

INFOWATCH

InfoWatch Traffic Monitor 7.2

Installation Guide

05/30/2022

© 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

2.1.1 Database template 5

2.1.2 Indexer template 6

2.1.3 Web console template 7

2.1.4 Interceptors template 8

2.1.5 Traffic Monitor primary editions 10

2.2 Hardware and Software Requirements 13

2.3 Operating System and Network Server Configuration Requirements 20

2.4 Configuring Remote Database 22

3 Installing the System 26

3.1 Installing Traffic Monitor Server and Database 27

3.1.1 All-in-one Installation Mode of TM Enterprise and TM Standard 27

3.1.2 Distributed Installation of TM Enterprise 43

3.1.3 Installing the System in silent mode using parameter file 76

Parameter file (option file) 77

Silent mode installation 78

Full composition of parameter file 79

3.2 Installing Crawler Subsystem 91

3.3 Installing InfoWatch Device Monitor 97

3.3.1 InfoWatch Device Monitor Server End Setup 98

Database Deployment Managed by Microsoft SQL Server DBMS 98

Database deployment managed by Oracle DBMS 99

Database deployment managed by PostgreSQL DBMS 100

Server Setup Recommendations 100

InfoWatch Device Monitor Server End Installation Procedure 101

3.3.2 InfoWatch Device Monitor Agent Installation 110

Standard Agent Installation 112

Agent Installation via Software Distribution Tools 113

3.3.3 Deployment Scheme for InfoWatch Device Monitor 117

3.4 Pre-installed Server Parameters 120

4 Updating the System 123

4.1 Updating TM All-in-one Enterprise and Standard 127

4.1.1 Parameter file (option file) 148

4.1.2 Silent mode installation 148

4.1.3 Full composition of parameter file 150

4.1.4 Parameter file (option file) 165

4.1.5 Silent mode installation 166

4.1.6 Full composition of parameter file 167

4.2 Updating TM in case of Distributed Installation 175

4.2.1 Parameter file (option file) 197

4.2.2 Silent mode installation 198

4.2.3 Full composition of parameter file 199

4.3 Updating Crawler Subsystem 207

4.4 Updating InfoWatch Device Monitor 208

4.4.1 Updating InfoWatch Device Monitor Server End 208

4.4.2 Updating InfoWatch Device Monitor Agent 210

4.5 Merging Configuration Files 211

4.5.1 Automatic merge of Traffic Monitor configuration files 211

4.5.2 Merging configuration files in Midnight Commander 213

4.5.3 Merging configuration files by means of vimdiff 215

5 Uninstalling the System 216

5.1 Deleting the Database Scheme 216

5.2 Deleting Crawler Subsystem 217

5.3 Uninstalling Device Monitor 217

5.3.1 Remove Agent Installed via Software Distribution Tools 219

5.4 Uninstalling Traffic Monitor 219

6 Appendix A. Username and Password Recommendations 222

7 Appendix B. Licenses for Third-Party Technologies 224

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 Configuration Requirements;
- Configuring Remote Database.

2.1 System Deployment Schemes and Installation Types

InfoWatch Traffic Monitor System can be delivered in several variants. The features depend on the installation mode, the database in use (Oracle / PostgreSQL), and the edition (Standard / Enterprise).

Traffic Monitor installation kit contains installation templates. Each template - is a set of components to be activated after the System is deployed. Sets of components are consistent with servers functional roles. Servers roles identified at installation stage facilitate the System deploy plan, reduce the time of installation and make it easy to operate. Using templates also makes it easier a large-scale System to be maintained.

Regardless the template selected, Traffic Monitor server will have all components installed and the template is used to define a set of components activated.

One server can have few templates at the same time.

There are four templates available to install:

- **Database**;
- **Indexer service**;
- **Web console**;
- **Traffic interceptors**.

> **Warning!**
>
> **Database**, **Indexer service** and **Web console** templates should be the only one as per one cluster.

2.1.1 Database template

This template components include DBMS and modules to interact with remote database in case you expect the connection to database which is already being used.

The modules active in this template, provide the storage of information about intercepted objects, data analysis results and policies application. The template components let you view the information stored via queries made in Traffic Monitor Management console.

The following processes are included to Database template:

Process name	Purpose brief description
`iw_agent`	Required to manage System's configuration
`iw_blackboard`	Responsible for:

Process name	Purpose brief description
	• adding/removing status to persons/workstations from policies; • adding new contacts; • adding new applications to automatic tips search; • adding notifications from policies to queue.
`iw_qmover_server`	Receiving objects from remote servers with `qmover_client` t o transfer to database. Disabled by default
`iw_system_check`	System state control
`iw_x2db`	Downloads objects to database
`iw_x2x`	Converts objects from interceptors to standardized format. Sends modified data to `iw_x2db` process

2.1.2 Indexer template

The template contains components to index objects text, intercepted by System and stored in database. Also, the template components are used to index interception events and audit events metadata. The template modules let using quries to search on the events. To perform fulltext search, a Sphinx mechanism is used.

The following processes are included to Indexer template:

Process name	Purpose brief description
`iw_agent`	Required to manage System's configuration
`iw_indexer`	Used to perform a fulltext search on the events
`iw_is`	Performs metadata indexing
`iw_metainfo_fetcher`	Data sampling to index from database
`iw_system_check`	System state control

Warning!

The following processes should be the only one as per one cluster:

- `iw_indexer`;
- `iw_is`.

Otherwise, there will be data inconsistencies in the System.

2.1.3 Web console template

The template contains components of Traffic Monitor Management console - graphical user interface. Also, this template includes text and graphical objects classifiers and license components.

When using a Management console you can administrate and manage Traffic Monitor to do the monitoring of summary, policies and protected objects created, contacts added, events review, data unloading and reports creation.

The following processes are included to Web console template:

Process name	Purpose brief description
`iw_adlibitum`	Provides integration with LDAP catalogues
`iw_agent`	Required to manage System's configuration
`iw_blackboard`	Responsible for: • adding/removing status to persons/workstations from policies; • adding new contacts; • adding new applications to automatic tips search; • adding notifications from policies to queue.
`iw_bookworm`	Used as System directory
`iw_configerator`	Builds configuration for Device Monitor
`iw_deliver`	Dispatches e-mail messages from quarantine as per Security officer solution
`iw_image_autoling`	Automatic classification of graphical objects
`iw_kicker`	Component interacts with other services and is required to/for: • import/export configuration; • add sample documents; • operation of `iw_image_autoling` and `iw_text_autoling` processes; • make notifications; • reports and queries operation; • Crawler subsystem operation.
`iw_licensed`	License management
`iw_sample_compiler`	Makes digital fingerprints from downloaded sample documents
`iw_system_check`	System state control

Process name	Purpose brief description
`iw_tech_tools`	Help utilities for content analysis module
`iw_text_autoling`	Automatic classification of text objects
`iw_updater`	Downloads configuration from database
`iw_warpd`	Manages text data extraction from intercepted objects

Warning!

The following processes should be the only one as per one cluster:

- `iw_adlibitum`;
- `iw_bookworm`;
- `iw_configerator`;
- `iw_deliver`;
- `iw_image_autoling`;
- `iw_kicker`;
- `iw_licensed`;
- `iw_text_autoling`.

Otherwise, there will be data inconsistencies in the System.

2.1.4 Interceptors template

The template contains the modules responsible for data collection and analysis, policies appliance. The template components provide with in stream/at the gateway traffic Interception sent via protocols:

- SMTP;
- POP3;
- HTTP;
- HTTPS;
- OSCAR;
- NRPC;
- IMAP;
- ICAP.

Also, the template components may interact with Device Monitor subsystems and Crawler. The template components may also interact with external systems, the special adapters, used for this purpose. Unlike the others, Interceptors template can be installed few times within one cluster. Using it you can easily scale the System. To provide processes effective operation which are high loading the server, you are recommended using few Traffic Monitor servers with this template.

The following processes are included to Interceptors template:

Process name	Purpose brief description
`iw_agent`	Required to manage System's configuration
`iw_analysis`	Used to perform objects content analisys from `iw_proxy_icq` and `iw_proxy_http` processes
`iw_blackboard`	Responsible for: • adding/removing status to persons/workstations from policies; • adding new contacts; • adding new applications to automatic tips search; • adding notifications from policies to queue.
`iw_capstack`	Processes traffic sent via POP3, IMAP, NRPC protocols. Disabled by default
`iw_cas`	Intercepted data context analysis
`iw_icap`	HTTP traffic processing, which was received from ICAP client
`iw_messed`	Used to process SMTP messages
`iw_pas`	Service to process data after analysis
`iw_proxy_icq`	Receives copy of ICQ traffic in copy mode. Disabled by default
`iw_proxy_http`	Receives copy of HTTP traffic in copy mode. Disabled by default
`iw_proxy_smtp`	Receives copy of SMTP traffic in copy mode. Disabled by default
`iw_qmover_client`	Client part of module to send objects to remote database. Disabled by default
`iw_sniffer`	Receives copy from switcher's SPAN port. Disabled by default
`iw_smtpd`	Receives SMTP messages
`iw_system_check`	System state control
`iw_updater`	Downloads configuration from database
`iw_warpd`	Manages text data extraction from intercepted objects
`iw_xapi_xapi`	Receives objects from Infowatch Device Monitor
`iw_xapi_puppy`	Receives objects from external systems

Process name	Purpose brief description
`iw_x2db`	Downloads objects to database
`iw_x2x`	Converts objects from interceptors to standart format. Resends modified data to `iw_x2db` process

Note:

See the description of processes in «*InfoWatch Traffic Monitor. Administration Guide*», "List of Traffic Monitor Server End Processes".

2.1.5 Traffic Monitor primary editions

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 on our official site). 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:
- **Separate Traffic Monitor Server with templates:**
  - **Database**;
  - **Indexer service**;
  - **Web console**;
  - **Traffic interceptors**.

    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.
  - **Adapters** are a set of interception modules for integration with external systems.

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	Limited by storage size only		Limited by storage size only

Feature	TM Enterprise	TM Standard
intercepted data		
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:

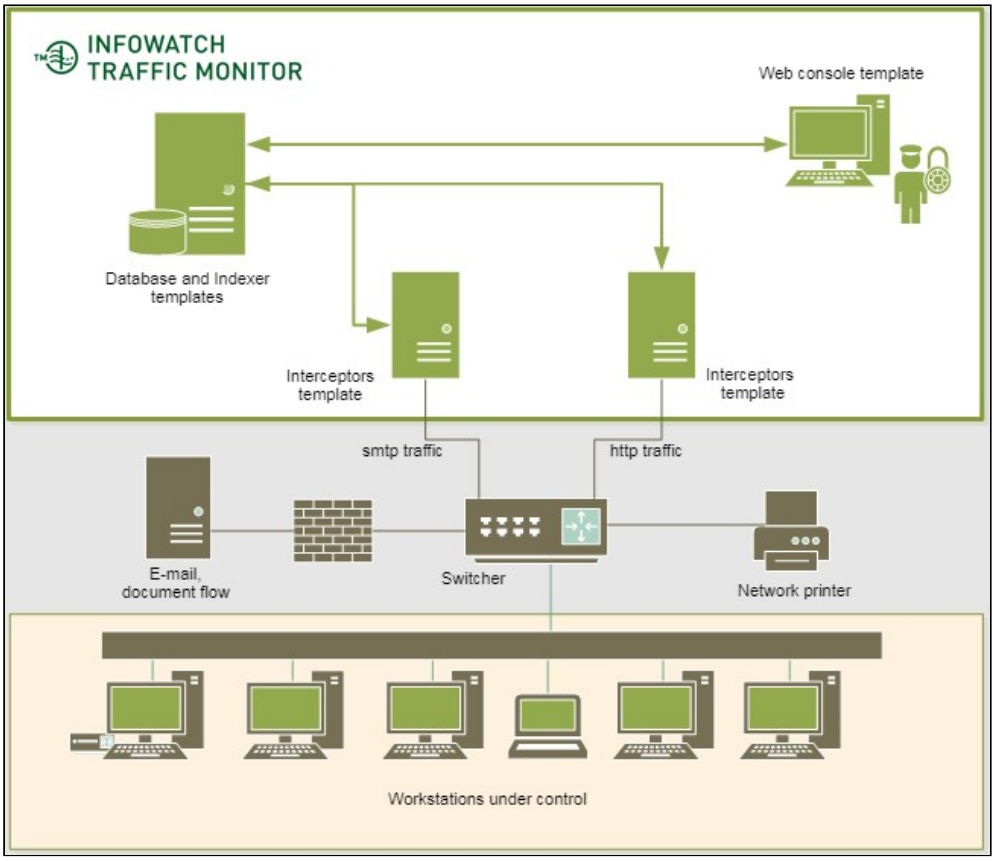
- *All-in-one Standard* – all the System components (together with Oracle Standard or PostgreSQL DBMS) are installed on the same server. This installation type is used if, with respect to the assumed load, the server has resources for DBMS and TM services.
- *All-in-one Enterprise* – all the System components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

Examples of System deployment using Traffic Monitor installation templates

Example 1:

The System is installed on 4 servers:

1. Server with Database and Indexer templates.
2. Server with Web console template.
3. Two servers with Interceptors template.

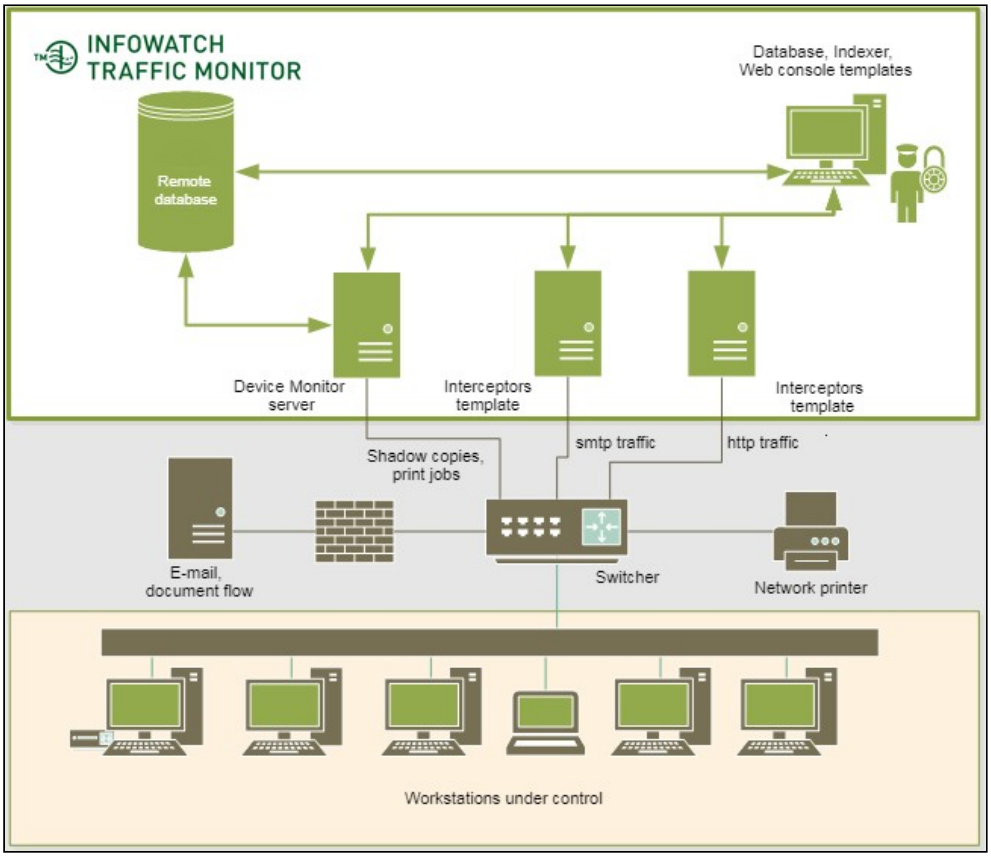


In the example below the Interceptors are installed on two servers to separate the load. According to interception purposes on each server you can disable interception modules which are not used.

Example 2:

The System is installed on 4 servers:

1. Server with Database, Indexer and Web console templates. Database template is installed connected to remote database, where Traffic Monitor security scheme is installed.
2. Two servers with Interceptors template.
3. Device Monitor server.



Interceptors are separated on two servers, remote database is used and Device Monitor Agents are operating on workstations under control.

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 based 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 Standard 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 the 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 the 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 the update; • CentOS 7.x starting from version 7.7. • OS Oracle Linux 7.x starting from version 7.7.	The server should have a network interface with the assigned IP address. If interceptors are used on the server, requirements imposed by the interceptors should be fulfilled*
TM Enterprise server, less than 10 GB per day				
RAID-array with fault tolerance: 600 GB	2CPU 8xC + Hyper-threading (Intel® Xeon®	24 GB	• OS Red Hat Enterprise Linux 7.x (the latest	The server should have a network

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
	Processor E5-2640 v3 - 2,6 Hz)		version) with subscription, required for the update; • CentOS 7.x starting from version 7.7; • OS Oracle Linux 7.x starting from version 7.7.	interface with the assigned IP address. 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	2SRVx2CPU 10xC	32-48 GB for each server	• OS Red Hat Enterprise Linux 7.x (the latest version) with subscription, required for the update; • CentOS 7.x starting from version 7.7. • OS Oracle Linux 7.x starting from version 7.7.	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 the update; • CentOS 7.x starting from version 7.7.; • OS Oracle Linux 7.x	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*

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
			starting from version 7.7.	
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)				
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 should be provided for logs storage.	2CPU от 6xC, 2,6 GHz	16GB and more depending on data volume, insertion and processing speed	OS Red Hat Enterprise Linux 7.x (the latest version) with subscription, required for the update	
Warning! When installing the System on CentOS starting from version 7.7, you should select PostgreSQL as a DB server.				
Crawler server and scanner				
30 GB of free space - for the server and the scanner: required for the temporary storage of files that are copied from checked resources and for installation purposes	From 2 cores	From 2 GB	OS: • Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8; • Microsoft Windows Server 2008 R2 Service Pack 1; • Microsoft Windows	• **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

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
			Server 2012 R 2; • Microsoft Win dows Server 2016; • Microsoft Win dows Server 2019. Platform: • Microsoft .Ne t Framework 4.5.1.	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 the 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. • Traffic Monitor and Crawler are compatible within the same version.

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
Device Monitor server				
Not less than 1 GB of 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; • Microsoft Windows Server 2019. Platform: • Microsoft .Net Framework 4.5.1. DBMS: • Oracle Database 19; • Microsoft SQL Server 2005, 2008, 2012, 2014, 2016, 2017, 2019 (Standard, Enterprise); • PostgreSQL version 13.	▪ 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				
Not less than 1 GB free space required for installation/ Also the free space is	From 2 cores	From 2,5 GB	OS:	• Local DNS is required to convert domain

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
required for files temporary storage, which are to be sent for analysis.			• [1]Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 и 8.1; • Microsoft Windows 10; • [1]Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019.	names into addresses • TLS 1.2 should be supported
Device Monitor Management Console				
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; • Microsoft Windows Server 2016;	

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
			• Microsoft Windows Server 2019; • Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 and 8.1; • Microsoft Windows 10.	

Note!

[1] - marked operating systems require the following Microsoft updates: KB4474419, KB4490628. The System is intended to check the computer for bug fix before starting the installation and/or update.

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 Microsoft RDS, Citrix XenApp 6.0, 7.6, 7.13, 7.14, and 7.15 LTSR virtualization environments.

* 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 the IW ICAP module. The proxy server should contain ICAP license; enabling ICAP support is performed according to support documentation of a 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:

- Server should have
  OS Red Hat Enterprise Linux 7.x (last version)

Note:

You can install the System on OS CentOS starting from version 7.7. Thus use all the following instructions on System installation and operation.

Note:

You can also install the System on OS Oracle Linux. Thus use all the following instructions on System installation and operation.

Warning!

When downloading OS Oracle Linux, please select Red Hat Compatible Kernel (RHCK), namely Oracle Linux Server 7.9, with Linux 3.10.0-1160.el7.x86_64

- OS repositories should be configured to install the packages `redhat-lsb-core` and `lshw`. See how to configure a local repository on the Red Hat Enterprise Linux official website.The following common repositories should be available:
  - `os`;
  - `updates`;
  - `optional`.

Note:

If you install Traffic Monitor on the server with no internet access, please make sure the offline access to specified repositories was provided.

For example, you can configure local repositories mirrors.See how to configure a local repository mirror on the Red Hat Enterprise Linux official website.

Warning!

Before installing the System on OS Oracle Linux make sure the internet connection is available with no interruptions.

Warning!

When working with OS Oracle Linux make sure, that:

- Repositories to install ISO Oracle Linux 7.9 are connected;
- the rest Oracle Linux repositories are connected. The data are written within `/etc/yum.repos.d/` repository by default;
- `/etc/yum.repos.d/` repository parameters are set to `enabled` status.

- 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.

2.4 Configuring Remote Database

If you plan using a database, which is already deployed, you have to do the following:

1. Update the database to version, supported by Traffic Monitor.
2. In case you use PostgreSQL DBMS, make the preliminary configuration.

To prepare a remote database of relevant version so that Traffic Monitor components were installed, the following actions should be taken on database server:

1. Install additional packages, running the commands:
   ```
   rpm -Uhv pg_stat_kcache13-2.1.3-1.rhel7.x86_64.rpm
   rpm -Uhv pg_pathman_13-1.5.12-1.rhel7.x86_64.rpm
   rpm -Uhv pgagent_13-4.0.0-4.rhel7.x86_64.rpm
   ```
2. Stop `postgresql` and `pgagent` services operation using the commands:
   ```
   systemctl stop postgresql-13
   systemctl stop pgagent-13
   ```
3. Edit the file's content `/etc/systemd/system/postgresql-13.service` , replacing a specififed directory to `/u01/postgres` in `Environment=PGDATA=` line.
4. To apply changes to service configuration, run the command:
   ```
   systemctl daemon-reload
   ```
5. Create directories for files and archives, initialize the database and change the directory's owner as well as the group to `postgres` :
   ```
   mkdir -p /u01/postgres
   chown postgres:postgres /u01/postgres
   export PGSETUP_INITDB_OPTIONS=" --encoding=UTF8"
   /usr/pgsql-13/bin/initdb --encoding=UTF8 --locale=en_US.UTF-8 -D /u01/
   postgres/
   mkdir -p /u01/postgres/tmp
   chown postgres:postgres /u01/postgres/tmp
   mkdir -p /u02/pgdata
   chown postgres:postgres /u02/pgdata
   ```

```
mkdir -p /u02/pgdata1
chown postgres:postgres /u02/pgdata1
mkdir -p /u02/arch
chown postgres:postgres /u02/arch
```

6. Create a configuration file `/u01/postgres/iwtm-postgres.conf`. For example, use the command as follows:
   ```
   touch /u01/postgres/iwtm-postgres.conf
   ```
7. Add to file `/u01/postgres/iwtm-postgres.conf` the following content:

```
# ------------------------------
# PostgreSQL configuration file
# ------------------------------
#
# IWTM custom values
listen_addresses = '*'
port = 5433
max_connections = 1000 # (change requires restart)
tcp_keepalives_idle = 60 # TCP_KEEPIDLE, in seconds'
tcp_keepalives_interval = 20 # TCP_KEEPINTVL, in seconds'
tcp_keepalives_count = 2 # TCP_KEEPCNT
shared_buffers = kB
huge_pages = try # on, off, or try
max_locks_per_transaction = 512
temp_buffers =  MB
work_mem = MB
effective_cache_size = MB
min_wal_size = MB
max_wal_size = MB
log_min_duration_statement = 120000 # -1 is disabled, 0 logs all statements
track_activity_query_size = 32768 # (change requires restart)
log_autovacuum_min_duration = 30000 # -1 disables, 0 logs all actions and
stats_temp_directory = '/u01/postgres/pg_stat_tmp'
autovacuum_max_workers = 5
autovacuum_naptime = 20
maintenance_work_mem = GB
autovacuum_freeze_max_age = 1000000000
shared_preload_libraries = 'pg_stat_statements,pg_stat_kcache,pg_pathman'
track_io_timing = on
track_activity_query_size = 32768
constraint_exclusion = off # on, off, or partition
```

Warning!

The configuration file's content above contains empty value fields as per parameters:

- `shared_buffers`
- `work_mem`
- `maintenance_work_mem`
- `effective_cache_size`
- `temp_buffers`

- `min_wal_size`
- `max_wal_size`

Configure these parameters according to official instructions.

8. Change the configuration file's owner and group to `postgres`:
   `chown postgres:postgres /u01/postgres/iwtm-postgres.conf`
9. Add to `/u01/postgres/postgresql.conf` a link to `iwtm-postgres.conf` file using the command:
   `echo "include = 'iwtm-postgres.conf'" >> /u01/postgres/postgresql.conf`
10. Configure the access file `pg_hba.conf` using the commands:
```
sed -i "s|local[[:space:]]*all[[:space:]]*all[[:space:]]*peer|local   all
          all                                    trust|" /u01/postgres/
pg_hba.conf
sed -i "s|
host[[:space:]]*all[[:space:]]*all[[:space:]]*127.0.0.1/32[[:space:]]*ident
|host    all             all             127.0.0.1/32            trust|" /
u01/postgres/pg_hba.conf
sed -i "s|
host[[:space:]]*all[[:space:]]*all[[:space:]]*::1/128[[:space:]]*ident|
host    all             all             ::1/128                 trust|" /
u01/postgres/pg_hba.conf
echo "# Enable not local access" >> /u01/postgres/pg_hba.conf
echo "host    postgres        all             0.0.0.0/0               md5"
>> /u01/postgres/pg_hba.conf
```
11. Run `postgresql` service and check its status using the commands:
```
systemctl enable postgresql-13
systemctl start postgresql-13
systemctl status postgresql-13
```
12. Change the DB administrator's default password:
```
su - postgres
psql -p 5433
alter user postgres password 'xxXX1234';
```
13. Create all required expansions running the queries below:
```
create extension if not exists adminpack;
create extension if not exists dblink;
create extension if not exists lo;
create extension if not exists xml2;
create extension if not exists tablefunc;
create extension if not exists intarray;
create extension if not exists file_fdw;
create extension if not exists "uuid-ossp";
create extension if not exists pgcrypto;
create extension if not exists pgrowlocks;
create extension if not exists autoinc;
create extension if not exists hstore;
create extension if not exists pg_stat_statements;
create extension if not exists pg_buffercache;
create extension if not exists pg_stat_kcache;
create extension if not exists pg_pathman;
create extension if not exists pgagent;
```

14. To exit enter the commands:
    `\q`
    `exit`
15. To configure `pgagent` in user OS run the commands:
    `touch /home/pgagent/.pgpass`
    `echo "127.0.0.1:5433:postgres:postgres:xxXX1234" > /home/pgagent/.pgpass`
    `chmod 0600 /home/pgagent/.pgpass`
    `chown pgagent:pgagent /home/pgagent/.pgpass`
    `usermod -s /bin/bash pgagent`
16. Create or edit the file `/etc/sudoers.d/pgagent` to make the following content:

```
# allow pgagent to execute any command
pgagent ALL = (postgres) NOPASSWD: ALL
Defaults:pgagent !requiretty
```

17. Change the privilleges, owner and group as per `/etc/sudoers.d/pgagent` running the commands:
    `chmod 440 /etc/sudoers.d/pgagent`
    `chown root:root /etc/sudoers.d/pgagent`
18. Run `pgagent` service and check its status using the commands:
    `systemctl enable pgagent-13`
    `systemctl start pgagent-13`
    `systemctl status pgagent-13`

Finalising the configuration make sure there are no critical errors in `/var/log/pgagent-13.log` .
and database logs.

