traffic Monitor

When uninstalling Traffic Monitor, **all the components installed on server will be also removed**: web console, interception modules, configuration files, settings, technologies, protected objects, users, roles, policies, license files.

If the database is located on the same server, where the unintstallation process is to be started, DBMS willl be removed as well as all the data, including events, indexes and settings.

Uninstallation influences only the server where the removal command is run.

If you require to restore events when reinstalling Traffic Monitor, you are recommended to create a database reserve copy before processing the uninstallation (for more details see "*InfoWatch Traffic Monitor. Administration Guide".* Database Administration - **PostgreSQ**L > Database Backup "Creating Database Backup" section; **Oracle** > Database Backup "Creating Database Backup" section;

We also recommend prior making a copy of configuration settings.

Traffic Monitor uninstallation process starts running in console mode, using InfoWatch Traffic Monitor installer.

The following actions are to be taken to uninstall Traffic Monitor:

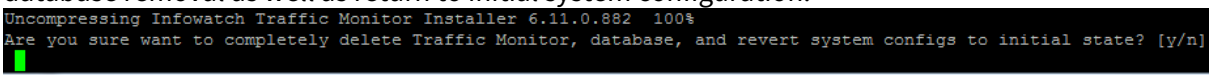
1. Enter login and password to log into operating system used (enter as a **root** user using the password created when the System was installed).

2. Create a directory where the InfoWatch Traffic Monitor installer will be located. For example, to create a directory called `distr` the following command is to be run within the filesystem root:
   `mkdir /distr`
3. Copy into created directory the file **iwtm-installer-x.x.x.xxx-rhel7.run** (where x.x.x.xxx - the assembling number), which is a part of InfoWatch Traffic Monitor distibution kit.
   As per our example:
   `iwtm-installer-6.11.0.882-rhel7.run`
4. To go to InfoWatch Traffic Monitor installer directory enter the command as per our example:
   `cd /distr`
5. To start the uninstallation process run the following command:
   `bash ./iwtm-installer-x.x.x.xxx-rhel7.run -- --uninstall`
   As per our example:
   `bash ./iwtm-installer-6.11.0.882-rhel7.run -- --uninstall`

   Warning:

   Running the command makes the server returning in the state before the installation of InfoWatch Traffic Monitor.

   Preparation to uninstall the Sytem will start.
6. After the preparation is finalized, you will see a notification informing about Traffic Monitor and database removal as well as return to initial system configuration.



To continue enter "**Y**" and press **Enter**.
Traffic Monitor services will be stopped, then the System and database packages will be removed.
The progress will be displayed.
Wait until the end of uninstalling process.

Note:

If you've used a distributed installation of Traffic Monitor, the actions described above should be done on each Traffic Monitor server (TM Node) as well as database server (DB Node).

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:

1. Capital letters in Latin characters (A-Z)
2. Lowercase letters in Latin characters (a-z)
3. Arabic numerals (0-9)
4. 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