3 Installing the System

This section contains instructions for each type of System installation.

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

Warning!

Before starting 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.

Traffic Monitor installer contains installation templates. Depending on the server purpose, a different set of components is to be installed.

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

Besides the installation from server console a graphical mode of installation is available. How to run the installer in graphical mode you can find in related installation articles.

You can also install Traffic Monitor in silent mode using a paremeters file `.options`. You can prepare the files where all required parameters are specified. Then you should copy these files together with Traffic Monitor distribution kits to servers where the System is planned to deploy. After this, you can run the installation on servers in silent mode, specifying the proper parameters files. Using it together with installation templates you can reduce the user role in System's primary deployment.

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

- Installing Traffic Monitor Server and Database
  - All-in-one Installation Mode of TM Enterprise and TM Standard
  - Distributed Installation of TM Enterprise
  - Installing the System in silent mode using parameter file
  - Installing InfoWatch Device Monitor (optional)
  - Installing Crawler Subsystem (optional)

Note:

During IW Traffic Monitor installation the operations that require sysdba rights will be performed:

Oracle DBMS

- Creation of iwtm_logon_trg trigger which is used to provide iwtm_linux and iwtm_web users access to objects of iwtm scheme;
- Creation of sp_iwtm_execute_os_command procedure to run OS commands when creating, removing, archiving and restoring table space files;
- Setting user profile by default (password lifetime, password change limit and connection attempts limit);
- Setting sevice windows of dbms_scheduler;
- Disabling access to XDB using http protocol;
- Disabling dispatcher, as a particular server is used;
- Providing iwtm user with:
  - DB installation, update and uninstallation rights;
  - Daily tablespaces creation, removing, archiving and restoring rights;

- Rights that are used in InfoWatch Traffic Monitor code;
- Rights to access DB statistics.

PostgreSQL DBMS

- Creation of wraper function to read files, stop and break sessions, create table spaces and provide iwtm with rights for them;
- Removing all views and functions from iwtm scheme in order to create the required ones later during update to a new version;
- Providing iwtm user with:
  - Rights to create DB objects;
  - Rights to install, update, ininstall DB scheme;
  - Rights to create, remove, archive and restore tablespaces;
  - Rights to clear postgres server statistics that are used in pgstat diagnostics script;
  - Rights for statistic views and tables to collect statistics of DB operation;
  - Rights that are used in InfoWatch Traffic Monitor code;
  - Rights to view DB statistics;
  - Rights for pgagent scheme to create and manage jobs.

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.

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:

- All-in-one Installation Mode of TM Enterprise and TM Standard
- Distributed Installation of TM Enterprise
- Installing the System in silent mode using parameter file

3.1.1 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. This type of installation is smilar to all templates installation on the same computer. The packages unpack will start before the installation process after all the perameters are specified.

Warning!

By default you are not allowed to install the System on server which has numbers at the beginning of its name. If you need to allow the server's name to begin with a number, use the command line to specify the value `1` of the parameter `--allow_digits_at_hostname_begin`.

Herewith, make sure that the network check is active – the parameter `--skip_check_network` should have the value `0` (the check is active by default).

The Traffic Monitor installer can work in two modes involving user:

- text mode in server console;
- graphical mode.

The installation steps and its sequence is similar in both modes.

Regardless the selected mode of installation, please take the following common actions:

1. To log into the System, enter login and password (you should enter as a **`root`** user).

   > **Warning!**
   >
   > Before running the installation make sure that the server complies with the OS and network settings requirements.
   > If you plan using a remote database, you should update it first to the version supported by Traffic Monitor. In case of PostgreSQL DBMS using, you should preliminarily configure it.
   >
   > Before installing to clear memory, it is recommended to reboot the server on which database will be deployed.

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`** (where x.x.x.xxx is a number of build);
   - **`iwtm-postgresql-13.2-x.xx.x.tar.gz`** - if you use PostgreSQL DBMS;
   - **`iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz`** - if you use Oracle DBMS.

   As per our example:
   - **`iwtm-installer-7.2.0.123-rhel7`** ;
   - **`iwtm-postgresql-13.2-7.2.0.tar.gz`** - if you use PostgreSQL DBMS;
   - **`iwtm-oracle-19.0.0.0.0-7.2.0.tar.gz`** - if you use Oracle DBMS.

   > **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. Before running the installation make the installer file executable. To do this use the following command :
   `chmod u+x ./iwtm-installer-x.x.x.xxx-rhel7`

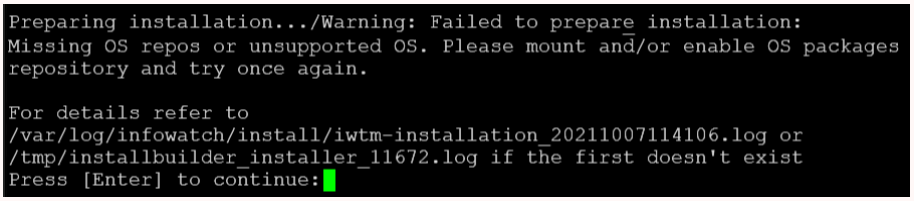
As per our example:

```
chmod u+x ./iwtm-installer-7.2.0.123-rhel7
```

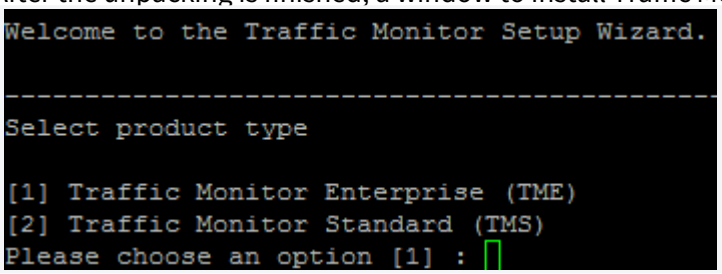
Installing in text mode using server console

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

1. Start the Traffic Monitor installer running the command:
   `./iwtm-installer-x.x.x.xxx-rhel7`
   Our example command:
   `./iwtm-installer-7.2.0.123-rhel7`
   Preparations will be made to start the installation. At this stage the unpacking of Traffic Monitor installation files is not performed.

   > **Warning!**
   >
   > If available configured OS repositories are missing, the preparation process will stop with the following error message:
   >
   > 
   >
   >
   > To fix this error press **Enter** to exit, connect the standard RHEL repository, EPEL repository and restart the installer.
   >
   > For more details on the error refer to the log files, specified in the error message.

   After the unpacking is finished, a window to install Traffic Monitor will be displayed:

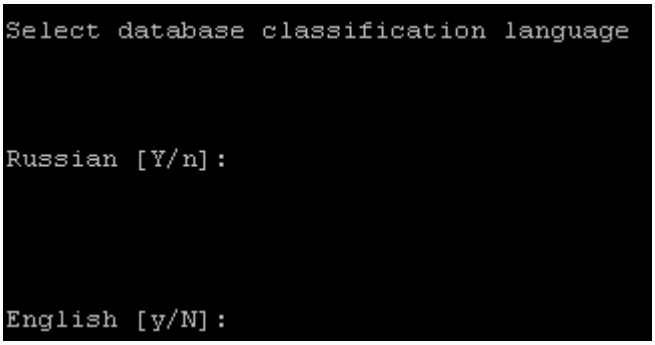
2. Select Traffic Monitor edition type:
   - **`Traffic Monitor Enterprise (TME)`** to install Enterprise edition;
   - **`Traffic Monitor Standard (TMS)`** to install Standard edition.

   > **Warning!**
   >
   > When you install **`Traffic Monitor Standard (TMS)`** edition, you can select only PostgreSQL database.

   For this, type the figure specified next to option selected, and press **Enter**.

> **Note:**
>
> When installing via server console you can see the default value which is specified in square brackets next to input field. This value will be used in case of leaving the field empty and pressing **Enter**.
>
> **Пример**
>
> If you do not input a value as per picture above and press Enter, the item `[1] Traffic Monitor Enterprise (TME)` will be selected.

3. If **`Traffic Monitor Enterprise (TME)`** edition was selected, in the window of installation type select **`All-in-one`**.
4. Then select the main language of user interface management console, as well as date and time displaying format and preset configuration language:
   - **`Russian`**;
   - **`English`**.
5. Select the classification base language. A classification base includes preset policies, elements of technology configuration and protected objects. Yor can select few languages at once. Options will be consistently displayed. To use an option type **Y**, to refuse it type **N**, to confirm selected option press **Enter**.

> **Note:**
>
> When installing via server console you can see the default value which is specified in square brackets next to input field. This value will be used in case of leaving the field empty and pressing **Enter**.
>
> **Default value using example**
>
> 
>

   The following languages are available to select:
   - **`Russia`**;
   - **`English`**;
   - **`Malay`**.

   If you do not require to install a classification base, do not select any language.
6. Select the database storage type:
   - **`Install database server locally`** - to install locally on current server;
   - **`Use remote database server`** - to use on remotely deployed database. In this case the Traffic Monitor scheme will be added to remote database.
7. In case **Enterprise** edition is selected, select a database the System to operate with:
   - **`Oracle Database Enterprise Edition`**

- **PostgreSQL**

> **Note:**
>
> When installing to CentOS, the only supported database is PostgreSQL.

8. If you use a remote database, please enter consistently:
   a. IP address and database server domain name.
   b. Connection port
   c. The name of database to be used, where the scheme is to be added.
9. If required you can change the default values of DB authentication parameters.
   In case of positive answer the following parameters will be offered to change:
   - Password of user account having sysdba permissions;
   - Name of database schema owner;
   - Password of database schema owner's account;
   - Name of Linux services user account;
   - Password of Linux services account;
   - Name of web services user account;
   - Password of web services account;
   - Name of nagios user account;
   - Password of nagios account.
10. Select a data storage mode:
    - **Norma** l - (regular) - switching to the following partition (when it is specified) happens after the previous one is overflow.
    - **Fast/Slow disks** - dividing pools into fast and slow ones. Recent data are to be kept in fast pool and to be relocated to the slow ones in a number of days specified. Slow pool operates in `normal` mode.
    - **Rotate** - switching to the following partition happens every day once the previous one is overflow.
11. You can change the default values of database storage parameters.
    In case of positive answer you may change the following parameters:
    - **Main tablespaces path** - path to main tablespaces data storage directory;
    - If you've selected **Fast/Slow disks** mode:
      - **Fast disk path** - path to daily tablespace data storage directory in **F ast/Slow disks** mode;
      - **Number of days to store daily tablespaces on fast disk** - number of days to store in fast tablespaces in **F ast/Slow disks** mode;
    - **Number of daily tablespaces paths** - number of daily tablespaces paths, a number from 1 to 10;

      > **Note:**
      >
      > If you specify the value which is more than 1, then you should specify consistently the relevent number of pathes to daily tablespaces.

    - **Daily tablespaces paths** - path to daily tablespace data storage directory.
12. For daily tablespaces you can change the default values of archiving parameters.
    In case of positive answer:

- **Path to archiving** - path to archived tablespaces files storage directory.

The query to use each of the following parameters will be displayed in advance:

- **Archive non-violation events** - enable the automatic deletion of events that are considered non-violations. If enabled, please specify the the number of days after which the event will be automatically archived, by default - 45 days.
- **Archive violation events** - enable the automatic archiving of events that are considered violations. If enabled, please specify the number of days after which the event will be automatically archived, by default - 45 days.
- **Archive screenshots** - enable the automatic archiving of screenshots received from Device Monitor Agents. If enabled, please specify the number of days after which the event will be automatically archived, by default - 45 days.

13. Similar to previous point you can configure the deletion parameters for daily tablespaces. If enabled, the default value for all the parameters - 90 days.
14. Specify the parameters to connect to Consul service:
    a. **Network interface address** - select IP address of network interface.
    b. **Datacenter name** - input name of Consul data center.
15. Select the server to be used to synchronize the time (NTP-server):
    - **Use system NTP-server**;
    - **Set manually** - you can manually specify NTP server name. If selected, you should input IP address or NTP server available.
16. Then you can enable indexing of words exact match for Sphinx service.

> **Warning!**
>
> Enabling the indexing of words exact match will increase the size of index two times minimum.

17. If required, you can change the standard configuration of Sphinx service operation. In this case an offer to set a list of languages including morphological support will be displayed. Indexing will be performed according to selected languages. You can specify few languages using a space to separate them.

> **Note:**
>
> The language priority is in accordance with sequence of selected languages. English is to be added by default and it has the highest priority.

18. You can enable OCR technology. In this case you should select one system to be used:
    - **ABBYY FineReader**;
    - **Tesseract**.
19. If ABBYY Finereader is selected as OCR extractor:
    a. Select a recognition mode:
        - **Quick** – a fast mode;
        - **Quality** – a detailed mode providing higher quality of recognition.
    b. Confirm that you have an active license to use ABBYY Finereader. In case you have no active license, type **N** and press **Enter**. In this case ABBYY Finereader will be installed with no license. To use ABBYY Finereader you can manually add an active license later. For more details, please see "*InfoWatch Traffic Monitor. Administation Guide*" "Configuring OCR Extractors " article.

20. After all the parameters were set a message to start the installation and query to continue will be displayed.

```
Setup is now ready to begin installing Traffic Monitor on your computer.

Do you want to continue? [Y/n]:
```

Type **Y** to start the installation and press **Enter**.
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed.

```
Please wait while Setup installs Traffic Monitor on your computer.

 Installing
 0% _____________ 50% _____________ 100%
 ########################################
```

The process may take some time.

21. After the installation is complete you can delete the packages created to install the System. When installation is successfully completed the data is recommended to delete.

> **Note:**
>
> If Consul service is configured incorrectly, the following warning message will be displayed:
>
> ```
> \Warning: You should run 'iwtm start' command manually after fixing problems with
> Consul.
> Press [Enter] to continue:
> ```
>
> To finish installation press **Enter**.
>
> **For correct work of System check and configure Consul service cluster**
>
> a. Start Consul service with the command:
> `service iwtm-consul start`
> To check the service status enter the command:
> `service iwtm-consul status`
> b. To check Consul enter the command:
> i. To display IP address of main server (leader) of cluster:
> `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
> ii. To display information about cluster members:
> `consul members`
> c. If the IP address of cluster leader is not displayed, configure cluster of Consul service.
> After configuration is complete, repeat checking (step ii).
>
> If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

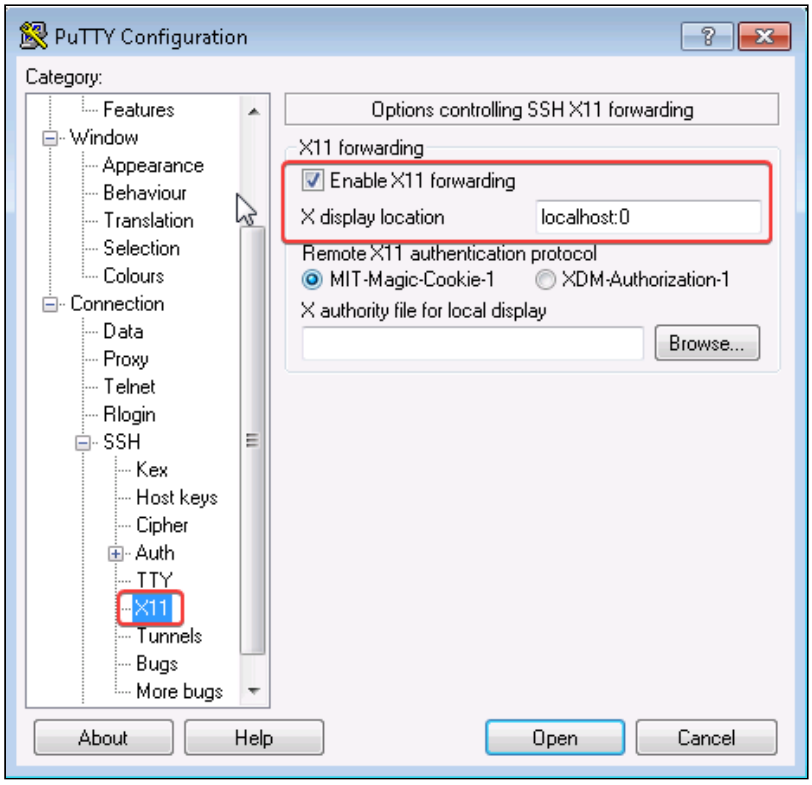
22. To apply the environment change you should certainly log off the System and log in again or restart the server.
23. If you require the list of Traffic Monitor services to be displayed enter the command as follows:
`iwtm status`

Installing in graphical mode

X Window System uses a client - server model. To run the installer in the graphical mode **X11 Forwarding** is used to forward the graphical output of remote system. This let you work directly with Linux graphical applications on the computer which is connected to server. This mode is implemented via SSH connection.

To install Traffic Monitor Enterprise or Traffic Monitor Standard in All-in-one mode using graphical mode of installation, take the folowing steps:

1. On the server, where Traffic Monitor components are planned to install:
   a. Install xauth utility using the command:
   `yum install xauth`
   b. In `/etc/ssh/sshd_config` configuration file uncomment the line "`X11Forwarding yes`". To do this, delete `#` placed before the line.
   c. Save changes in configuration file.
   d. Restart SSH service using the command:
   `systemctl restart sshd`
2. On the computer, where the graphical mode is to be used:
   a. To connect to Traffic Monitor installation server you will require a SSH client with enabled X11 Forwarding option, e.g. PuTTY.
   b. To start the installer in the graphical mode you will require an application configured to access to X Window System, for example:
      - Xming application - for OS MS Windows;
      - Gnome 3 shell - for OS Linux.
3. Run the application client which was previously configured to access to X Window System.
4. Connect to server, where Traffic Monitor components are planned to install, using selected SSH client.
   Example of PuTTY configuration window used to connect



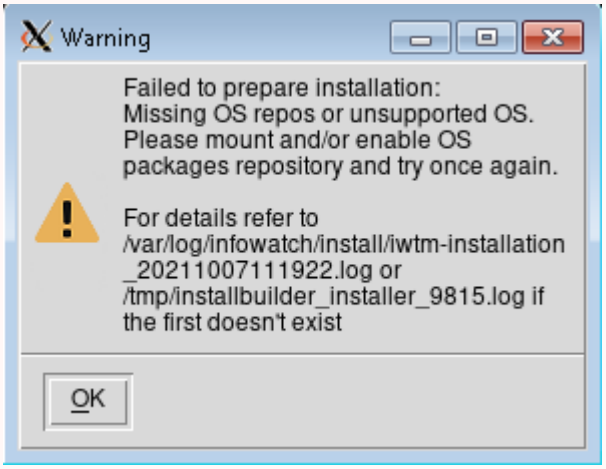
5. To install Traffic Monitor run the installer using the command:
   `./iwtm-installer-x.x.x.xxx-rhel7`
   As per our example:

`./iwtm-installer-7.2.0.123-rhel7`

Preparations will be made to start the installation. At this stage the unpacking of Traffic Monitor installation files is not being performed.

Warning!

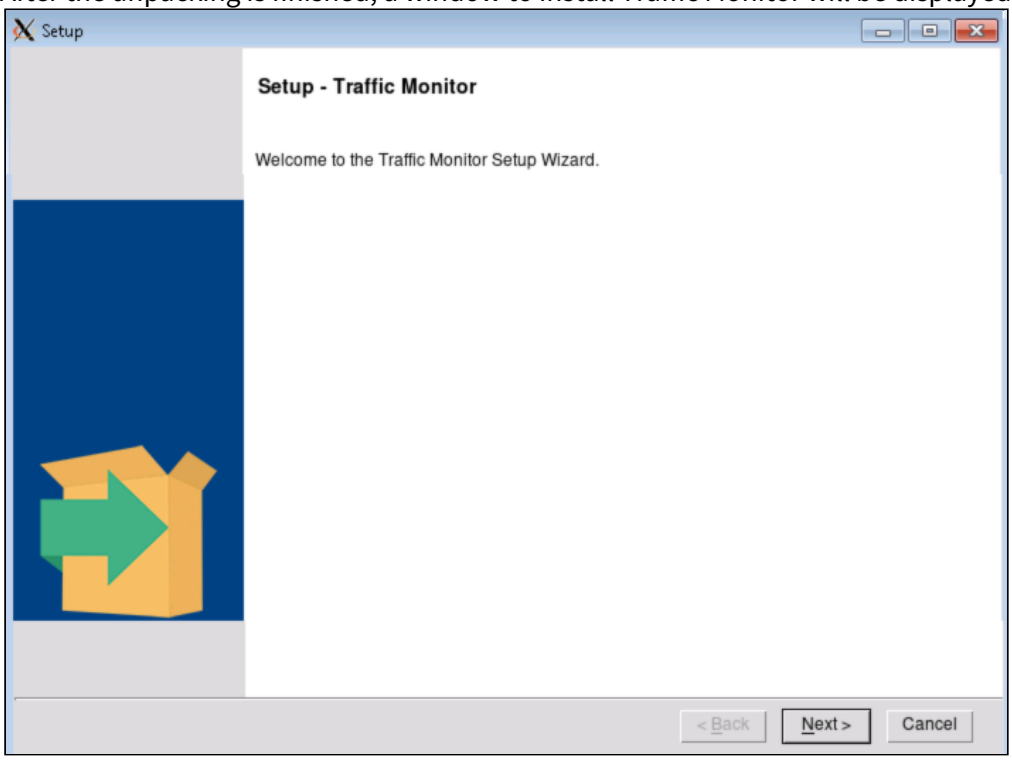
If available configured OS repositories are missing, the preparation process will stop with the following alert box:



To fix this error press **OK** to dismiss, connect the standard RHEL repository, EPEL repository and restart the installer.

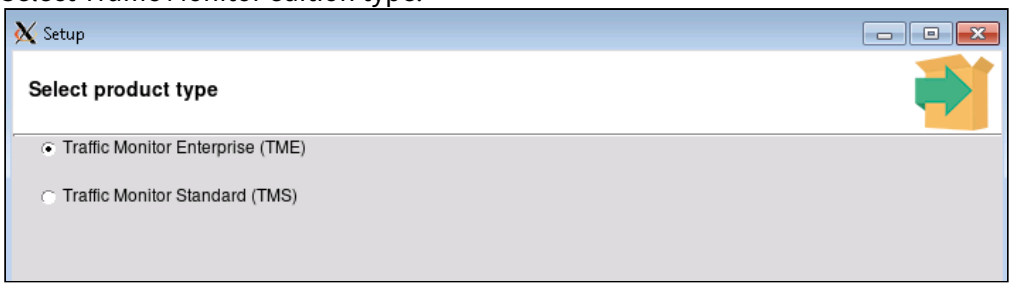
For more details on the error refer to the log files specified in the alert box.

After the unpacking is finished, a window to install Traffic Monitor will be displayed:



To go to the next parameter press **Next** button, to go back press - **Back**. To exit the installer press **Cancel** button.

6. Select Traffic Monitor edition type:

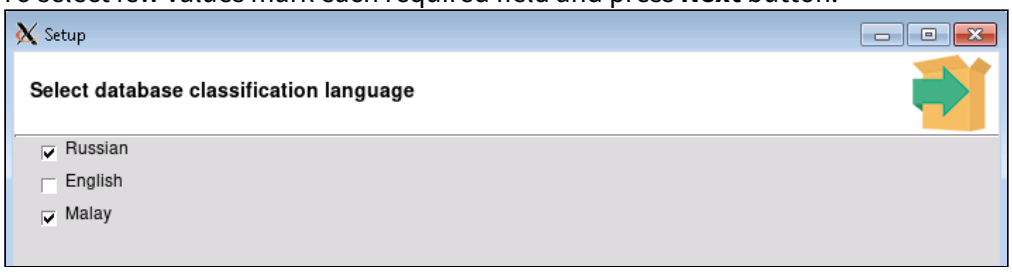


- `Traffic Monitor Enterprise (TME)` to install Enterprise edition;
- `Traffic Monitor Standard (TMS)` to install Standard edition.

> **Warning!**
>
> When you install `Traffic Monitor Standard (TMS)` edition, you can select only PostgreSQL database.

To select click in the checkbox next to required value and press **Next** button.

7. If `Traffic Monitor Enterprise (TME)` edition was selected, in the window of installation type select `All-in-one`.
8. Then select the main language of user interface management console, as well as date and time displaying format and preset configuration language:
   - `Russian`;
   - `English`.
9. Select the classification base language. A classification base includes preset policies, elements of technology configuration and protected objects. Yor can select few languages at once.
   To select few values mark each required field and press **Next** button.

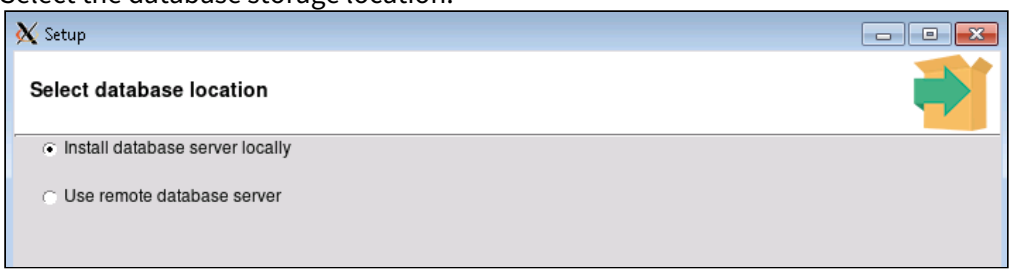


The following languages are available to select:

- `Russian`;
- `English`;
- `Malay`.

If you do not require to install a classification base, do not select any language.

10. Select the database storage location:

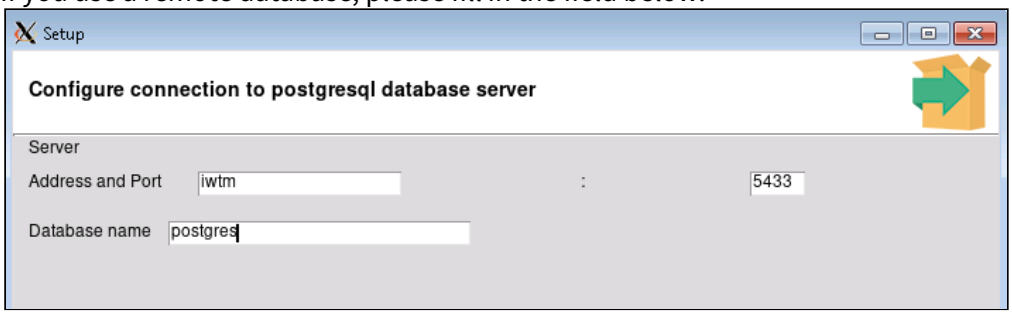


- **`Install database server locally`** - to install locally on current server;
- **`Use remote database server`** - to use on remotely deployed database. In this case the Traffic Monitor scheme will be added to remote database.

11. In case **Enterprise** edition is selected, select a database the System to operate with:
    - **`Oracle Database Enterprise Edition`**
    - **`PostgreSQL`**

> **Note:**
>
> When installing to CentOS, the only supported database is PostgreSQL

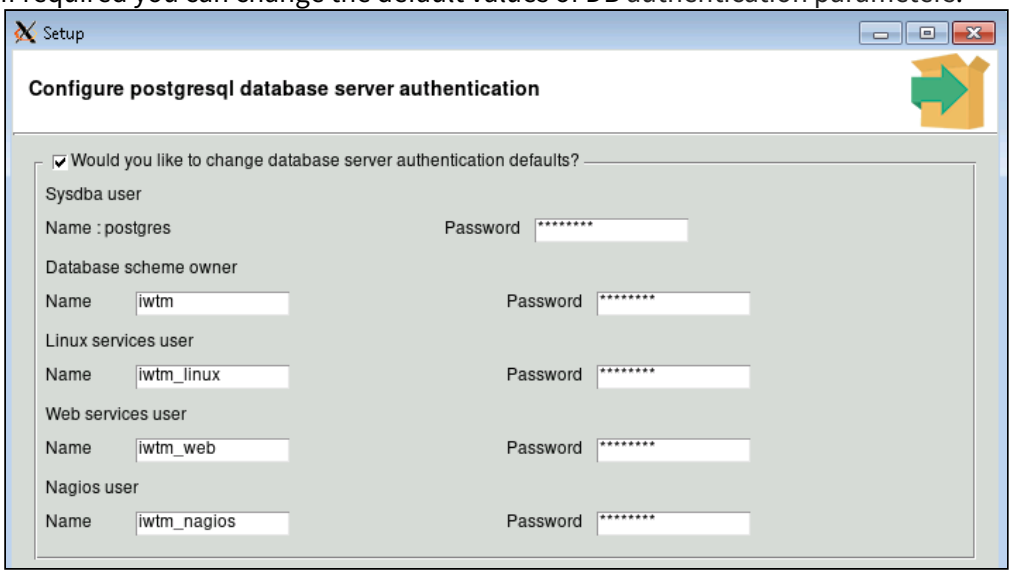
12. If you use a remote database, please fill in the field below:



    a. **`Address and Port`** - IP address or database server domain name and connection port.
    b. **`Database name`** - The name of database to be used, where the scheme is to be added.

> **Note:**
>
> In the graphical mode active fields contain the default values.

13. If required you can change the default values of DB authentication parameters.



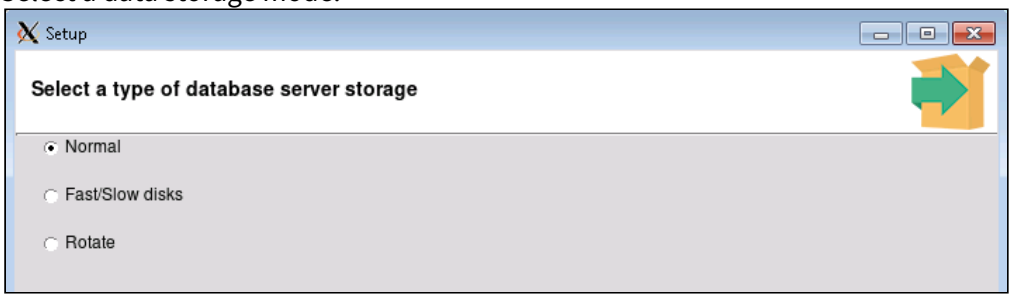
To edit the values mark the field next to question. This will let you edit the following sections:

- **`Sysdba user`** - Password of user account having sysdba permissions;
- **`Database scheme owner`** - Name and password of database schema owner;
- **`Linux services user`** - Name and password of Linux services user;

- **Web services user** - Name and password of web services user;
- **Nagios user** - Name and password of nagios user.

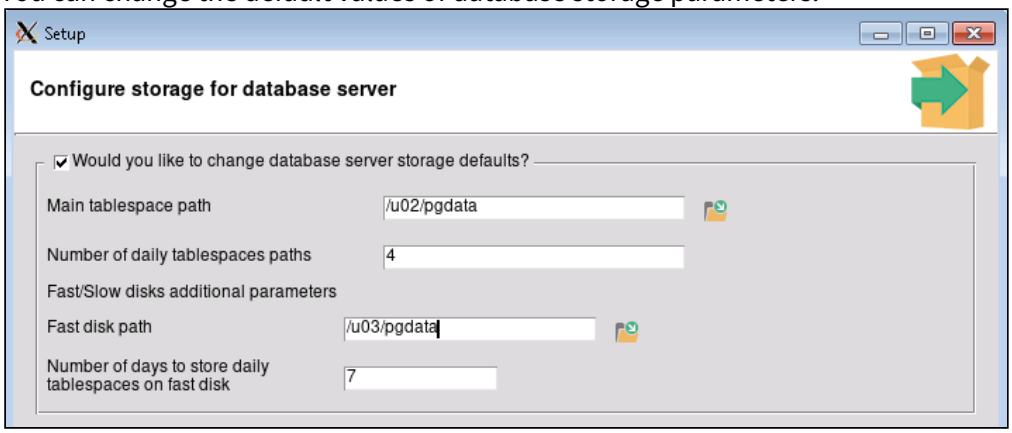
To leave the default values please do not mark the field and press **Next** button. In this case the fields cannot be edited and the installer will use the default parameters.

14. Select a data storage mode:



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

15. You can change the default values of database storage parameters.

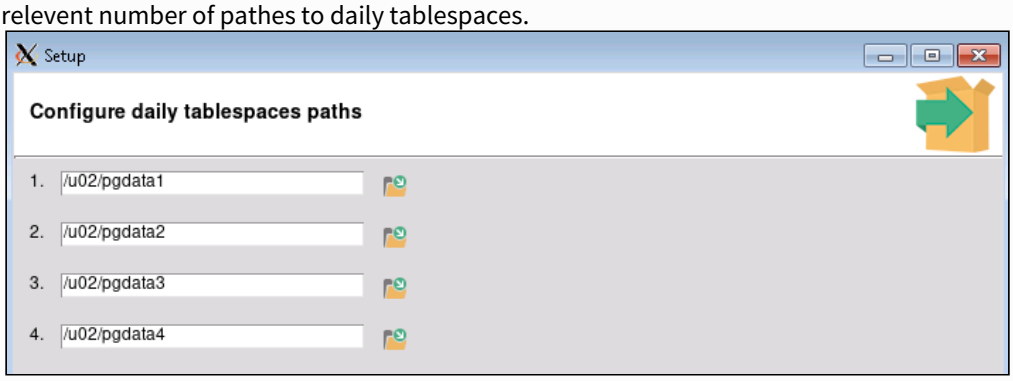


- **Main tablespaces path** - path to main tablespaces data storage directory;

  You can add the path to the field or specify it via file manager window using  button.
- If you've selected **Fast/Slow disks** mode:
  - **Fast disk path** - path to daily tablespace data storage directory in **F ast/Slow disks** mode;
  - **Number of days to store daily tablespaces on fast disk** - number of days to store in fast tablespaces in **F ast/Slow disks** mode;
- **Number of daily tablespaces paths** - number of daily tablespaces paths, a number from 1 to 10;

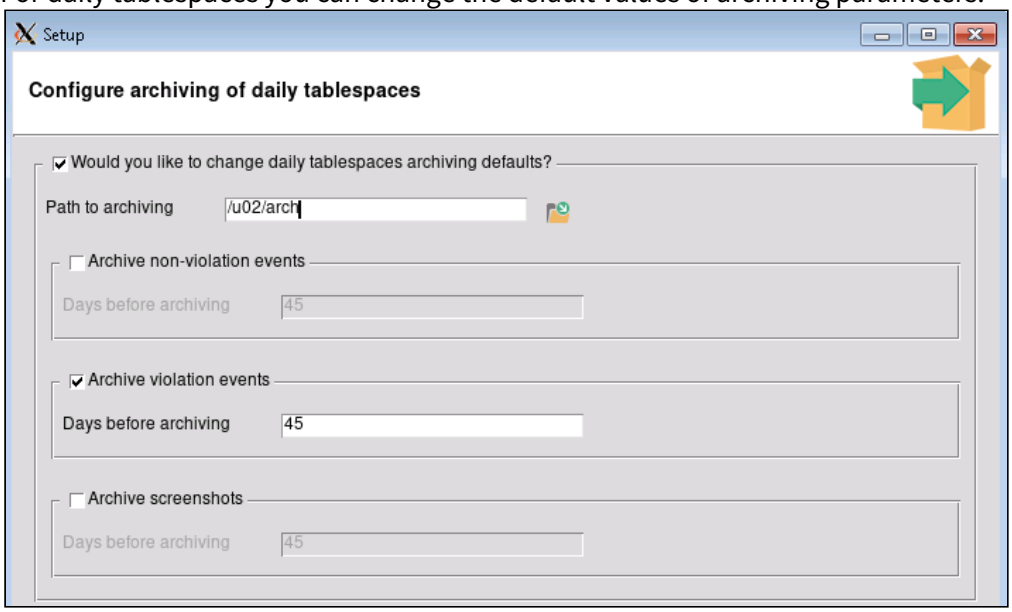
> **Note:**

If you specify the value which is more than 1, then you should specify consistently the relevent number of pathes to daily tablespaces.



- **`Daily tablespaces paths`** - path to daily tablespace data storage directory.

16. For daily tablespaces you can change the default values of archiving parameters.



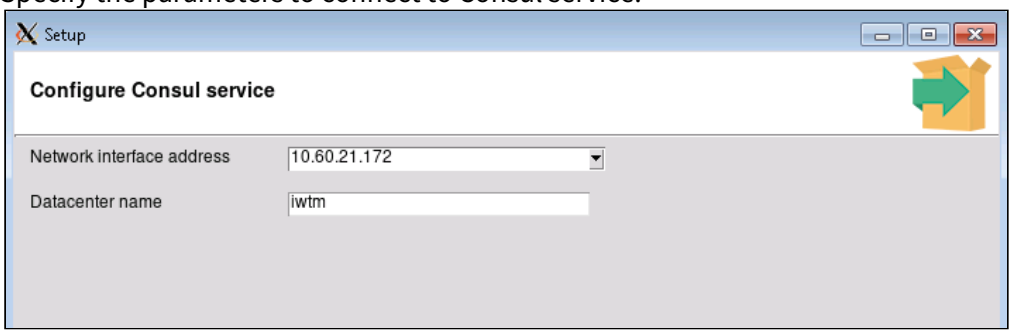
- **`Path to archiving`** - path to archived tablespaces files storage directory.

To use any parameter you should enable it:

- **`Archive non-violation events`** - enable the automatic deletion of events that are considered non-violations. If enabled, please specify the the number of days after which the event will be automatically archived, by default - 45 days.
- **`Archive violation events`** - enable the automatic archiving of events that are considered violations. If enabled, please specify the number of days after which the event will be automatically archived, by default - 45 days.
- **`Archive screenshots`** - enable the automatic archiving of screenshots received from Device Monitor Agents. If enabled, please specify the number of days after which the event will be automatically archived, by default - 45 days.

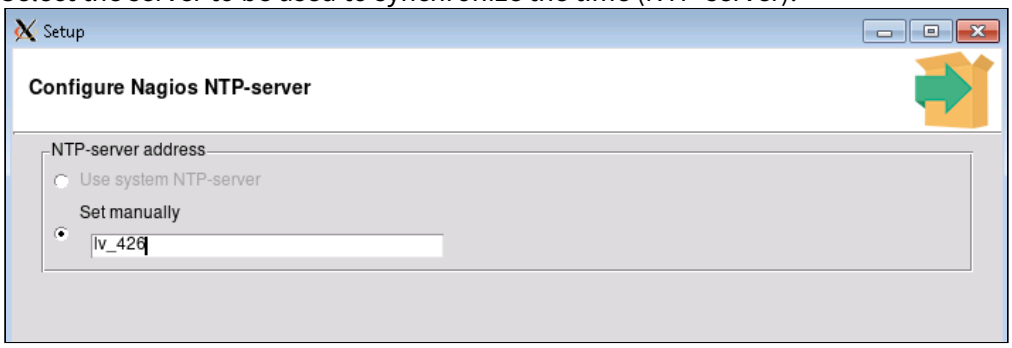
17. Similar to previous point you can configure the deletion parameters for daily tablespaces. If enabled, the default value for all the parameters - 90 days.

18. Specify the parameters to connect to Consul service:



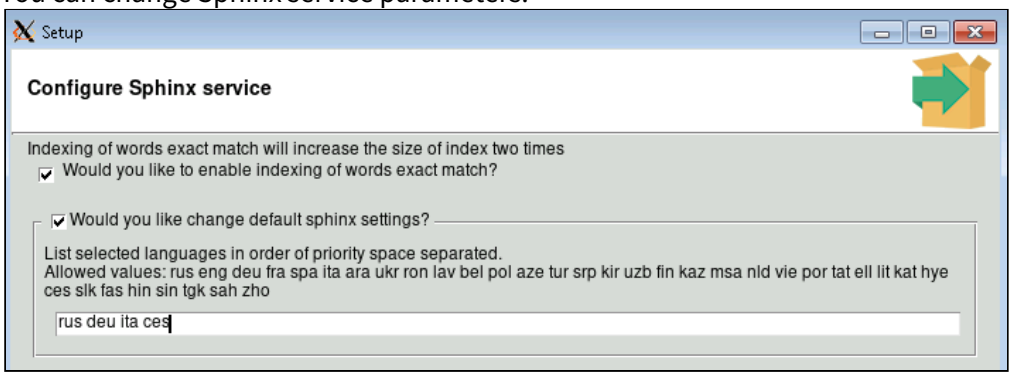
    a. **`Network interface address`** - select IP address of network interface. To select from the list of parameters click ▼ and select the required value.
    b. **`Datacenter name`** - input name of Consul data center.

19. Select the server to be used to synchronize the time (NTP-server):



- **`Use system NTP-server`**;
- **`Set manually`** - you can manually specify NTP server name. If selected, you should input IP address or NTP server available.

20. You can change Sphinx service parameters:



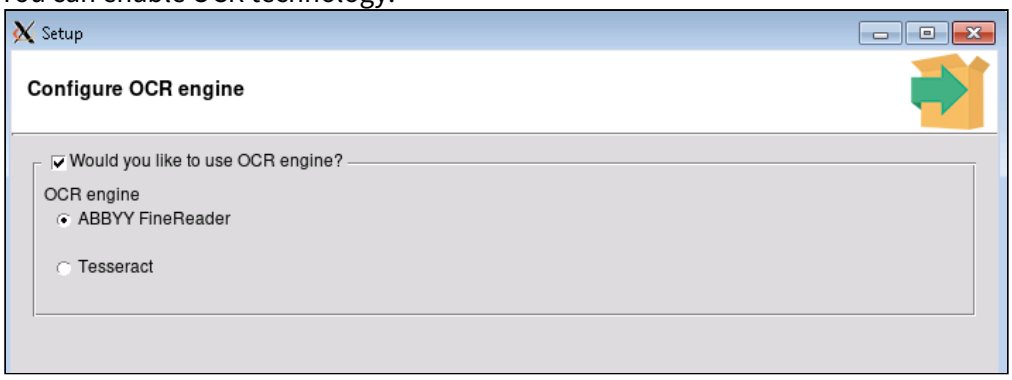
- **`Enable indexing of words exact match`**;

> **Warning!**
>
> Enabling the indexing of words exact match will increase the size of index two times minimum.

- If required, you can change the standard configuration of Sphinx service operation (**`default sphinx settings`**). In this case specify a list of languages including morphological support. Indexing will be performed according to selected languages. You can specify few languages using a space to separate them.

> **Note:**
>
> The language priority is in accordance with sequence of selected languages. English is to be added by default and it has the highest priority.

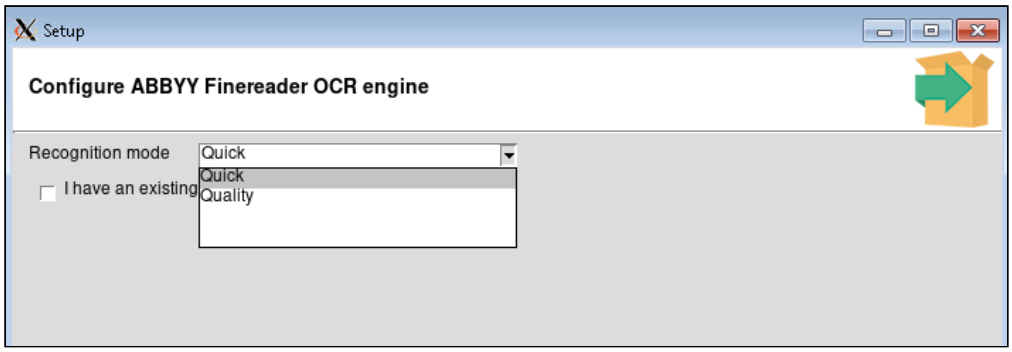
21. You can enable OCR technology.



In this case you should select one system to be used:

- `ABBYY FineReader`;
- `Tesseract`.

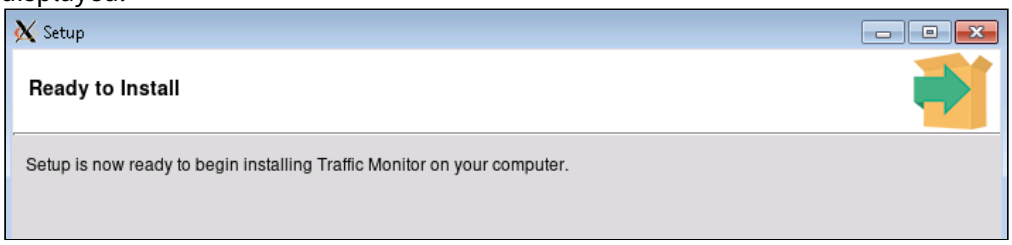
22. If ABBYY Finereader is selected as OCR extractor:



a. Select a recognition mode:
   - `Quick` – a fast mode;
   - `Quality` – a detailed mode providing higher quality of recognition.

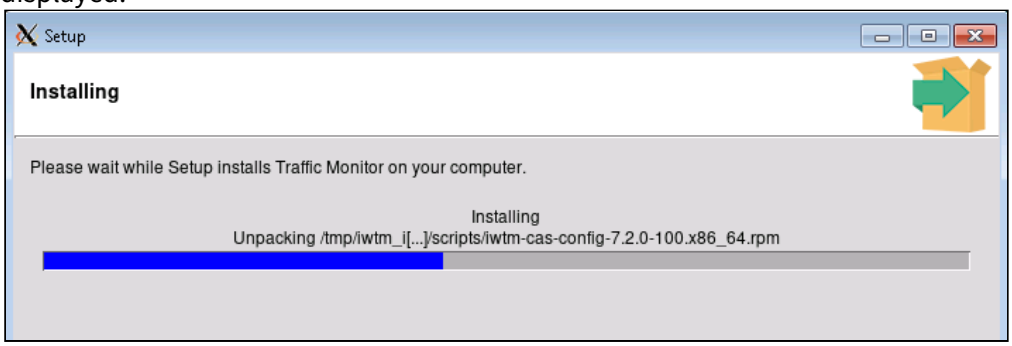
b. Confirm that you have an active license to use ABBYY Finereader.
   In case you have no active license, leave the box empty. In this case ABBYY Finereader will be installed with no license. To use ABBYY Finereader you can manually add an active license later. For more details, please see "*InfoWatch Traffic Monitor. Administation Guide*","Configuring OCR Extractors " article.

23. After all the parameters were set a message to start the installation and query to continue will be displayed.



To start the installation and press **Next**.
The unpacking of Traffic Monitor installation files will start. Implementation progress will be

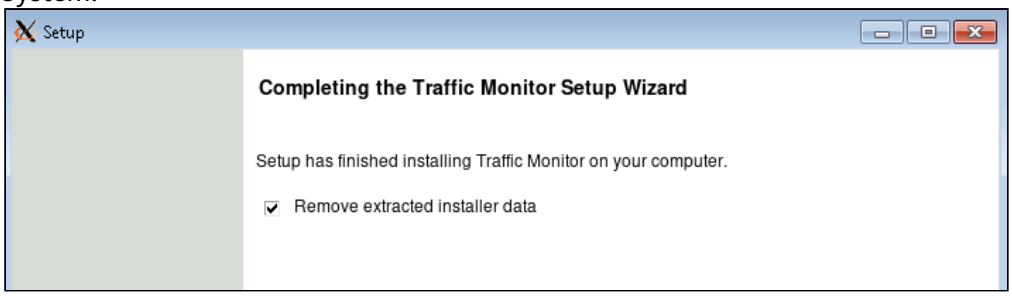
displayed.



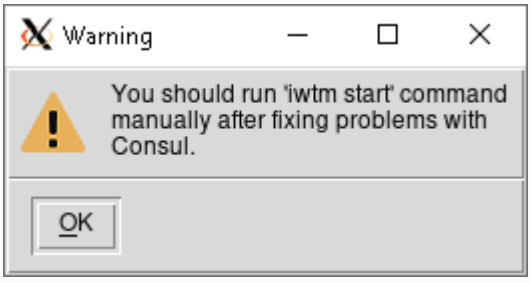
The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

24. When installation is successfully completed you can delete the packages created to install the System.



This data is recommended to delete. To do this mark the field **`Remove exctracted installer data`**.

> **Note:**
>
> If Consul service is configured incorrectly, the following warning message will be displayed:
>
> 
>
>
> To finish installation press **OK**.
>
> **For correct work of System check and configure Consul service cluster**
>
> a. Start Consul service with the command:
> `service iwtm-consul start`

To check the service status enter the command:
`service iwtm-consul status`

b. To check Consul enter the command:
   i. To display IP address of main server (leader) of cluster:
   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   ii. To display information about cluster members:
   `consul members`

c. If the IP address of cluster leader is not displayed, configure cluster of Consul service.
   After configuration is complete, repeat checking (step ii).

If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

25. To finalise the installation press **Finish**.
26. To apply the environment change you should certainly log off the System and log in again or restart the server.
27. If you require the list of Traffic Monitor services to be displayed enter the command as follows:
`iwtm status`

As a result of installation, the System creates accounts listed in "Pre-installed Server Settings".

After the completion of 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*».

3.1.2 Distributed Installation of TM Enterprise

The Enterprise edition of the Traffic Monitor allows you to deploy the System, so that DBMS modules or web console were installed on different servers. Such installation is used if Traffic Monitor services and DBMS cannot efficiently operate on the same server with respect to the supposed load.

Important!

By default you are not allowed to install the System on server which has numbers at the beginning of its name. If you need to allow the server's name to begin with a number, use the command line to specify the value `1` of the parameter `--allow_digits_at_hostname_begin`.

Herewith, make sure that the network check is active – the parameter `--skip_check_network` should have the value `0` (the check is active by default).

To install the Traffic Monitor components easily on few servers there is a Traffic Monitor installer, containing installation templates which are used to distribute the load effectively and plan the deployment. For more details about templates please see "System deployment schemes and installation types".

There are four templates available to install:

- **Database**;
- **Indexer service**;
- **Web console**;
- **Traffic interceptors**.

The templates can be installed in random order.

> **Note:**
>
> We recommend installing the templates as per one cluster in the following order:
>
> 1. Database.
> 2. Indexer service.
> 3. Web console.
> 4. Interceptors.

One server can have few templates installed at the same time. Installing all the templates on one server is consistent with "All-in-one installation mode".

> **Warning!**
>
> **Database**, **Indexer service** and **Web console** templates should be the only one as per one cluster. **Interceptors** template can be used few times as per one cluster according to the planned System load.

The Traffic Monitor installer can work in two modes involving user:

- text mode in server console;
- graphical mode.

The installation steps and its sequence is similar in both modes.

Regardless the selected mode of installation, please take the following common actions:

1. To log into the System, enter login and password (you should enter as a **root** user).

   > **Warning!**
   >
   > Before running the installation make sure that the server complies with the OS and network settings requirements.
   >
   > Each server should have unique and correct FQDN.
   >
   > If you plan using a remote database, you should update it first to the version supported by Traffic Monitor. In case of PostgreSQL DBMS using, you should preliminarily configure it.
   >
   > Before installing to clear memory, it is recommended to reboot the server on which database will be deployed.

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`** (where x.x.x.xxx is a number of build);
   - **`iwtm-postgresql-13.2-x.xx.x.tar.gz`** - if you use PostgreSQL DBMS;
   - **`iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz`** - if you use Oracle DBMS.

   As per our example:
   - **`iwtm-installer-7.2.0.123-rhel7`**;

- **`iwtm-postgresql-13.2-7.2.0.tar.gz`** - if you use PostgreSQL DBMS;
- **`iwtm-oracle-19.0.0.0.0-7.2.0.tar.gz`** - if you use Oracle DBMS.

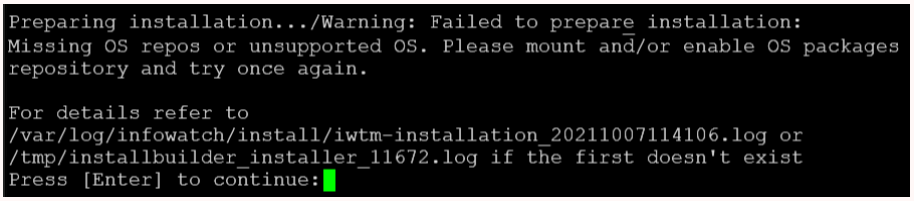
> **Note:**
>
> If you are using **Oracle DBMS** and Network File System (NFS), before running the installer:
>
> **In case you are using Oracle Real Application Clusters (RAC)**
>
> Set mount options according to the article from official website.
>
> **In case you are not using RAC:**
>
> Check in 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. Before running the installation make the installer file executable. To do this use the following command:
   `chmod u+x ./iwtm-installer-x.x.x.xxx-rhel7`
   As per our example:
   `chmod u+x ./iwtm-installer-7.2.0.123-rhel7`

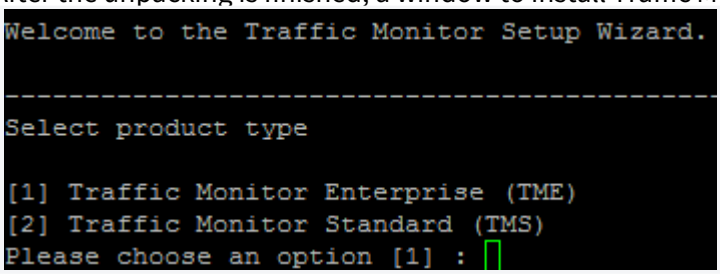
Installing in text mode using server console

To install Traffic Monitor Enterprise in the text mode using server console, take the following steps:

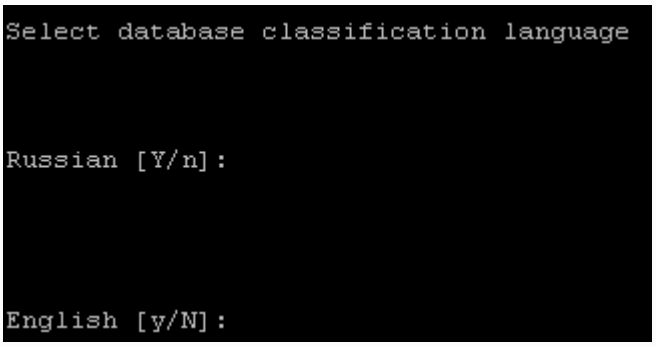
1. Start the Traffic Monitor installer running the command:
   `./iwtm-installer-x.x.x.xxx-rhel7`
   Our example command:
   `./iwtm-installer-7.2.0.123-rhel7`
   Preparations will be made to start the installation. At this stage the unpacking of Traffic Monitor installation files is not performed.

> **Warning!**
>
> If available configured OS repositories are missing, the preparation process will stop with the following error message:
>
> 
>
>
> To fix this error press **Enter** to exit, connect the standard RHEL repository, EPEL repository and restart the installer.
>
> For more details on the error refer to the log files, specified in the error message.

After the unpacking is finished, a window to install Traffic Monitor will be displayed:



2. Select **Traffic Monitor Enterprise (TME)** to install Enterprise edition. For this, enter the figure specified next to option selected, and press **Enter**.

> **Note:**
>
> When installing via server console you can see the default value, which is specified in square brackets next to input field. This value will be used in case of leaving the field empty and pressing **Enter**.
>
> **Example**
>
> If you do not input a value as per picture above and press **Enter**, the item `[1] Traffic Monitor Enterprise (TME)` will be selected.
> Also, the default value, which is in square brackets can be specified with a capital letter.
>
> **Example:**
>
> 
>

3. In the window of installation type select `Distributed`.
4. Then selecting templates you can consistently specify which sets of components are to be used on current server after the installation.

> **Warning!**
>
> Sets of required components, template combinations and number of servers are specified in accordance with expected system loads and environment. In case remote database is used, install Database template together with at least one another template.

> **Note:**
>
> If Consul service is configured incorrectly, the following warning message will be displayed:

```
\Warning: You should run 'iwtm start' command manually after fixing problems with
Consul.
Press [Enter] to continue:
```

To finish installation press **Enter**.

Check and configure Consul service cluster for correct work of System

a. Start Consul service with the command:
`service iwtm-consul start`
To check the service status enter the command:
`service iwtm-consul status`
b. To check Consul enter the command:
   i. To display IP address of main server (leader) of cluster:
   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   ii. To display information about cluster members:
   `consul members`
c. If the IP address of cluster leader is not displayed, configure cluster of Consul service.
After configuration is complete, repeat checking (step ii).

If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

Below you can find the instructions how to install each template on a separate server.

Installing Database template

If you've selected Database installation template:

1. Select the main language of user interface management console, as well as the date and time displaying format and preset configuration language:
   - **`Russian`**;
   - **`English`**.
2. Select classification base language. A classification base includes preset policies, elements of technology configuration and protected objects. Yor can select few languages at once. Options will be consistently displayed.
   The following languages are available to select:
   - **`Russia`**;
   - **`English`**;
   - **`Malay`**.

   If you do not require to install a classification base, do not select any language.
3. Select database storage type:
   - **`Install database server locally`** - to install locally on current server;
   - **`Use remote database server`** - to use on remotely deployed database. In this case the Traffic Monitor scheme will be added to remote database.
4. Select database the System to operate with:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

   Note:

When installing on CentOS, the only supported database is PostgreSQL.

5. If you use a remote database, please enter consistently:
   a. IP address and database server domain name.
   b. Connection port.
   c. The name of database to be used, where the scheme is to be added.
6. If required you can change the default values of DB authentication parameters.
   In case of positive answer the following parameters will be offered to change:
   - Password of user account having sysdba permissions;
   - Name of database schema owner;
   - Password of database schema owner's account;
   - Name of Linux services user account;
   - Password of Linux services account;
   - Name of web services user account;
   - Password of web services account;
   - Name of nagios user account;
   - Password of nagios account.
7. Select data storage mode:
   - `Norma` l - (regular) - switching to the following partition (when it is specified) happens after the previous one is overflow.
   - `Fast/Slow disks` - dividing pools into fast and slow ones. Recent data are to be kept in fast pool and to be relocated to the slow ones in a number of days specified. Slow pool operates in normal mode.
   - `Rotate` - switching to the following partition happens every day once the previous one is overflow.
8. You can change the default values of database storage parameters:
   In case of positive answer you can change the following parameters:
   - `Main tablespaces path` - path to main tablespaces data storage directory;
   - If you've selected `Fast/Slow disks` mode:
     - `Fast disk path` - path to daily tablespace data storage directory in `F ast/Slow disks` mode;
     - `Number of days to store daily tablespaces on fast disk` - number of days to store in fast tablespaces in `F ast/Slow disks` mode;
   - `Number of daily tablespaces paths` - number of daily tablespaces paths, a number from 1 to 10;

     Note:

     If you specify the value which is more than 1, then you should specify consistently the relevent number of pathes to daily tablespaces.

   - `Daily tablespaces paths` - path to daily tablespace data storage directory.
9. For daily tablespaces you can change the default values of archiving parameters.
   In case of positive answer:
   - `Path to archiving` - path to archived tablespaces files storage directory.

   The query to use each of the following parameters will be displayed in advance:

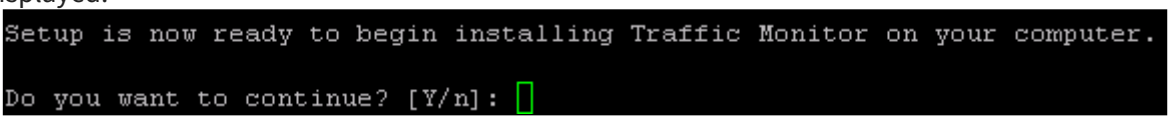
- **Archive non-violation events** - enable the automatic deletion of events that are considered non-violations. If enabled, please specify the the number of days after which the event will be automatically archived, by default - 45 days.
- **Archive violation events** - enable the automatic archiving of events that are considered violations. If enabled, please specify the number of days after which the event will be automatically archived, by default - 45 days.
- **Archive screenshots** - enable the automatic archiving of screenshots received from Device Monitor Agents. If enabled, please specify the number of days after which the event will be automatically archived, by default - 45 days.

10. Similar to previous point you can configure the deletion parameters for daily tablespaces. If enabled, the default value for all the parameters - 90 days.
11. Specify the parameters to connect to Consul service:
    a. **Network interface address** - select IP address of network interface.
    b. Consul operation mode. Two modes are available:
    - **Server**
    - **Client**

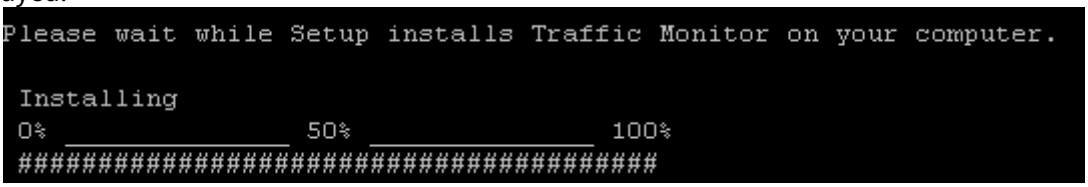
    > **Warning!**
    >
    > One cluster must have an odd number of Consul servers, but not more than 5.

    c. **Datacenter name** - input name of Consul data center.
    d. **Node name** - server name, where Traffic Monitor components are installed.
    e. **Consul retryjoin servers** - list of Consul servers, which are required to connect to. Input values via comma separated list. If you have one Consul server per one cluster on the current computer, leave thy field empty.
    f. **Consul retryjoin port –** connection port to specified Consul servers.

12. Select the server to be used to synchronize the time (NTP-server):
    - **Use system NTP-server** ;
    - **Set manually** - you can manually specify NTP server name. If selected, you should input IP address or NTP server available.
13. After all the parameters were set a message to start the installation and query to continue will be displayed.



Type **Y** to start the installation and press **Enter**.
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed.



The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

14. After the installation is complete you can delete the packages created to install the System. When installation is successfully completed the data is recommended to delete.
15. To apply the environment change you should certainly log off the System and log in again or restart the server.
16. If you require the list of Traffic Monitor services to be displayed enter the command as follows: `iwtm status`

Installing Indexer template

If you've selected Indexer service installation template:

1. Select a database the System to operate with:

- **`Oracle Database Enterprise Edition`**
- **`PostgreSQL`**

> **Note:**
>
> DBMS type should comply with selected Database template.

- Specify consistently the database connection parameters:
  a. IP address and database server domain name
  b. Connection port
  c. The name of database to be used, where the scheme is to be added.
- If required you can change the default values of DB authentication parameters.
  In case of positive answer the following parameters will be offered to change:
  - Password of user account having sysdba permissions;
  - Name of Linux services user account;
  - Password of Linux services account;
  - Name of web services user account;
  - Password of web services account;
  - Name of nagios user account;
  - Password of nagios account.
- Specify the parameters to connect to Consul service:
  a. **`Network interface address`** - select IP address of network interface.
  b. Consul operation mode. Two modes are available:
  - **`Server`**
  - **`Client`**

> **Warning!**
>
> One cluster must have an odd number of Consul servers, but not more than 5.

  c. **`Datacenter name`** - input name of Consul data center.
  d. **`Node name`** - server name, where Traffic Monitor components are installed.

e. `Consul retryjoin servers` - list of Consul servers, which are required to connect to. Input values via comma separated list. If you have one Consul server per one cluster on the current computer, leave thy field empty.
f. `Consul retryjoin port –` connection port to specified Consul servers.

- Select the server to be used to synchronize the time (NTP-server):
  - `Use system NTP-server`;
  - `Set manually` - you can manually specify NTP server name. If selected, you should input IP address or NTP server available.
- Then you can enable indexing of words exact match for Sphinx service.

> **Warning!**
>
> Enabling the indexing of words exact match will increase the size of index two times minimum.

- If required, you can change the standard configuration of Sphinx service operation. In this case specify a list of languages including morphological support. Indexing will be performed according to selected languages. You can specify few languages using a space to separate them.

> **Note:**
>
> The language priority is in accordance with sequence of selected languages. English is to be added by default and it has the highest priority.

- After all the parameters were set a message to start the installation and query to continue will be displayed.

```
Setup is now ready to begin installing Traffic Monitor on your computer.

Do you want to continue? [Y/n]:
```

Type **Y** to start the installation and press **Enter**.
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed.

```
Please wait while Setup installs Traffic Monitor on your computer.

Installing
0% _____________ 50% _____________ 100%
########################################
```

The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

- After the installation is complete you can delete the packages created to install the System.
- When installation is successfully completed the data is recommended to delete.
- To apply the environment change you should certainly log off the System and log in again or restart the server.
- If you require the list of Traffic Monitor services to be displayed enter the command as follows:
  `iwtm status`

Installing Web console template

If you've selected Web console installation template:

1. Select a database the System to operate with:
   - `Oracle Database Enterprise Edition`
   - `PostgreSQL`

   > **Note:**
   >
   > DBMS type should comply with the one selected for Database template.

2. Specify consistently the database connection parameters:
   - IP address and database server domain name.
   - Connection port
   - The name of database to be used, where the scheme is to be added.
3. If required you can change the default values of DB authentication parameters.
   In case of positive answer the following parameters will be offered to change:
   - Password of user account having sysdba permissions;
   - Name of database schema owner;
   - Name of Linux services user account;
   - Password of Linux services account;
   - Name of web services user account;
   - Password of web services account;
   - Name of nagios user account;
   - Password of nagios account.
4. Specify the parameters to connect to Consul service:
   a. `Network interface address` - select IP address of network interface.
   b. Consul operation mode. Two modes are available:
   - `Server`
   - `Client`

   > **Warning!**
   >
   > One cluster must have an odd number of Consul servers, but not more than 5.

   c. `Da tacenter name` - input name of Consul data center.
   d. `Node name` - server name, where Traffic Monitor components are installed.
   e. `Consul retryjoin servers` - list of Consul servers, which are required to connect to. Input values via comma separated list. If you have one Consul server per one cluster on the current computer, leave thy field empty.
   f. `Consul retryjoin port –` connection port to specified Consul servers.
5. Select the server to be used to synchronize the time (NTP-server):
   - `Use system NTP-server`;
   - `Set manually` - you can manually specify NTP server name. If selected, you should input IP address or NTP server available.
6. Then you can enable indexing of words exact match for Sphinx service.

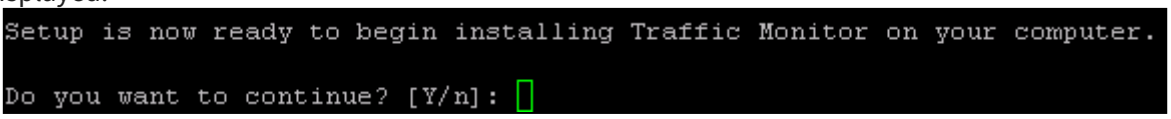
   > **Note:**

If you install Indexer and Web console templates on one server this parameter will not be requested by installer.

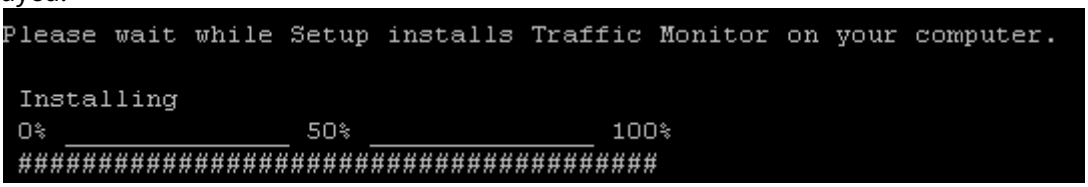
7. You can enable OCR technology.

> **Note:**
>
> OCR extractor can be selected when installing Interceptors template.

8. After all the parameters were set a message to start the installation and query to continue will be displayed.



Type **Y** to start the installation and press **Enter**.
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed.



The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

9. After the installation is complete you can delete the packages created to install the System. When installation is successfully completed the data is recommended to delete.
10. To apply the environment change you should certainly log off the System and log in again or restart the server.
11. If you require the list of Traffic Monitor services to be displayed enter the command as follows: `iwtm status`

Installing Interceptors template

If you've selected Interceptors installation template:

1. Select a database the System to operate with:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

> **Note:**
>
> DBMS type should comply with the one selected for Database template.

2. Specify consistently the database connection parameters:

- IP address and database server domain name.
- Connection port
- The name of database to be used, where the scheme is to be added.

3. If required you can change the default values of DB authentication parameters.
   In case of positive answer the following parameters will be offered to change:
   - Password of user account having sysdba permissions;
   - Name of Linux services user account;
   - Password of Linux services account;
   - Name of web services user account;
   - Password of web services account;
   - Name of nagios user account;
   - Password of nagios account.
4. Specify the parameters to connect to Consul service:
   a. `Network interface address` - select IP address of network interface.
   b. Consul operation mode. Two modes are available:
      - `Server`
      - `Client`

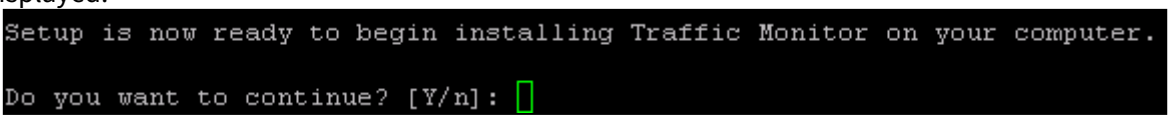
   > **Warning!**
   >
   > One cluster must have an odd number of Consul servers, but not more than 5.

   c. `Da tacenter name` - input name of Consul data center.
   d. `Node name` - server name, where Traffic Monitor components are installed.
   e. `Consul retryjoin servers` - list of Consul servers, which are required to connect to. Input values via comma separated list. If you have one Consul server per one cluster on the current computer, leave thy field empty.
   f. `Consul retryjoin port –` connection port to specified Consul servers.
5. Select the server to be used to synchronize the time (NTP-server):
   - `Use system NTP-server`;
   - `Set manually` - you can manually specify NTP server name. If selected, you should input IP address or NTP server available.
6. You can enable OCR technology. In this case you should select one system to be used:
   - `ABBYY FineReader`;
   - `Tesseract`.

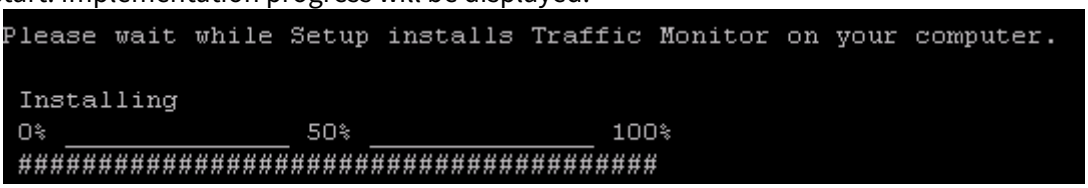
   > **Note:**
   >
   > For OCR operation you should enable the technology when installing Web console template.

7. If ABBYY Finereader is selected as OCR extractor:
   a. Select a recognition mode:
      - `Quick` – a fast mode;
      - `Quality` – a detailed mode providing higher quality of recognition.
   b. Confirm that you have an active license to use ABBYY Finereader. In case you have no active license, type **N** and press **Enter**. In this case ABBYY Finereader will be installed with no license. To use ABBYY Finereader you can manually add an active license later. For more details, please see "*InfoWatch Traffic Monitor. Administation Guide*" "Configuring OCR Extractors " article.

8. After all the parameters were set a message to start the installation and query to continue will be displayed.



Type **Y** to start the installation and press **Enter**.The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed.



The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

9. After the installation is complete you can delete the packages created to install the System. When installation is successfully completed the data is recommended to delete.
10. To apply the environment change you should certainly log off the System and log in again or restart the server.
11. If you require the list of Traffic Monitor services to be displayed enter the command as follows:
`iwtm status`

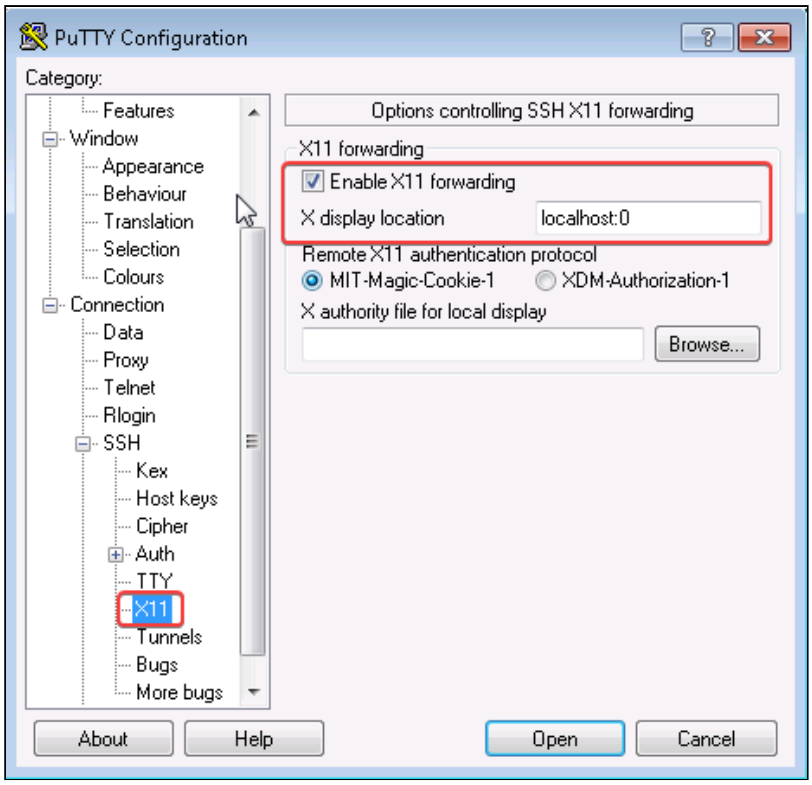
Installing in graphical mode

X Window System uses a client - server model. To run the installer in the graphical mode **X11 Forwarding** is used to forward the graphical output of remote system. This let you work directly with Linux graphical applications on the computer which is connected to server. This mode is implemented via SSH connection.

To install Traffic Monitor Enterprise or Traffic Monitor Standard in All-in-one mode using graphical mode of installation, take the folowing steps:

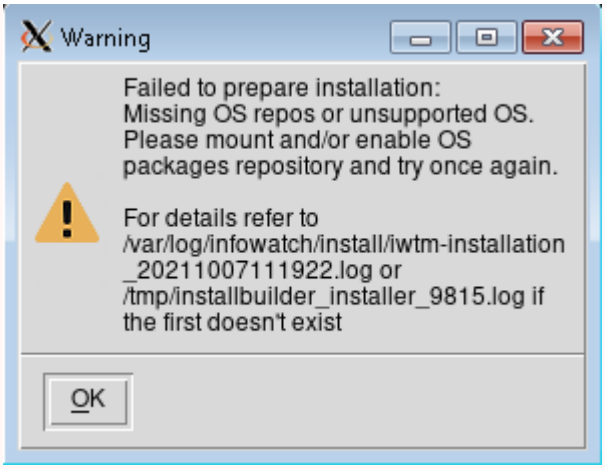
1. On the server, where Traffic Monitor components are planned to install:
a. Install xauth utility using the command:
`yum install xauth`
b. In `/etc/ssh/sshd_config` configuration file uncomment the line "`X11Forwarding yes`".
To do this, delete `#` placed before the line.
c. Save changes in configuration file.
d. Restart SSH service using the command:
`systemctl restart sshd`
2. On the computer, where the graphical mode is to be used:
a. To connect to Traffic Monitor installation server you will require a SSH client with enabled X11 Forwarding option, e.g. PuTTY.
b. To start the installer in the graphical mode you will require an application configured to access to X Window System, for example:
    - Xming application - for OS MS Windows;
    - Gnome 3 shell - for OS Linux.

3. Run the application client which was previously configured to access to X Window System.
4. Connect to server, where Traffic Monitor components are planned to install, using selected SSH client.
   Example of PuTTY configuration window used to connect



5. To install Traffic Monitor run the installer using the command:
   `./iwtm-installer-x.x.x.xxx-rhel7`
   As per our example:
   `./iwtm-installer-7.2.0.123-rhel7`
   Preparations will be made to start the installation. At this stage the unpacking of Traffic Monitor installation files is not being performed.

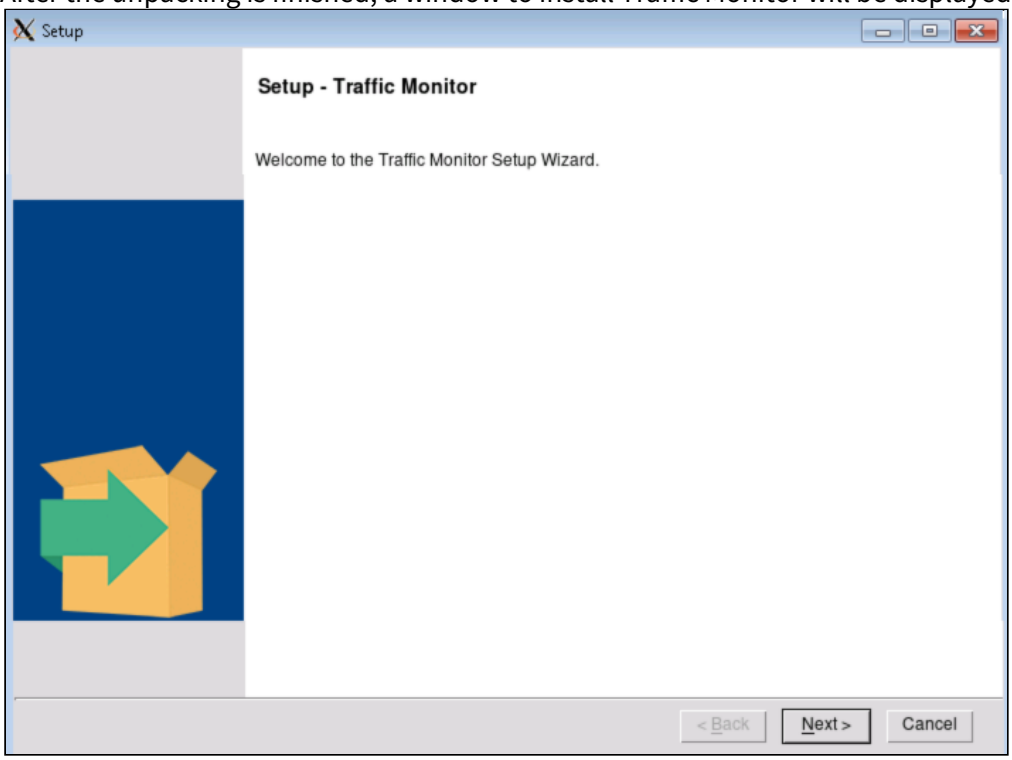
> **Warning!**
>
> If available configured OS repositories are missing, the preparation process will stop with the following alert box:



To fix this error press **OK** to dismiss, connect the standard RHEL repository, EPEL repository and restart the installer.

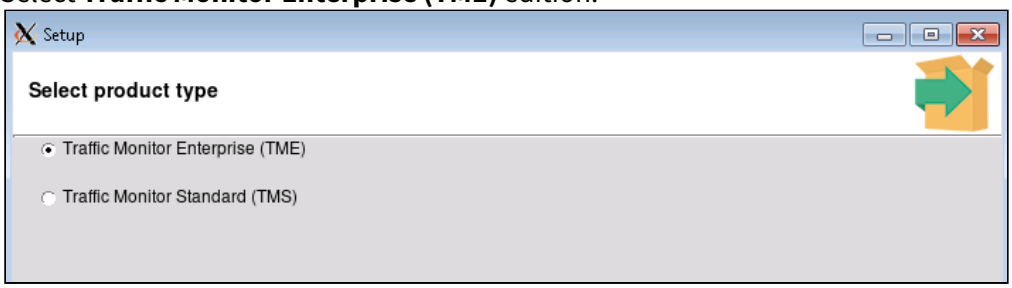
For more details on the error refer to the log files specified in the alert box.

After the unpacking is finished, a window to install Traffic Monitor will be displayed:



To go to the next parameter press **Next** button, to go back press - **Back**. To exit the installer press **Cancel** button.

6. Select **Traffic Monitor Enterprise (TME)** edition.



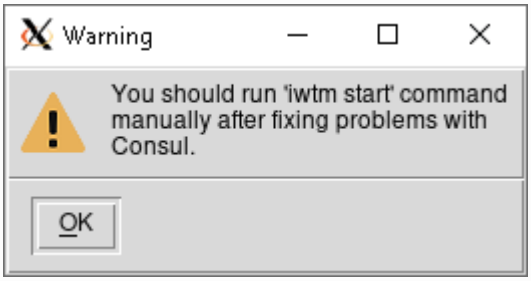
To select click in the checkbox next to required value and press **Next** button.

7. In the window of installation type select `Distributed`.
8. Then selecting templates you can consistently specify which sets of components are to be used on current server after the installation.



To select few values mark each required field and press **Next** button.

> **Warning!**
>
> Sets of required components, template combinations and number of servers are specified in accordance with expected system loads and environment.
>
> In case remote database is used, install Database template together with at least one another template.

> **Note:**
>
> If Consul service is configured incorrectly, the following warning message will be displayed:
>
> 
>
>
> To finish installation press **OK**.
>
> **For correct work of System check and configure Consul service cluster**
>
> a. Start Consul service with the command:
> `service iwtm-consul start`

To check the service status enter the command:
`service iwtm-consul status`

b. To check Consul enter the command:
   i. To display IP address of main server (leader) of cluster:
   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   ii. To display information about cluster members:
   `consul members`

c. If the IP address of cluster leader is not displayed, configure cluster of Consul service.
   After configuration is complete, repeat checking (step ii).

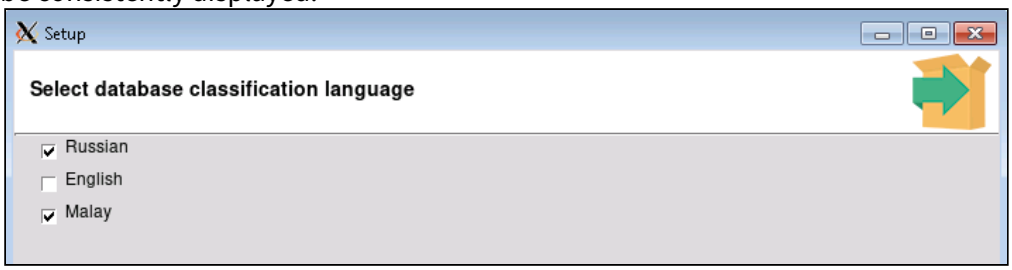
If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

Below you can find the instructions how to install each template on a separate server.

Installing Database template

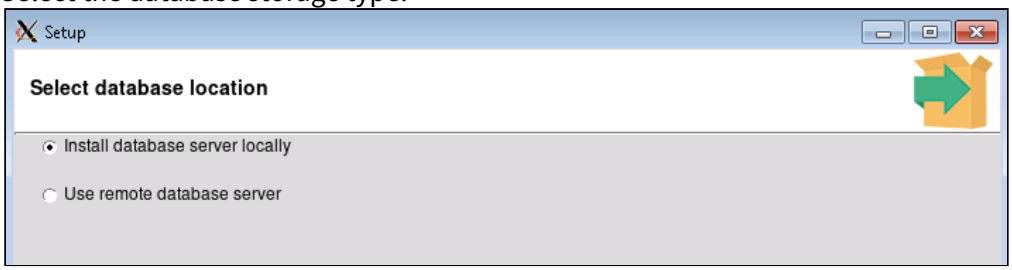
If you've selected Database installation template:

1. Select the main language of user interface management console, as well as date and time displaying format and preset configuration language:
   - **`Russian`**;
   - **`English`**.
2. Select the classification base language. A classification base includes preset policies, elements of technology configuration and protected objects. Yor can select few languages at once. Options will be consistently displayed.



The following languages are available to select:
   - **`Russia`**;
   - **`English`**;
   - **`Malay`**.

If you do not require to install a classification base, do not select any language.
3. Select the database storage type:



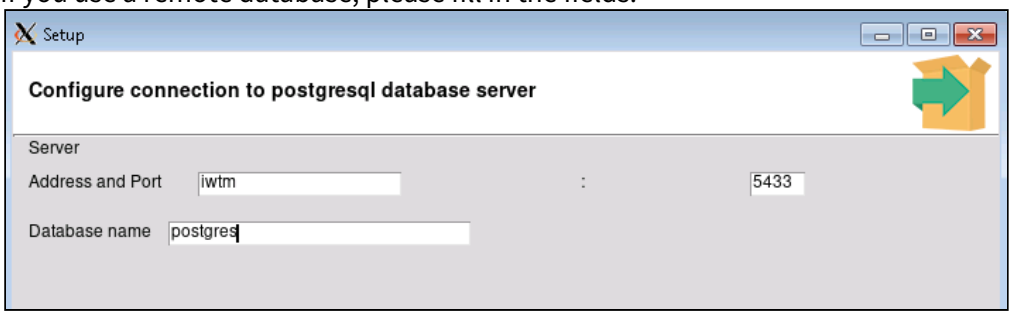
   - **`Install database server locally`** - to install locally on current server;

- **Use remote database server** - to use on remotely deployed database. In this case the Traffic Monitor scheme will be added to remote database.

4. Select a database the System to operate with:
   - **Oracle Database Enterprise Edition**
   - **PostgreSQL**

> **Note:**
>
> When installing on CentOS, the only supported database is PostgreSQL.

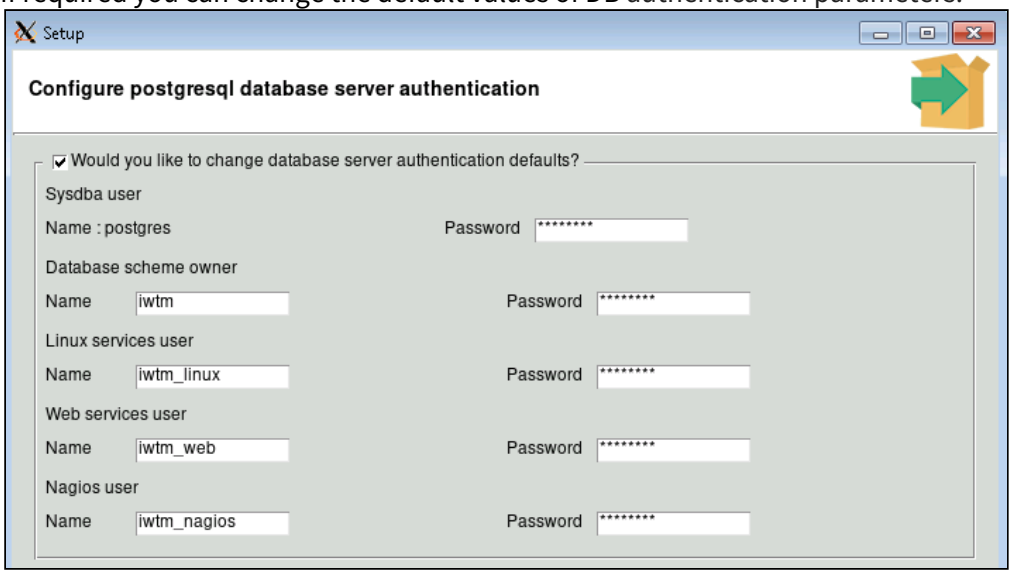
5. If you use a remote database, please fill in the fields:



   - **Address and Port –** IP address and database server domain name and connection port.
   - **Database name** - The name of database to be used, where the scheme is to be added.

> **Note:**
>
> In the graphical mode active fields contain the default values.

6. If required you can change the default values of DB authentication parameters.

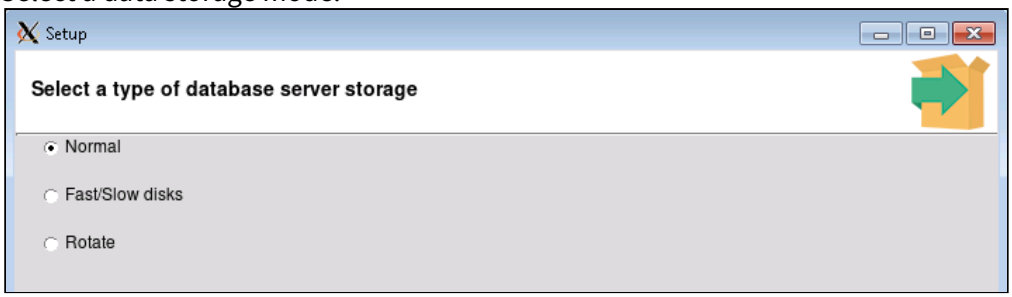


To edit the values mark the field next to question. This will let you edit the following sections:

- **Sysdba user** - Password of user account having sysdba permissions;
- **Database scheme owner** - Name and password of database schema owner;
- **Linux services user** - Name and password of Linux services user;

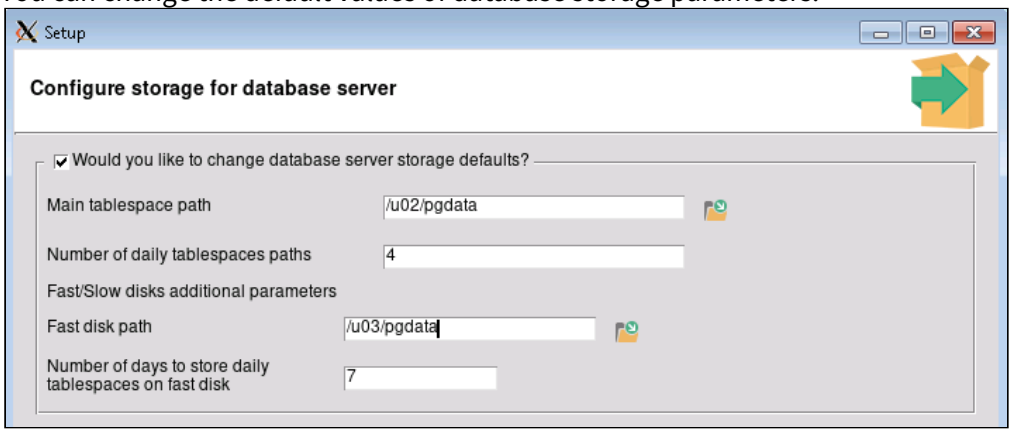
- **Web services user** - Name and password of web services user;
- **Nagios user** - Name and password of nagios user.

7. Select a data storage mode:



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

8. You can change the default values of database storage parameters.

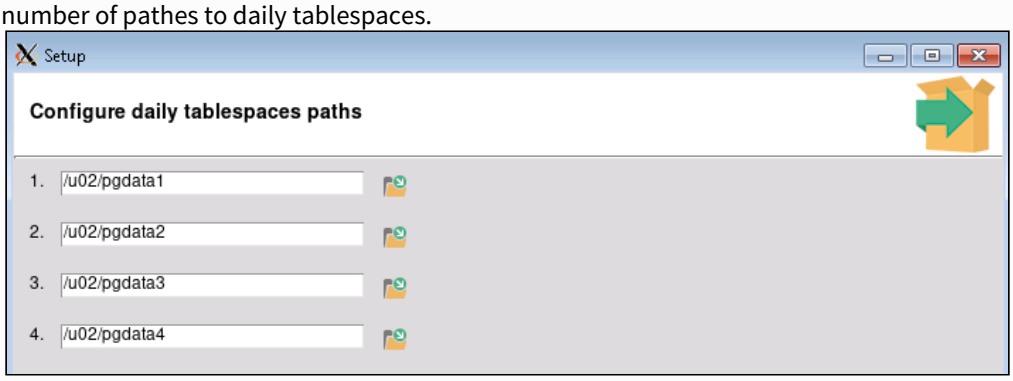


- **Main tablespaces path** - path to main tablespaces data storage directory;

  You can add the path to the field or specify it via file manager window using  button.
- If you've selected **Fast/Slow disks** mode:
  - **Fast disk path** - path to daily tablespace data storage directory in **F ast/Slow disks** mode;
  - **Number of days to store daily tablespaces on fast disk** - number of days to store in fast tablespaces in **F ast/Slow disks** mode;
- **Number of daily tablespaces paths** - number of daily tablespaces paths, a number from 1 to 10;

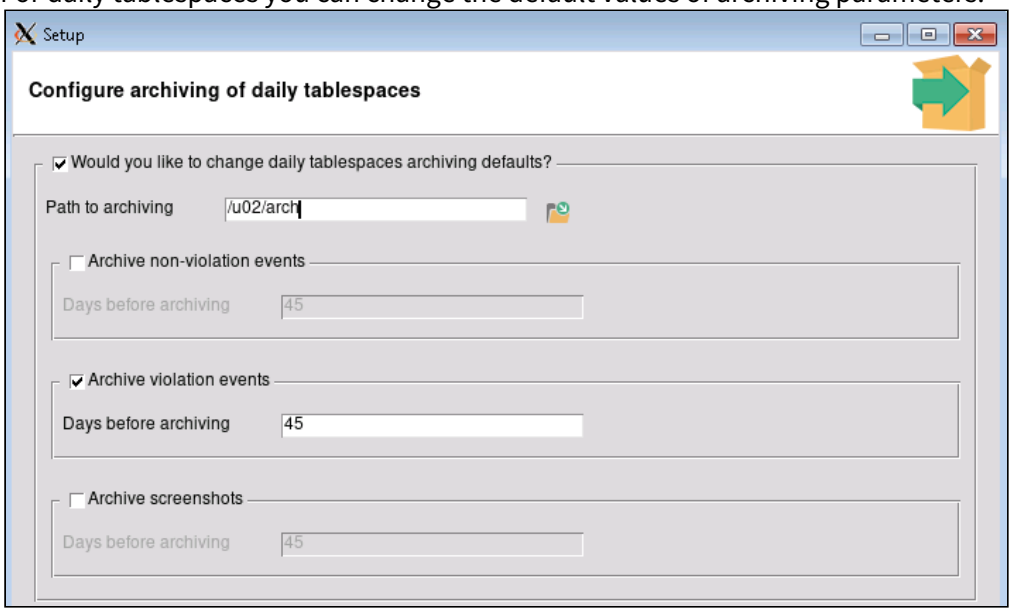
> **Note:**

If you specify the value which is more than 1, then you should specify consistently the relevent number of pathes to daily tablespaces.



- **`Daily tablespaces paths`** - path to daily tablespace data storage directory.

9. For daily tablespaces you can change the default values of archiving parameters.



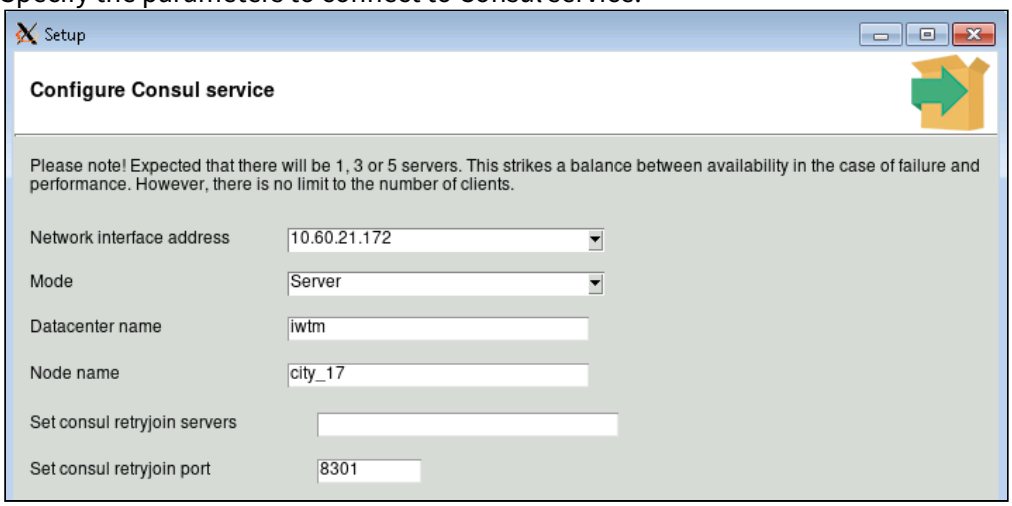
- **`Path to archiving`** - path to archived tablespaces files storage directory.

To use any parameter you should enable it:

- **`Archive non-violation events`** - enable the automatic deletion of events that are considered non-violations. If enabled, please specify the the number of days after which the event will be automatically archived, by default - 45 days.
- **`Archive violation events`** - enable the automatic archiving of events that are considered violations. If enabled, please specify the number of days after which the event will be automatically archived, by default - 45 days.
- **`Archive screenshots`** - enable the automatic archiving of screenshots received from Device Monitor Agents. If enabled, please specify the number of days after which the event will be automatically archived, by default - 45 days.

10. Similar to previous point you can configure the deletion parameters for daily tablespaces. If enabled, the default value for all the parameters - 90 days.

11. Specify the parameters to connect to Consul service:

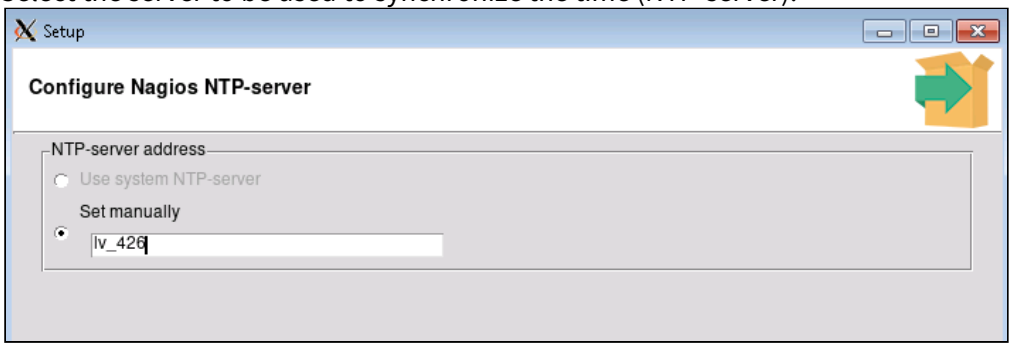


- **`Network interface address`** - select IP address of network interface. To select from the list of parameters click ▼ and select the required value.
- Consul operation mode. Two modes are available:
  - **`Server`**
  - **`Client`**

> **Warning!**
>
> One cluster must have an odd number of Consul servers, but not more than 5.

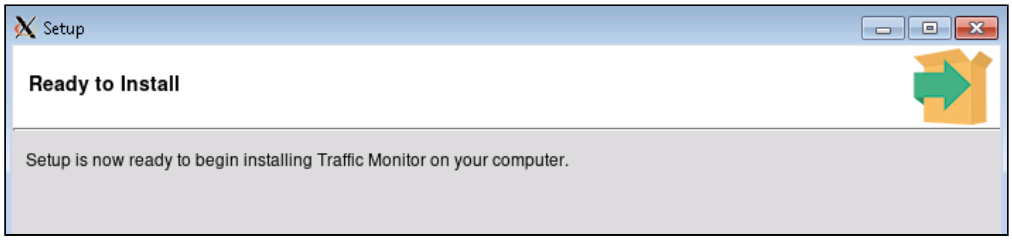
- **`Database name`** - The name of database to be used, where the scheme is to be added.
- **`Node name`** - server name, where Traffic Monitor components are installed.
- **`Consul retryjoin servers`** - list of Consul servers, which are required to connect to. Input values via comma separated list. If you have one Consul server per one cluster on the current computer, leave thy field empty.
- **`Consul retryjoin port –`** connection port to specified Consul servers.

12. Select the server to be used to synchronize the time (NTP-server):

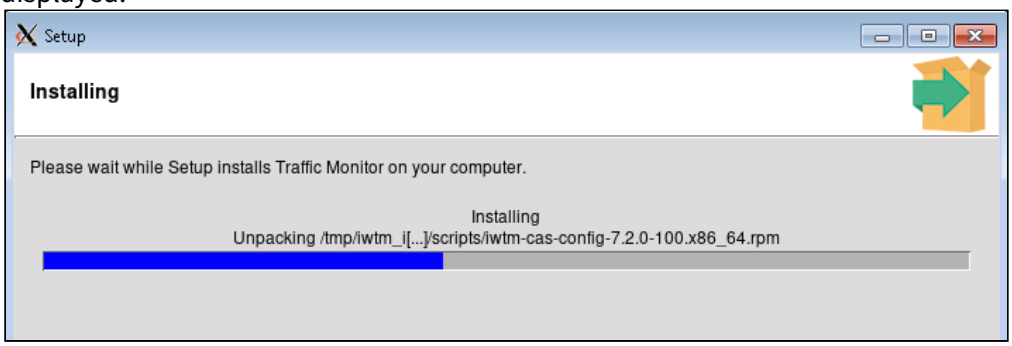


  - **`Use system NTP-server`**;
  - **`Set manuall`** y - you can manually specify NTP server name. If selected, you should input IP address or NTP server available.

13. After all the parameters were set a message to start the installation and query to continue will be displayed.



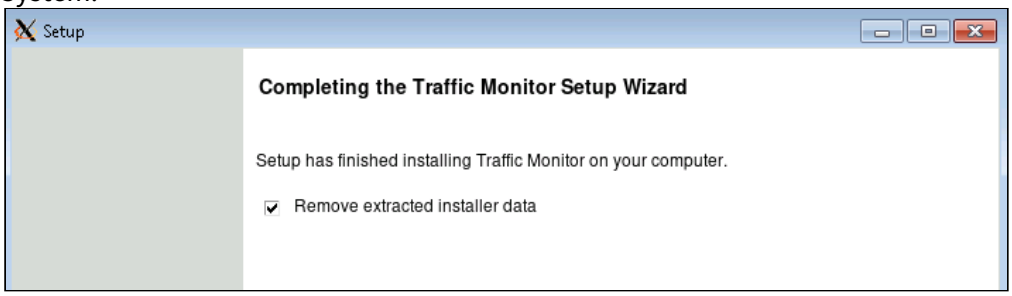
To start the installation and press **Nex**t
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed.



The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

14. When installation is successfully completed you can delete the packages created to install the System.



This data is recommended to delete. To do this mark the field **`Remove exctracted installer data`**.

15. To finalise the installation press **Finish**.
16. To apply the environment change you should certainly log off the System and log in again or restart the server.
17. If you require the list of Traffic Monitor services to be displayed enter the command as follows: `iwtm status`

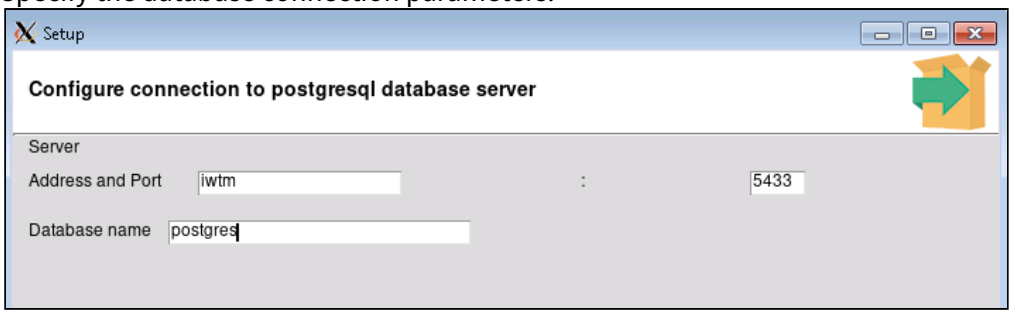
Installing Indexer template

If you've selected Indexer service installation template:

1. Select a database the System to operate with:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

> **Note:**
>
> DBMS type should comply with the one selected for Database template.

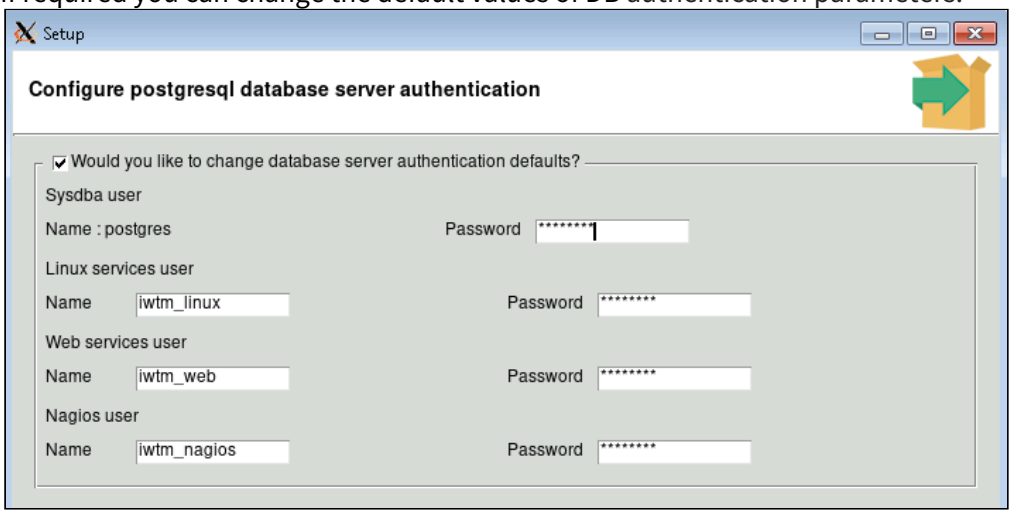
2. Specify the database connection parameters:



- **`Address and Port –`** IP address, database server domain name and connection port.
- **`Database name`** - The name of database to be used, where the scheme is to be added.

> **Note:**
>
> In the graphical mode active fields contain the default values.

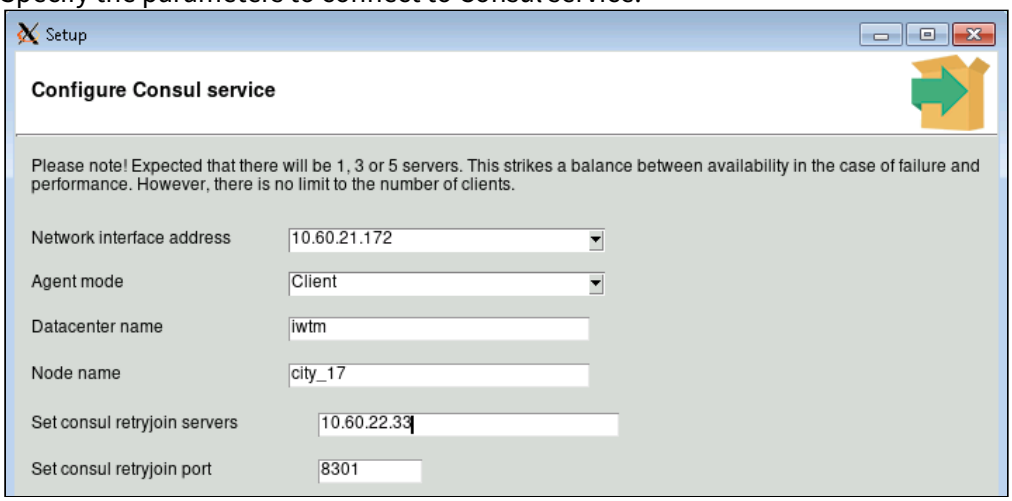
3. If required you can change the default values of DB authentication parameters.



To edit the values mark the field next to question. This will let you edit the following sections:

- **`Sysdba user`** - Password of user account having sysdba permissions;
- **`Linux services user`** - Name and password of Linux services user;
- **`Web services user`** - Name and password of web services user;
- **`Nagios user`** - Name and password of nagios user.

4. Specify the parameters to connect to Consul service:

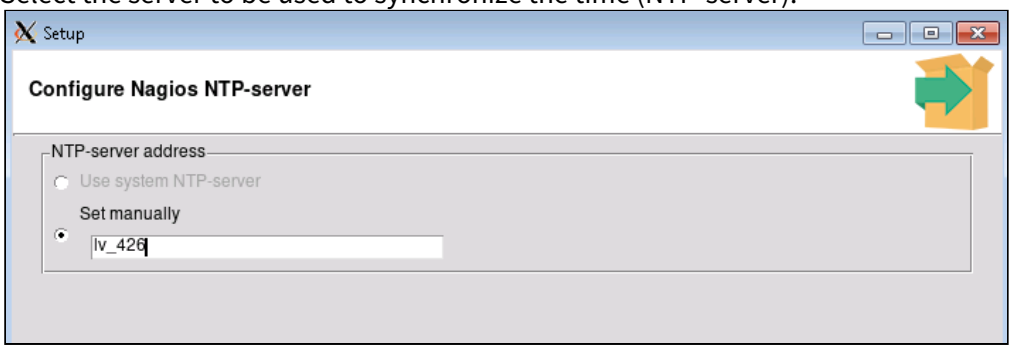


- **`Network interface address`** - select IP address of network interface. To select from the list of parameters click ▼ and select the required value.
- Consul operation mode. Two modes are available:
  - **`Server`**
  - **`Client`**

> **Warning!**
>
> One cluster must have an odd number of Consul servers, but not more than 5.

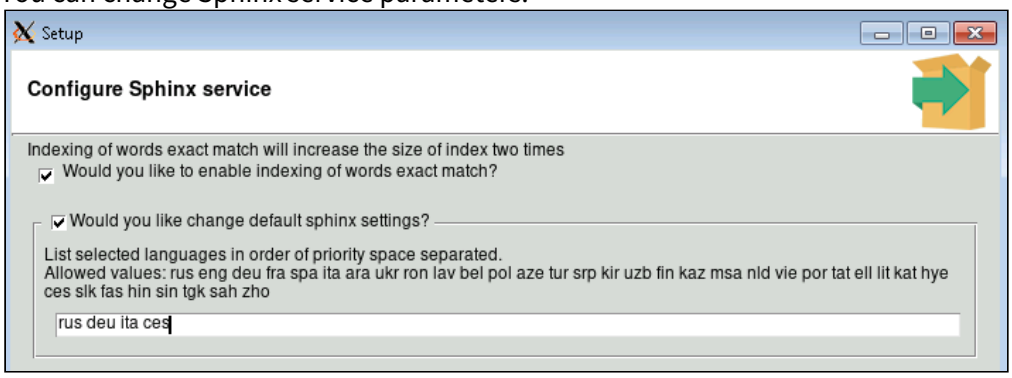
- **`Database name`** - The name of database to be used, where the scheme is to be added.
- **`Node name`** - server name, where Traffic Monitor components are installed.
- **`Consul retryjoin servers`** - list of Consul servers, which are required to connect to. Input values via comma separated list. If you have one Consul server per one cluster on the current computer, leave thy field empty.
- **`Consul retryjoin port –`** connection port to specified Consul servers

5. Select the server to be used to synchronize the time (NTP-server):



- **`Use system NTP-server`**;
- **`Set manually`** - you can manually specify NTP server name. If selected, you should input IP address or NTP server available.

6. You can change Sphinx service parameters:



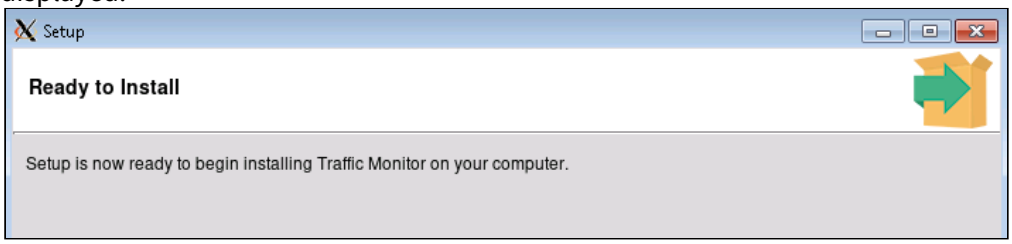
- **`Enable indexing of words exact match`**;

> **Warning!**
>
> Enabling the indexing of words exact match will increase the size of index two times minimum.

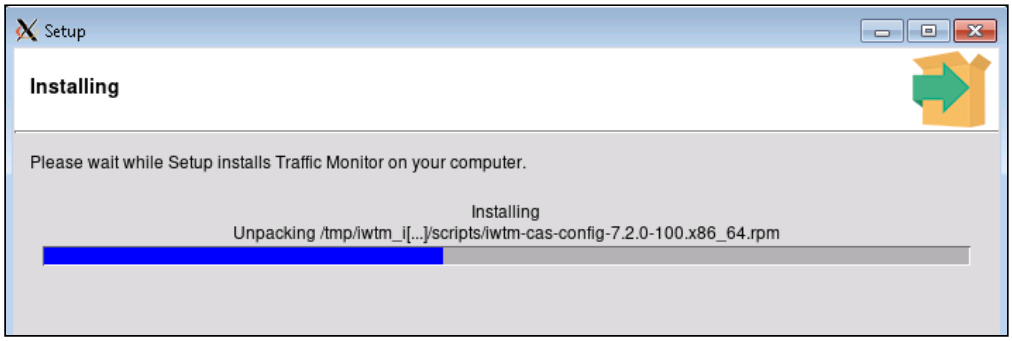
- If required, you can change the standard configuration of Sphinx service operation (**`default sphinx settings`**). In this case specify a list of languages including morphological support. Indexing will be performed according to selected languages. You can specify few languages using a space to separate them.

> **Note:**
>
> The language priority is in accordance with sequence of selected languages. English is to be added by default and it has the highest priority.

7. After all the parameters were set a message to start the installation and query to continue will be displayed.



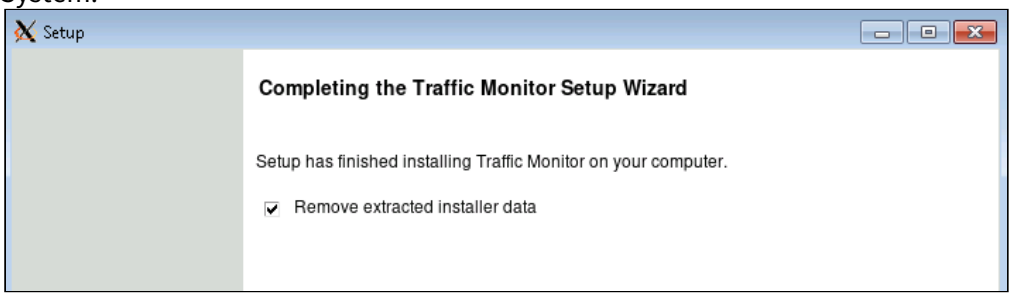
To start the installation and press **Nex**t
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed



The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

8. When installation is successfully completed you can delete the packages created to install the System.



This data is recommended to delete. To do this mark the field **`Remove exctracted installer data`**.

9. To finalise the installation press **Finish**.
10. To apply the environment change you should certainly log off the System and log in again or restart the server.
11. If you require the list of Traffic Monitor services to be displayed enter the command as follows: `iwtm status`

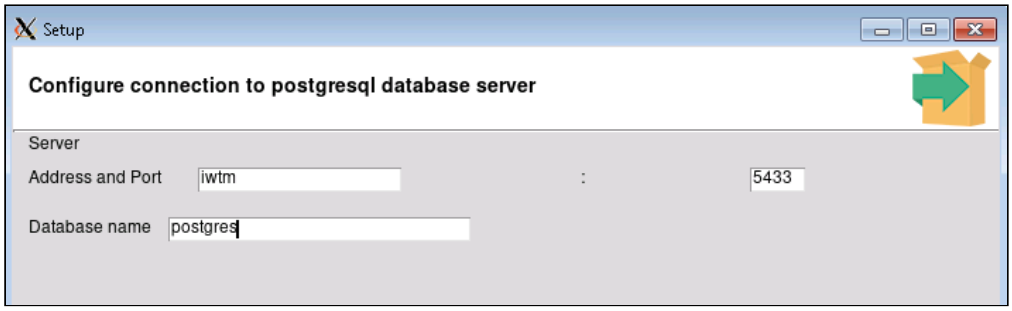
Installing Web console template

If you've selected Interceptors installation template:

1. Select a database the System to operate with:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

   > **Note:**
   >
   > DBMS type should comply with the one selected for Database template.

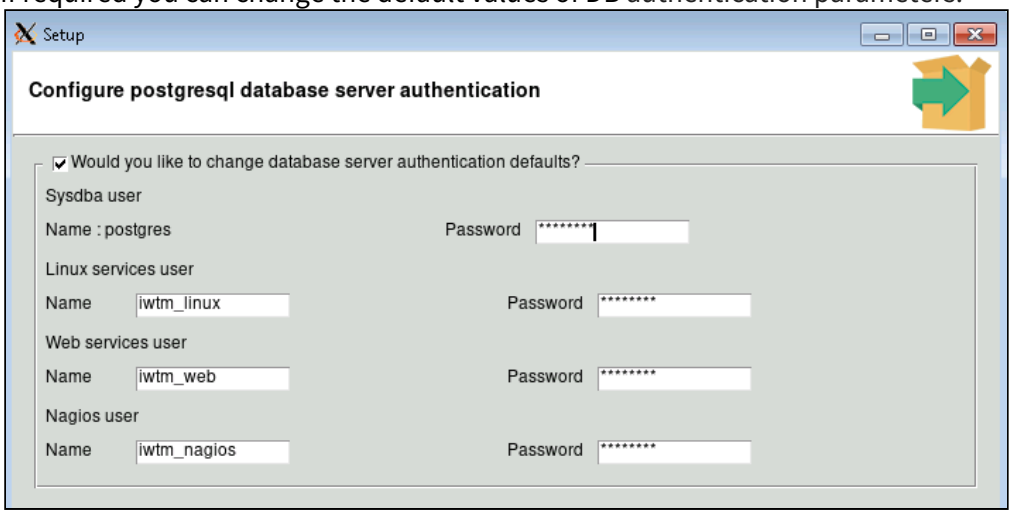
2. Specify the database connection parameters:



- **`Address and Port –`** IP address, database server domain name and connection port.
- **`Database name`** - The name of database to be used, where the scheme is to be added.

> **Note:**
>
> In graphical mode active fields contain the default values.

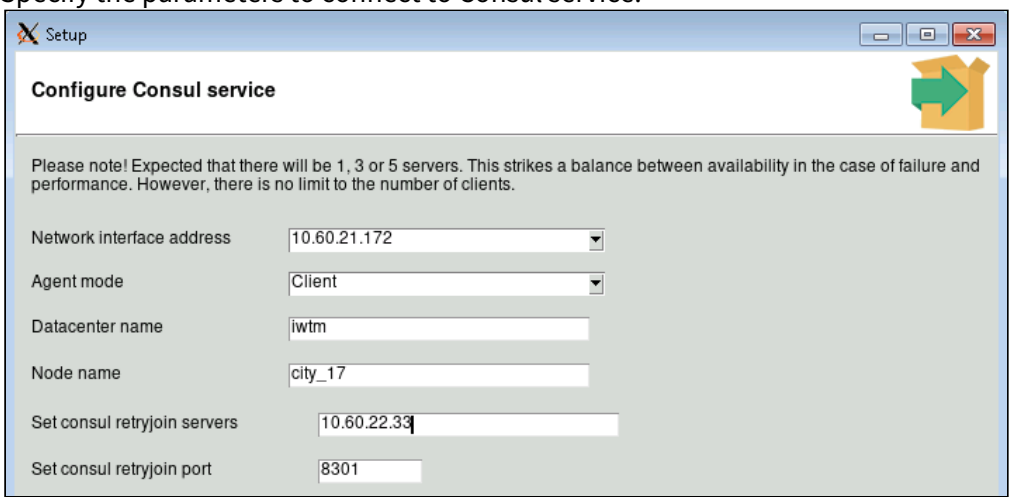
3. If required you can change the default values of DB authentication parameters.



To edit the values mark the field next to question. This will let you edit the following sections:

- **`Sysdba user`** - Password of user account having sysdba permissions;
- **`Database scheme owner`** - Name of database owner;
- **`Linux services user`** - Name and password of Linux services user;
- **`Web services user`** - Name and password of web services user;
- **`Nagios user`** - Name and password of nagios user.

4. Specify the parameters to connect to Consul service:

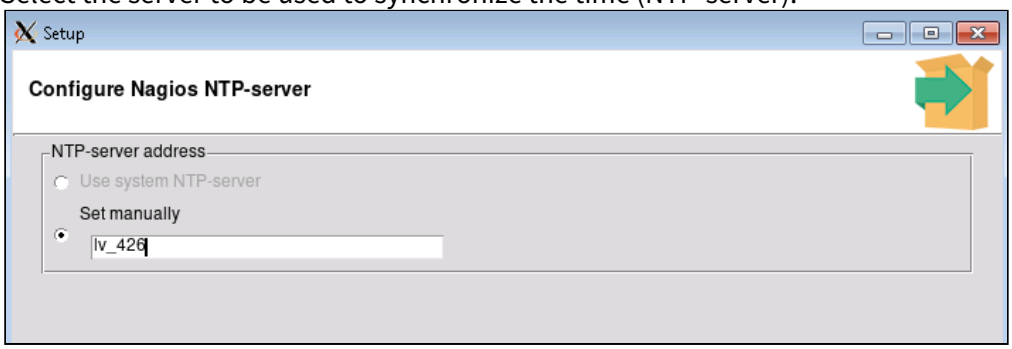


- **`Network interface address`** - select IP address of network interface. To select from the list of parameters click ▼ and select the required value.
- Consul operation mode. Two modes are available:
  - **`Server`**
  - **`Client`**

> **Warning!**
>
> One cluster must have an odd number of Consul servers, but not more than 5.

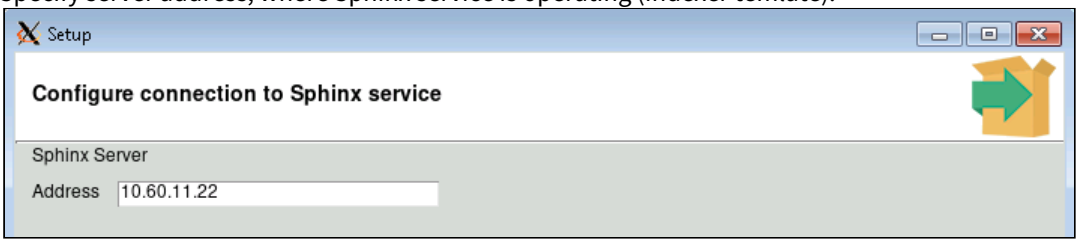
- **`Database name`** - The name of database to be used, where the scheme is to be added.
- **`Node name`** - server name, where Traffic Monitor components are installed.
- **`Consul retryjoin servers`** - list of Consul servers, which are required to connect to. Input values via comma separated list. If you have one Consul server per one cluster on the current computer, leave thy field empty.
- **`Consul retryjoin port –`** connection port to specified Consul servers

5. Select the server to be used to synchronize the time (NTP-server):



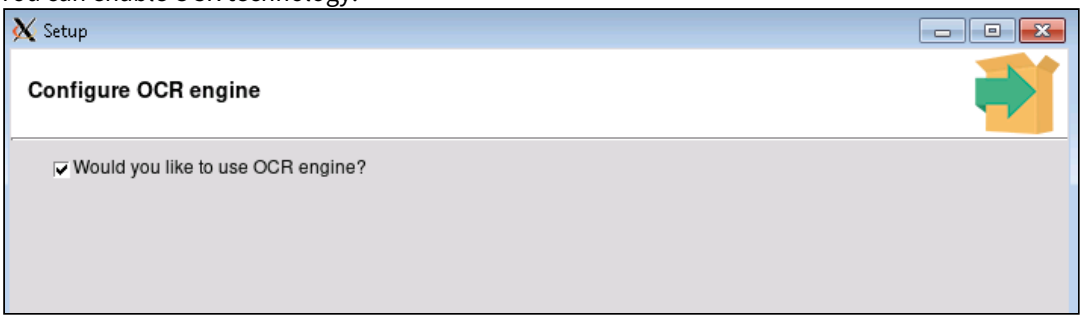
- **`Use system NTP-server`** ;
- **`Set manually`** - you can manually specify NTP server name. If selected, you should input IP address or NTP server available.

- Specify server address, where Sphinx service is operating (Indexer temlate).



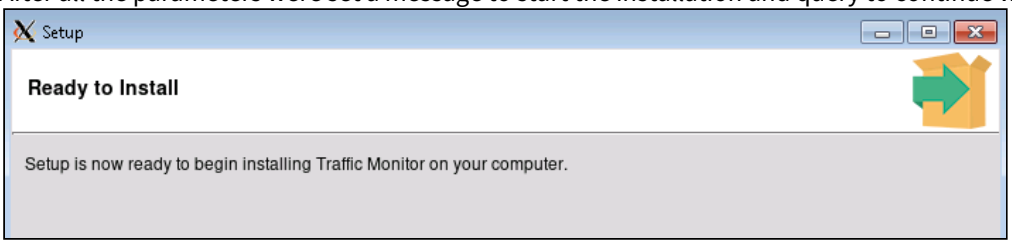
> **Note:**
>
> In case Indexer and Web console templates are installed on one server, this parameter will not be requested by installer.

- You can enable OCR technology.

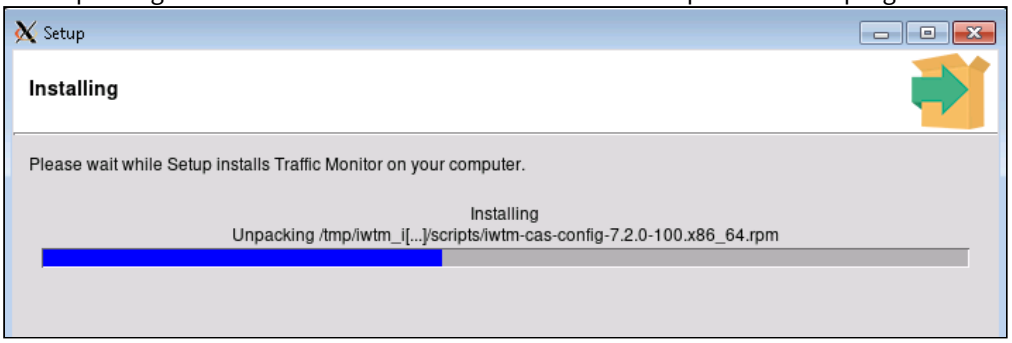


> **Note:**
>
> OCR is to be selected when installing Interceptors template.

- After all the parameters were set a message to start the installation and query to continue will be displayed.



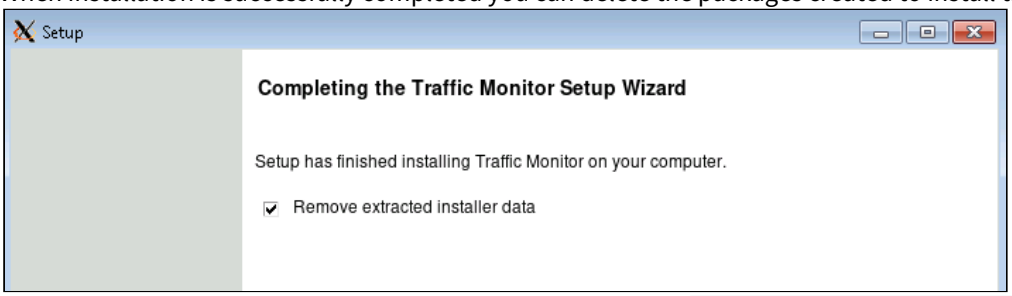
To start the installation and press **Nex**t
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed



The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

- When installation is successfully completed you can delete the packages created to install the System.



  This data is recommended to delete. To do this mark the field **`Remove exctracted installer data`**.
- To finalise the installation press **Finish**.
- To apply the environment change you should certainly log off the System and log in again or restart the server.
- If you require the list of Traffic Monitor services to be displayed enter the command as follows:
  `iwtm status`

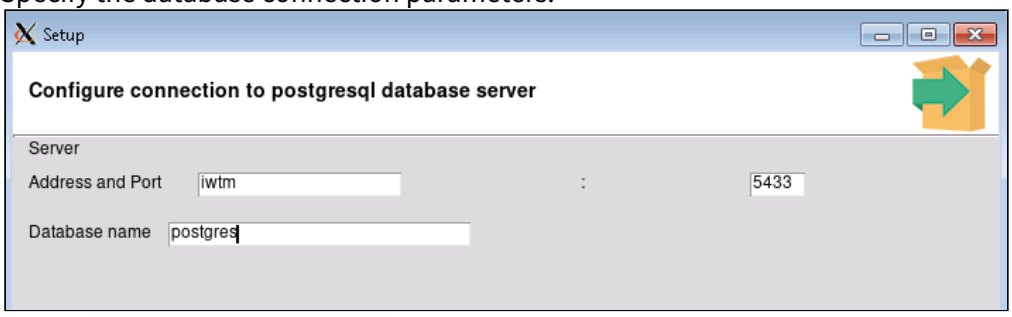
Installing Interceptors template

If you've selected Interceptors installation template:

1. Select a database the System to operate with:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

   > **Note:**
   >
   > DBMS type should comply with the one selected for Database template.

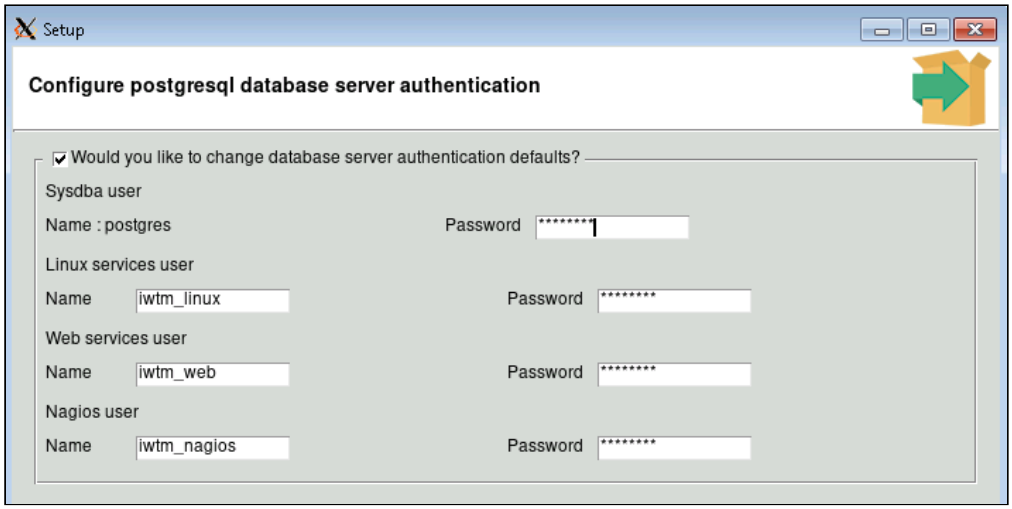
2. Specify the database connection parameters:



   - **`Address and Port -`** IP address, database server domain name and connection port.
   - **`Database name`** - The name of database to be used, where the scheme is to be added.

   > **Note:**
   >
   > In graphical mode active fields contain the default values.

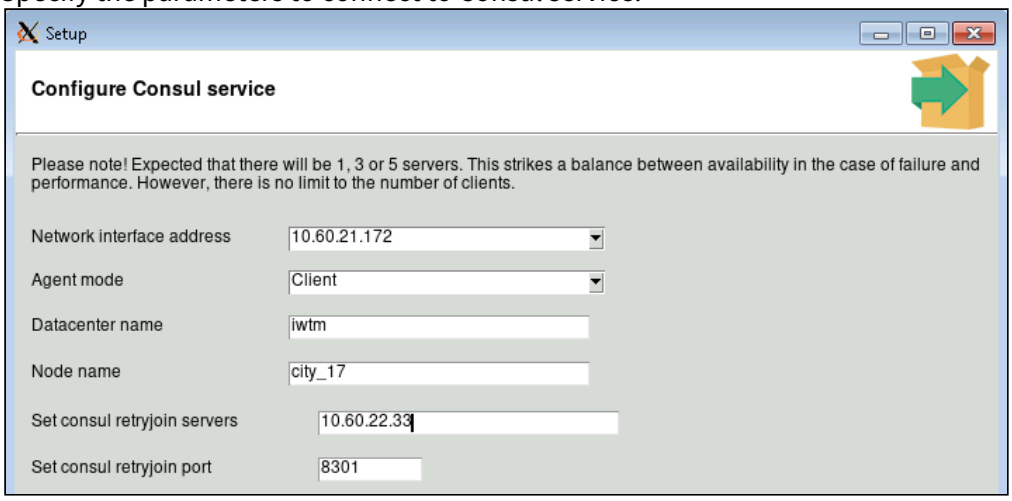
3. If required you can change the default values of DB authentication parameters.



To edit the values mark the field next to question. This will let you edit the following sections:

- **`Sysdba user`** - Password of user account having sysdba permissions;
- **`Linux services user`** - Name and password of Linux services user;
- **`Web services user`** - Name and password of web services user;
- **`Nagios user`** - Name and password of nagios user.

4. Specify the parameters to connect to Consul service:



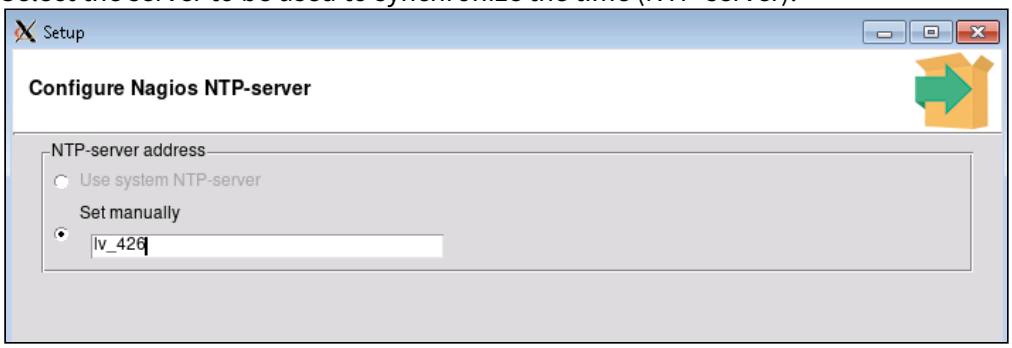
- **`Network interface address`** - select IP address of network interface. To select from the list of parameters click ▼ and select the required value.
- Consul operation mode. Two modes are available:
  - **`Server`**
  - **`Client`**

> **Warning!**
>
> One cluster must have an odd number of Consul servers, but not more than 5.

- **`Database name`** - The name of database to be used, where the scheme is to be added.
- **`Node name`** - server name, where Traffic Monitor components are installed.

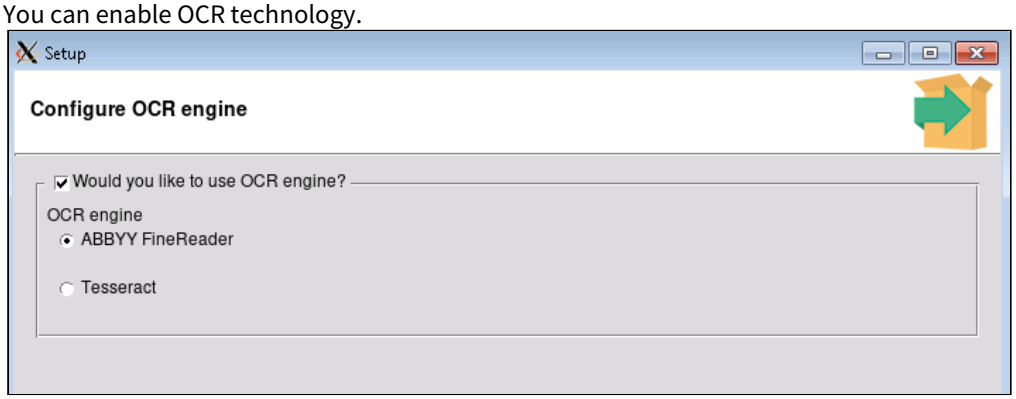
- **`Consul retryjoin servers`** - list of Consul servers, which are required to connect to. Input values via comma separated list. If you have one Consul server per one cluster on the current computer, leave thy field empty.
- **`Consul retryjoin port –`** connection port to specified Consul servers

5. Select the server to be used to synchronize the time (NTP-server):



- **`Use system NTP-server`** ;
- **`Set manually`** - you can manually specify NTP server name. If selected, you should input IP address or NTP server available.

- You can enable OCR technology.

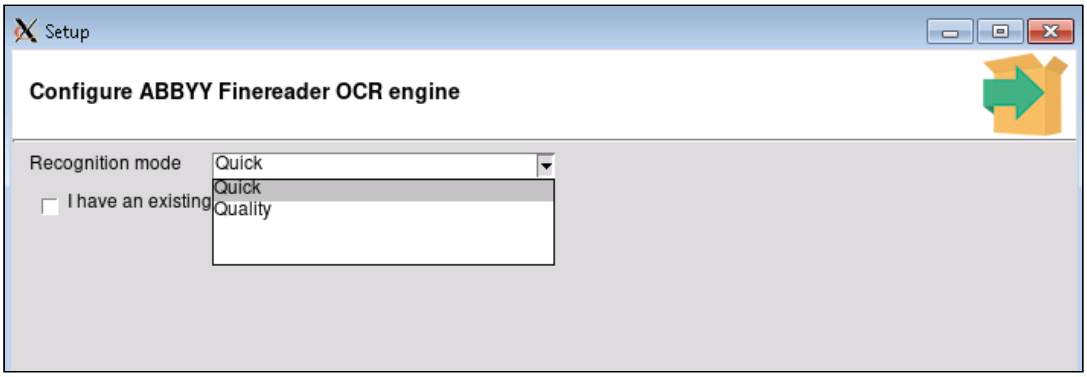


In this case you should select one system to be used:

- **`ABBYY FineReader`** ;
- **`Tesseract`** .

> **Note:**
>
> For OCR operation you should enable the technology when installing Web console template.

- If ABBYY Finereader is selected as OCR extractor:



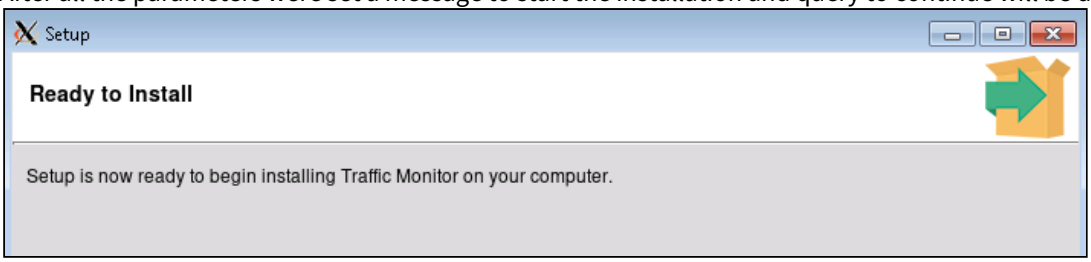
a. Select a

recognition mode:

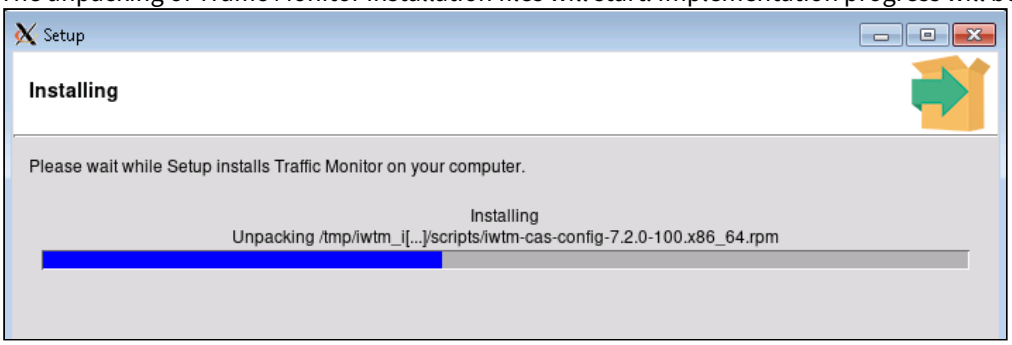
- `Quick` – a fast mode;
- `Quality` – a detailed mode providing higher quality of recognition.

b. Confirm that you have an active license to use ABBYY Finereader. In case you have no active license, type **N** and press **Enter**. In this case ABBYY Finereader will be installed with no license. To use ABBYY Finereader you can manually add an active license later. For more details, please see "*InfoWatch Traffic Monitor. Administation Guide*" "Configuring OCR Extractors " article.

- After all the parameters were set a message to start the installation and query to continue will be displayed.



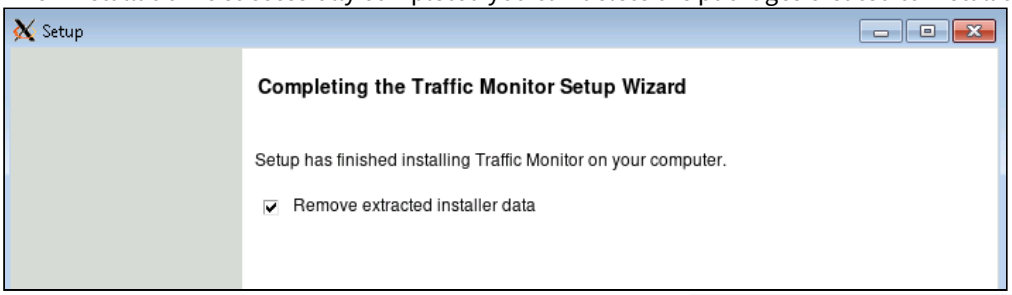
To start the installation and press **Nex**t
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed



The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

- When installation is successfully completed you can delete the packages created to install the System.



This data is recommended to delete. To do this mark the field `Remove exctracted installer data`.

- To finalise the installation press **Finish**.
- To apply the environment change you should certainly log off the System and log in again or restart the server.
- If you require the list of Traffic Monitor services to be displayed enter the command as follows:
  `iwtm status`

As a result of installation, the System creates accounts listed in "Pre-installed Server Settings".

After the completion of 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*».

> **Note:**
>
> If you require expand the System after is was installed anв add some additional servers you should register each of them in Consul cluster. For more details, please see «*InfoWatch Traffic Monitor. Administration Guide*», "Distributed installation" of "
>
> Service-to-service cooperation setup (Consul service)" section.

The list of processes to be run on one server onsly is described in «*InfoWatch Traffic Monitor. Administration Guide*» "Check of Process Autostart" article. More details on how to enable and disable processes autostart please see "Enabling and Disabling Process Autorun" article. You can read more about the processes in «*InfoWatch Traffic Monitor. Administration Guide*» "List of Traffic Monitor Server End Processes" article.

3.1.3 Installing the System in silent mode using parameter file

To reduce a user's role in the System installation process there is a silent mode of installation. In this mode Traffic Monitor can be installed using default parameters.

An options file is realized to be used as a parameter file. In this file you can set required installation parameters. When starting the installation via parameter file, the values specified in this file will be considered the default parameters.

Before starting the installation make sure the common actions are performed:

1. To log into the System, enter login and password (you should enter as a **root** user).

> **Warning!**
>
> Before running the installation make sure that the server complies with the OS and network settings requirements. If you plan using a remote database, you should update it first to the version supported by Traffic Monitor. In case of PostgreSQL DBMS using, you should preliminarily configure it.
>
> Before installing to clear memory, it is recommended to reboot the server on which database will be deployed.

> **Warning!**
>
> By default you are not allowed to install the System on server which has numbers at the beginning of its name. If you need to allow the server's name to begin with a number, use the command line to specify the value 1 of the parameter --allow_digits_at_hostname_begin.
>
> Herewith, make sure that the network check is active – the parameter --skip_check_network should have the value 0 (the check is active by default).

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`** (where x.x.x.xxx is a number of build);
   - **`iwtm-postgresql-13.2-x.xx.x.tar.gz`** - if you use PostgreSQL DBMS;
   - **`iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz`** - if you use Oracle DBMS.

   As per our example:
   - **`iwtm-installer-7.2.0.123-rhel7`**;
   - **`iwtm-postgresql-13.2-7.2.0.tar.gz`** - if you use PostgreSQL DBMS;
   - **`iwtm-oracle-19.0.0.0.0-7.2.0.tar.gz`** - if you use Oracle DBMS.

   > **Note:**
   >
   > When using Oracle DBMS and network file system, before running the installation:
   >
   > - **when using Oracle Real Application Clusters (RAC):**
   >
   >   Install the mount options according to official website instructions.
   > - **if RAC is not used:**
   >
   >   Open the mount points (`/etc/fstab` by default) and make sure the `noac` option is not used and the value of `actimeo` is not set to `0`.
   >
   >   For more details, please see official website info.

4. Enter the command to shift to Traffic Monitor distributive directory.
   As per our example:
   `cd /distr`
5. Before running the installation make the installer file is executable. To do this use the following command:
   `chmod u+x ./iwtm-installer-x.x.x.xxx-rhel7`
   As per our example:
   `chmod u+x ./iwtm-installer-7.2.0.123-rhel7`

Parameter file (option file)

The file contains the following parameters description:

<parameter's_name>=<parameter's_value>

You may leave comments using #.

Parameter file example:

```
# This file is just an example
product_type=tme
installation_type=distributed
template_database=1
template_indexer=1
template_web=1
template_interceptors=0
product_language=rus
```

The example above contains the parameters as follows:

- product edition type - Traffic Monitor Enterprise (TME);
- installation type - distributed;
- the templates used to be installed on the server:
    - Database;
    - Indexer;
    - Web console.
- main product language - Russian.

Warning!

The parameters which are not specified in the file will have the default values. The full list of parameters is specified in the table below.

To use the parameter file go to installer directory and run it using `--optionfile` specifying the file which was previosly created.

Example of using parameter file:

```
./iwtm-installer-7.2.0.84-rhel7 --optionfile /some_directory/option-file-example
```

An alternative way to use: give the parameter file the same name the installer has, but use `.options` extension and copy it to installer directory. In this case the running installer will consider the file parameters the default values.

Silent mode installation

To install in silent mode use `--mode unattended` option.

Level of interaction with user is set by `--unattendedmodeui` parameter, which has the following values:

- `none` - no information displayed while installing and no interaction is required;
- `minimal` - status of implementation is displayed while installing, no interaction is required;
- `minimalWithDialogs` - status of implementation is displayed while installing, pop-up windows can be displayed and interaction with user can be required.

Example of installer running command in silent mode with no user assistance and using parameter file:

```
./iwtm-installer-7.2.0.84-rhel7 --optionfile /some_directory/option-file-example --mode unattended --
unattendedmodeui minimal
```

Warning!

If available configured OS repositories are missing, the preparation process will stop with the following error message:

```
Preparing installation.../Warning: Failed to prepare installation:
Missing OS repos or unsupported OS. Please mount and/or enable OS packages
repository and try once again.

For details refer to
/var/log/infowatch/install/iwtm-installation_20211007114106.log or
/tmp/installbuilder_installer_11672.log if the first doesn't exist
Press [Enter] to continue:
```

To fix this error press **Enter** to exit, connect the standard RHEL repository, EPEL repository and restart the installer.

For more details on the error refer to the log files, specified in the error message.

Note:

If Consul service is configured incorrectly, the following warning message will be displayed:

```
\Warning: You should run 'iwtm start' command manually after fixing problems with
Consul.
Press [Enter] to continue:
```

To finish installation press **Enter**.

For correct work of System check and configure Consul service cluster

1. Start Consul service with the command:
   `service iwtm-consul start`
   To check the service status enter the command:
   `service iwtm-consul status`
2. To check Consul enter the command:
   a. To display IP address of main server (leader) of cluster:
      `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   b. To display information about cluster members:
      `consul members`
3. If the IP address of cluster leader is not displayed, configure cluster of Consul service. After configuration is complete, repeat checking (step ii).

If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

Note:

If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

In case the process is over with no errors, the packages created for installation will be removed by installer.

Full composition of parameter file

The table below contains full list of possible parameters and their default values.

Note:

`<ora|pg>` in default values means you should select one value in accordance with DBMS specified earlier:

- `ora` - for Oracle DBMS;
- `pg` - for PostgreSQL DBMS.

Name	Default value	Valid values	Description	Note
`use_debug`	`0`	`0, 1`	Enabling the scripts debug mode, which are a part of the installer	The parameter is used to collect the detailed logs in case of errors occured while the installer operation
`skip_check_swap`	`0`	`0, 1`	Disabling the check of Swap space volume	
`skip_check_space`	`0`	`0, 1`	Disabling the check of free space volume on disk	
`skip_check_ram`	`0`	`0, 1`	Disabling the check of RAM volume	
`skip_check_network`	`0`	`0, 1`	Disabling the check of available network	
`skip_check_tmp`	`0`	`0, 1`	Disabling the check of temporary directory	
`skip_check_home`	`0`	`0, 1`	Disabling the check of home directory	
`setup_cron_jobs`	`1`	`0, 1`	Set targets for cron planner	
`log_dir`	`/var/log/infowatch/install`		Path to log files directory	

Name	Default value	Valid values	Description	Note
`product_type`	`tme`	`tme`, `tms`	Traffic Monitor edition type	
`product_language`	`rus`	`rus`, `eng`	Main product language	
`installation_type`	`all_in_one`	`distributed`, `all_in_one`	Installation type	In case Traffic Monitor Enterprise edition is selected (`product_type=tme`)
`template_database`	`0`	`0, 1`	Install Database template	In case distributed installation is selected (`installation_type=distributed`)
`template_indexer`	`0`	`0, 1`	Install Indexer template	
`template_web`	`0`	`0, 1`	Install Web console template	
`template_interceptors`	`0`	`0, 1`	Install Interceptors template	
`db_classification_lang_ru`	`1`	`0, 1`	Set Russian for classification base	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected
`db_classification_lang_en`	`0`	`0, 1`	Set English for classification base	
`db_classification_lang_ma`	`0`	`0, 1`	Malay is set for classification base	
`db_installation_type`	`local`	`local`, `remote`	Database location	
`db_type`	`postgresql`	`oracle`, `postgresql`	Selecting DBMS	Available when installing to OS Red Hat Enterprise Linux and edition type is Traffic Monitor Enterprise (`product_type=tme`)

Name	Default value	Valid values	Description	Note
`db_server_address`	`iwtm`		Server address with Database template or remote database server address	For Indexer, Interceptors and Web console templates For all in one installation type and Database template when using a remote database (`db_installation_type=remote`)
`db_server_port`			Server port with database	
`db_name`	`postgres` or `iwtm` (according to `db_type` parameter)		Database name	
`db_sysdba_password`	`xxXX1234`		Password of SYSDBA user	
`db_scheme_owner_name`	`iwtm`		Name of database security scheme owner	In case all-in-one installation type (`installation_type=all_in_one`), Database template (`template_database=1`) or Web console template (`template_web=1`) are selected
`db_scheme_owner_password`	`xxXX1234`		Пароль владельца схемы базы данных	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected
`db_linux_user_name`	`iwtm_linux`		Name of Linux services user	

Name	Default value	Valid values	Description	Note
`db_linux_user_password`	`xxXX1234`		Password of Linux services user	
`db_web_user_name`	`iwtm_web`		Name of web services user	
`db_web_user_password`	`xxXX1234`		Password of web services user	
`db_nagios_user`	`iwtm_nagios`		Name of nagios user	
`db_nagios_password`	`xxXX1234`		Password of nagios user	
`db_auth_change_defaults`	`0`	`0, 1`	Change the default database connection parameters	
`db_storage_type`	`normal`	`normal, fast_slow, rotate`	Data storage mode	
`db_storage_main_tbs_path`	`/u02/<ora|pg>data`		Path to main tablespace	
`db_storage_dtbs_paths_number`	`1`	1 - 10	Number of pathes to daily tablespaces	
`db_storage_fast_disk_path`	`/u03/<ora|pg>data`		Path to directory where daily tablespaces are stored on fast drive	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) and `fast_slow` data storage mode (`db_storage_t`

Name	Default value	Valid values	Description	Note
db_storage_dtbs_days_on_fast_disk	7		Storage period of daily tablespaces data on fast drives, in days	vpe=fast_slow) are selected
db_storage_change_defaults	0	0, 1	Change the database storage parameters	
db_storage_dtbs_path_1	/u02/<orapg>data1		Path to daily tablespace #1	Если выбран тип установки all-in-one (installation_type=all_in_one) или шаблон База данных (template_database=1), также зависит от значения параметра db_storage_dtbs_paths_number
db_storage_dtbs_path_2	/u02/<orapg>data2		Path to daily tablespace #2	
db_storage_dtbs_path_3	/u02/<orapg>data3		Path to daily tablespace #3	
db_storage_dtbs_path_4	/u02/<orapg>data4		Path to daily tablespace #4	
db_storage_dtbs_path_5	/u02/<orapg>data5		Path to daily tablespace #5	
db_storage_dtbs_path_6	/u02/<orapg>data6		Path to daily tablespace #№6	
db_storage_dtbs_path_7	/u02/<orapg>data7		Path to daily tablespace #7	
db_storage_dtbs_path_8	/u02/<orapg>data8		Path to daily tablespace #8	
db_storage_dtbs_path_9	/u02/<orapg>data9		Path to daily tablespace #9	
db_storage_dtbs_path_10	/u02/<orapg>data10		Path to daily tablespace #10	
db_archiving_dtbs_path	/u02/arch		Path to directory where archived tablespaces are stored	In case all-in-one installation type (installation_type=all_in_one) or Database template (

Name	Default value	Valid values	Description	Note
				`template_database=1`) is selected
`db_days_before_archiving_nonviolations`	`45`		Number of days to store events without violations before archiving	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected, and `db_archive_nonviolations=1`
`db_archive_nonviolations`	`0`	`0, 1`	Archive events without violations	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected
`db_days_before_archiving_violations`	`45`		Number of days to store events with violations before archiving	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected, and `db_archive_violations=1`
`db_archive_violations`	`0`	`0, 1`	Archive events with violations	In case all-in-one installation type (`installation_type=all_in_one`) or Database

Name	Default value	Valid values	Description	Note
				template (`template_database=1`) is selected
`db_days_before_archiving_screenshots`	`45`		Number of days to store screenshots before archiving	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected, and `db_archive_screenshots=1`
`db_archive_screenshots`	`0`	`0, 1`	Archive screenshot events	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected
`db_archiving_dtbs_change_defaults`	`0`	`0, 1`	Change default archiving parameters	
`db_days_before_removing_nonviolations`	`90`		Number of days to store events without violations before deleting	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected, and `db_remove_nonviolations=1`
`db_remove_nonviolations`	`0`	`0, 1`	Delete events without violations	In case all-in-one installation type (`installation_type=all_in_`

Name	Default value	Valid values	Description	Note
				`one`) or Database template (`template_database=1`) is selected
`db_days_before_removing_violations`	`90`		Number of days to store events with violations before deleting	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected, and `db_remove_violations=1`
`db_remove_violations`	`0`	`0, 1`	Delete events with violations	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected
`db_days_before_removing_screenshots`	`90`		Number of days to store screenshot events before deleting	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected, and `db_remove_screenshots=1`
`db_remove_screenshots`	`0`	`0, 1`	Delete screenshot events	In case all-in-one installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected

Name	Default value	Valid values	Description	Note
`db_removing_dtbs_change_defaults`	`0`	`0, 1`	Change default deleting parameters	
`consul_bind_addr`	`<list_of_ip_addresses>`		Consul network interface address	
`consul_mode`	`server` - for Database template and All in one installation type `client` - for the rest of templates	`server, client`	Consul operation mode, server and client	
`consul_datacenter_name`	`iwtm`		Consul data center name	
`consul_node_name`	`<hostname>`		Node name	
`consul_retryjoin_manual`			List of Consul agents	
`consul_retryjoin_port`	`8301`		Port to connect Consul agents	
`ntp_manual_addr`			NTP server address	In case NTP server manual specification is selected (`ntp_mode=ntp_manual_addr`)
`ntp_mode`	`ntp_use_system`	`ntp_use_system`, `ntp_manual_addr`	NTP server type: • `ntp_use_system` - use system NTP-server; • `ntp_manual_addr` - specify NTP	

Name	Default value	Valid values	Description	Note
			server manually.	
`sphinx_server_address`			Sphinx server address	In case Web console template (`template_web=1`) is selected and Indexer template (`template_indexer=0`) is not selected
`sphinx_exact_match_words`	`0`	`0, 1`	Enable exact word match indexing	In case all-in-one installation type (`installation_type=all_in_one`) or Indexer template (`template_indexer=1`) is selected
`sphinx_change_language_settings`	`0`	`0, 1`	Change list of sphinx languages	
`sphinx_langs`	`rus`	`rus eng deu fra spa ita ara ukr ron lav bel pol aze tur srp kir uzb fin kaz msa nld vie por tat ell lit kat hye ces slk fas hin sin tgk sah zho`	List of sphinx languages	Sequence of languages defines the priority

Name	Default value	Valid values	Description	Note
`ocr_enabled`	`1`	`0, 1`	Enable OCR using	In case all-in-one installation type (`installation_type=all_in_one`), Interceptors template (`template_interceptors=1`) or Web console template (`template_web=1`) are selected
`ocr_type`	`ts`	`fre`, ts	Selecting OCR extractor: • `fre` - ABBYY FineReader; • `ts` - Tesseract.	In case all-in-one installation type (`installation_type=all_in_one`) or Interceptors template (`template_interceptors=1`) is selected
`ocr_finereader_mode`	`quality`	`quick, quality`	OCR ABBYY FineReader operation mode	In case OCR ABBYYFineReader (`ocr_type=fre`) is selected
`ocr_finereader_have_license`	`1`	`0, 1`	License issued for OCR ABBYY FineReader	
`db_unpack_dir`	`/tmp/iwtm_installer/database`	Line - path to directory	DB archive will be unpacked to derictory	Directory will be created automatically. You can specify an existing directory. In case the installation is over with no errors, the directory will be removed automatically.

Name	Default value	Valid values	Description	Note
`packages_unpack_dir`	`/tmp/iwtm_installer/packages`	Line - path to directory	Traffic Monitor installation packages will be unpacked to directory	Directory will be created automatically. You can specify an existing directory. In case the installation is over with no errors, the directory will be removed automatically.

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.

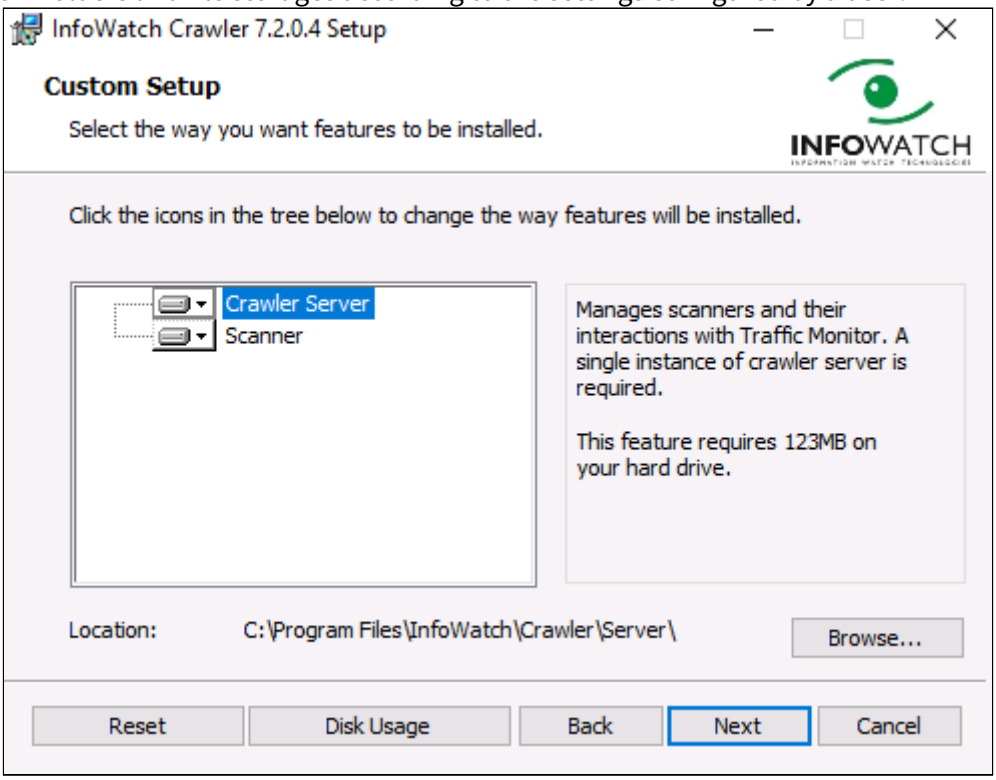
> **Warning!**
>
> Before the installation, make sure that the servers Traffic Monitor and Crawler are connected. For this, check Crawler server's availability by running the following command on Traffic Monitor server: ping <short name of Crawler server>. Otherwise, Crawler subsystem can be installed,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

To install Crawler:

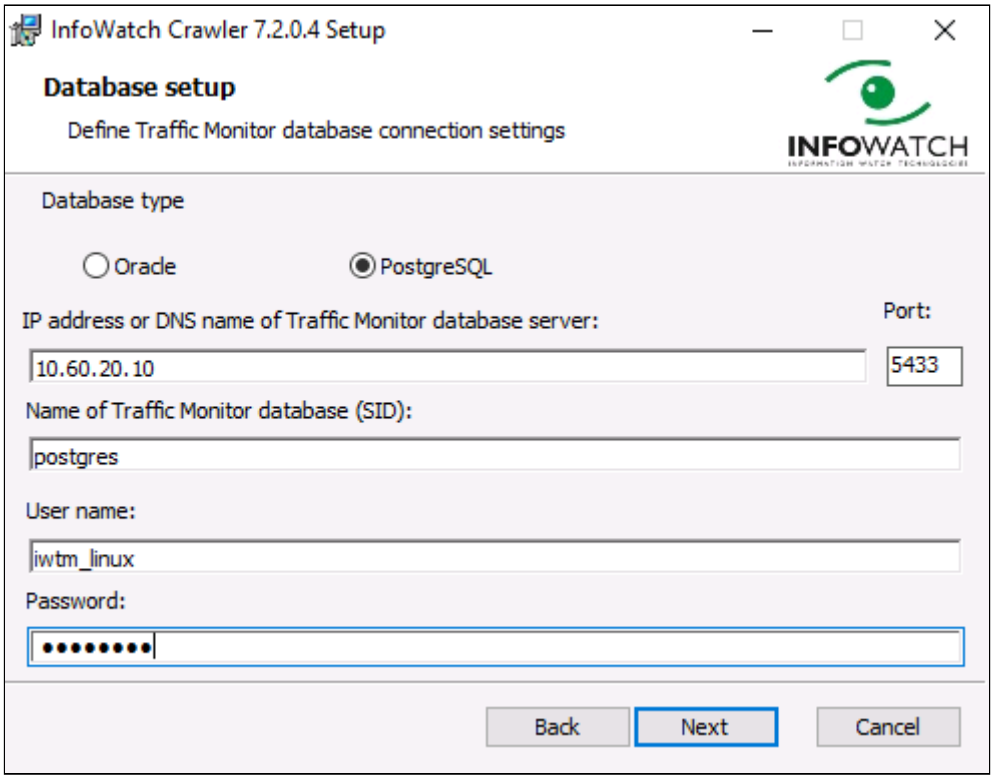
1. Run `Crawler_vx.x.x.xxx.msi` installation package, where x.x.x.xxx is a version number.

> **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. Read the End User License Agreement. If you accept the licensing terms, select **I accept the terms in the License Agreement** and click **Next.**
4. In the Installation Scope screen, click **Next**.
5. 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.



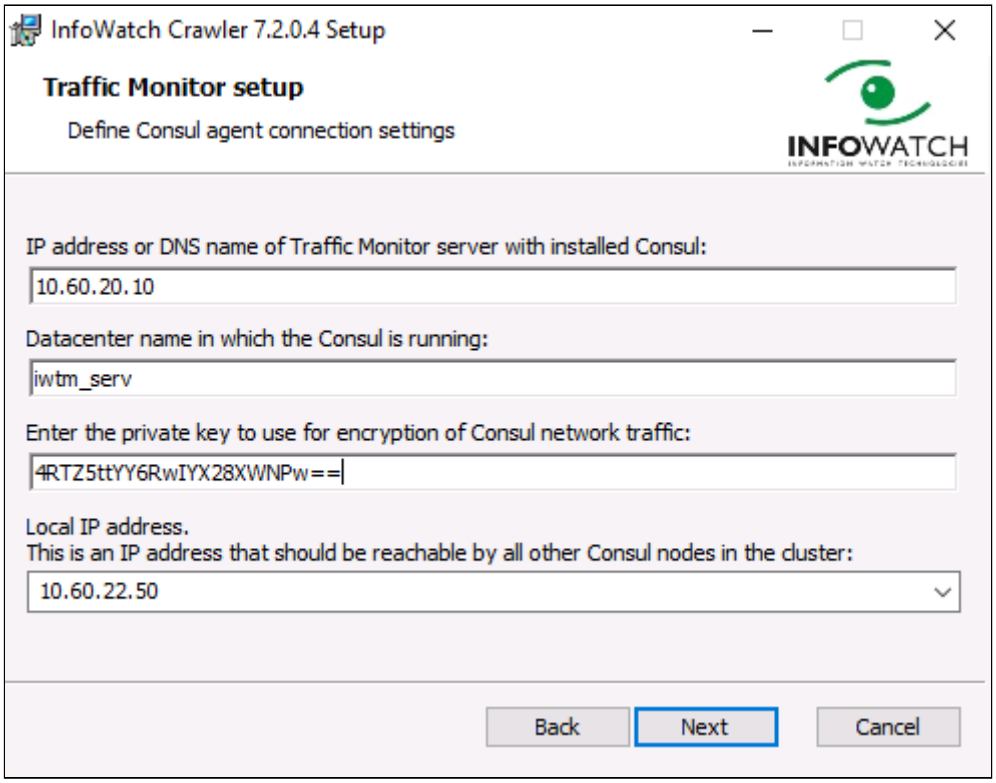
   If you do not want to install a particular component, click on this feature and select ✕ **Entire feature will be unavailable**.
   Specify paths to the directories where selected components will be installed and click **Next**.
6. If at the **Custom Setup** step, you have chosen the **Server Crawler**:
   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.

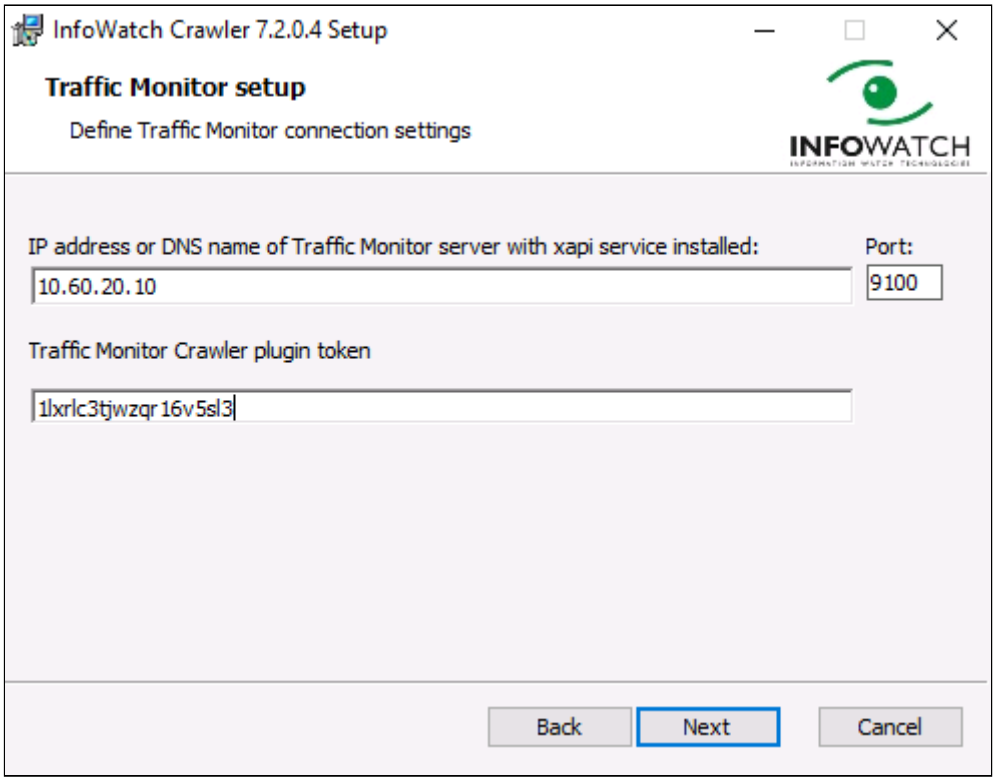
b. Specify the parameters to connect Consul agent to Traffic Monitor server, click **Next**.



To enter data in the fields **Datacent name in which the Consul is running** and **Enter the private key to use for encryption of consul network traffic** 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.

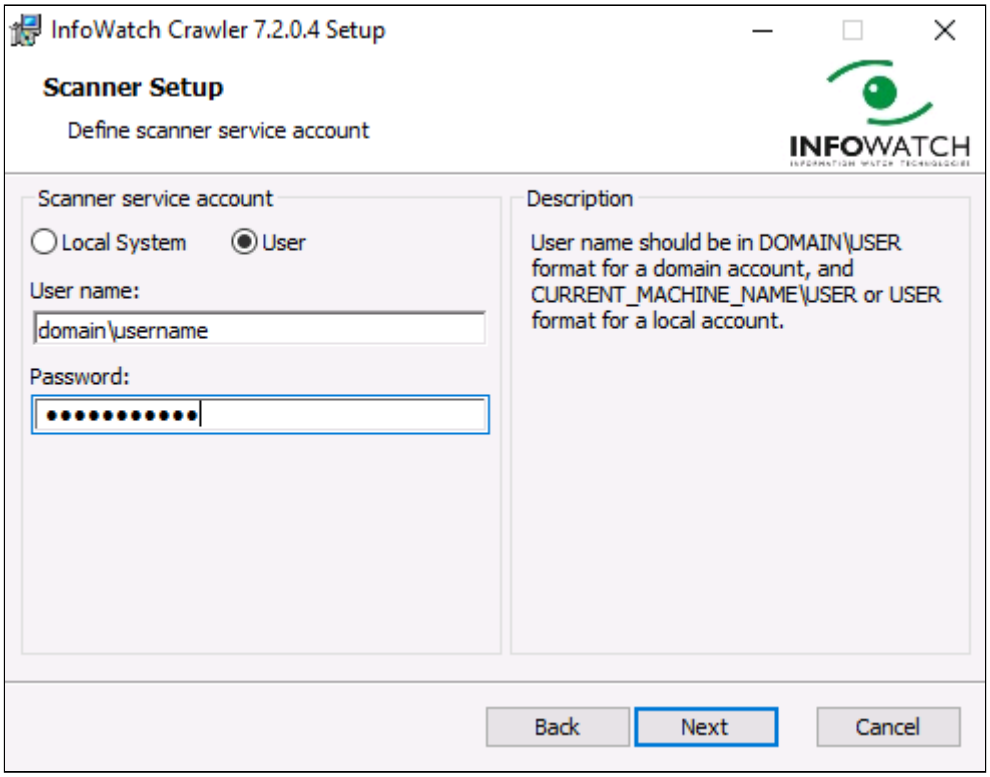
c. Specify parameters of connection between `InfoWatch.Crawler.Server` and Traffic Monitor server, click **Next**.



Fill in the fields the following way:

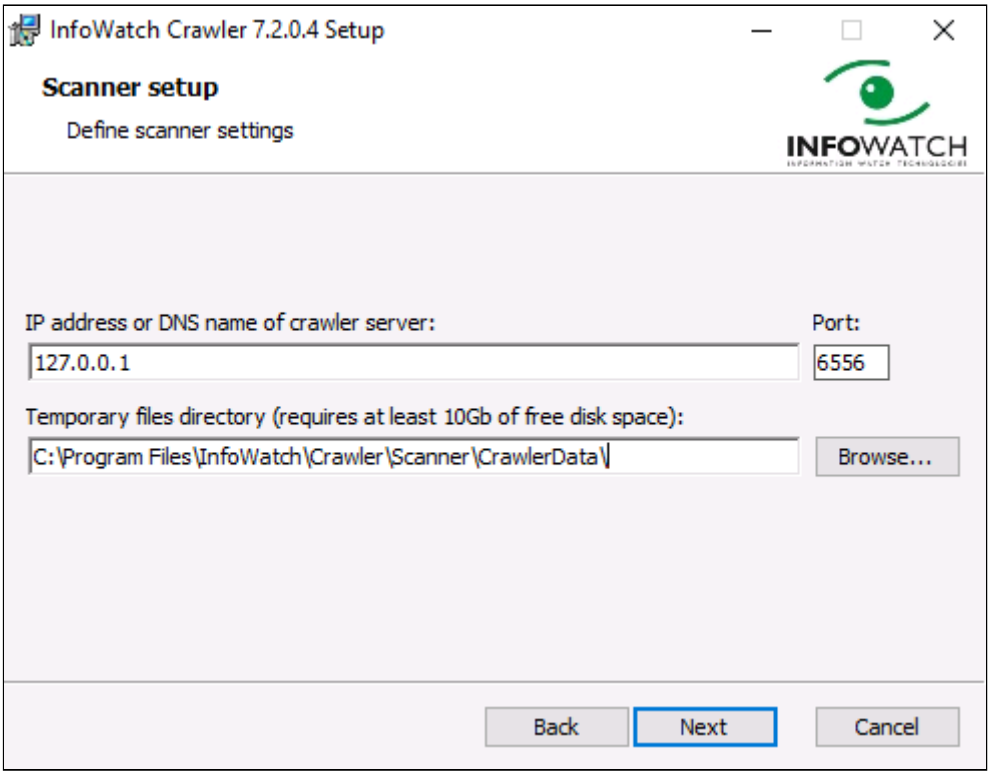
- **IP address or DNS name of Traffic Monitor server with xapi service installed** - in case of distributed installation, specify the IP address or DNS name of TM server (TME Node Server).
- **Traffic Monitor Crawler plugin token** - use data from the **Plugins** section of Traffic Monitor Management Console.

7. 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.



8. Click **Next**.
9. Click **Install** to start the installation. When the installation is complete, click **Finish**.
10. 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. enter 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 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 7).

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 R2/2016/2019;
- Microsoft .NET Framework 4.5.2 pack.

Download PostgreSQL 13 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.

After PostgreSQL is installed, please open `postgresql.conf` configuration file and assign value 250 to `"max_connections"` parameter.

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.

Device Monitor server and Device Monitor Agent should be installed in the same time zone. This will assure that the time of intercepted event is correct.

> **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

> **Warning!**
>
> Before starting the installation, see "Installing InfoWatch Device Monitor ".

> **Warning!**
>
> 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**
   Open the folder where Device Monitor distribution kit is kept. 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
   - Distribution service

   You can change the list of components you want to install. All components are to be installed on one workstation by default. If you plan to use a Management Console or Distribution service, in the opened window 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. When installing a Distribution service, a new Agents distribution kit will be automatically placed in the distribution directory.
   Click **Next**.
4. **Configuring server settings**
   On **Type of installed server** page select:
   - **Primary Server** - should be installed first. Agents and Management Console will connect to it.
   - **Secondary Server** - an additional server that balances Agents' workload.

   > **Warning!**
   >
   > 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.

   > **Warning!**
   >
   > 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 the 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**.

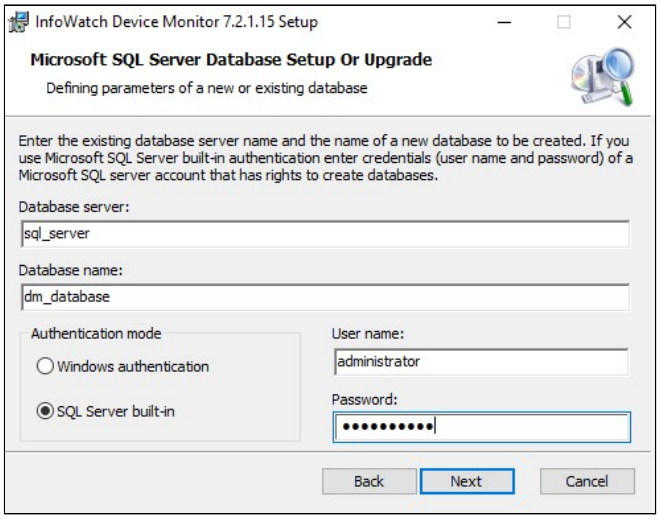
5. **Choosing a configuration file**
   If the new database installation is not performed, this step is skipped.
   To use the server configuration file exported before (see "*InfoWatch Traffic Monitor. User Guide*", "Import/Export Configuration" article), click **Open** and specify the configuration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

   > **Warning!**
   >
   > 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. See the recommendations of password creation in the article "Appendix A. Username and Password Recommendations".



When using Oracle DBMS configure the following settings:

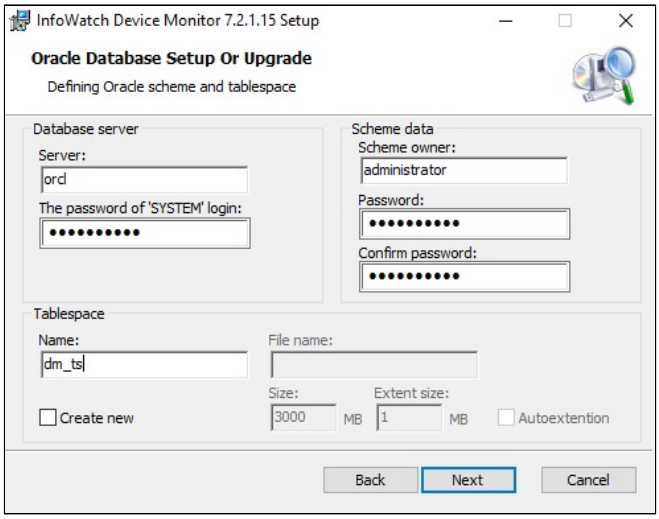
a. Set database server connection options:
- **Database server**. Database server name. For this parameter, use server alias `tns_name` from the **tnsnames.ora** file or TNS string representation.
- **The password of 'SYSTEM' login**. SYSTEM account password.

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

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

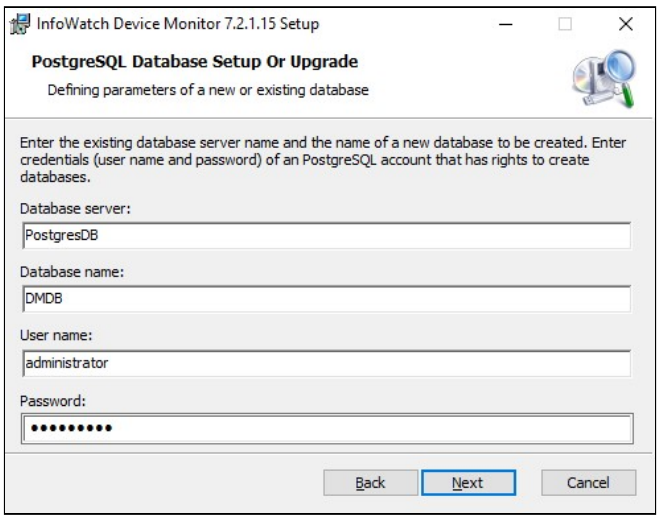
- **Scheme owner**. Database schema owner account name.
- **Password, Confirm password**. Database schema owner account password.
Password is assigned based on requirements specified in Oracle DBMS documentation.

c. Configure tablespace settings in the **Tablespace** box.
You can use an existing tablespace or create a new one. If you are using an 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: «*», «?», «/», «\», «|», «^», «:», «"». The 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**

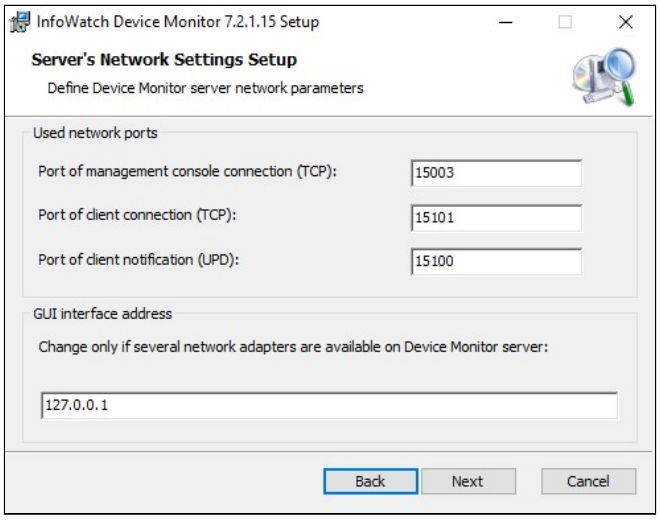
Configure Server parameters:

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.

> **Warning!**
>
> 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 used for InfoWatch Device Monitor launch according to "InfoWatch Device Monitor Server Setup Recommendations". If you select **User**, specify Windows domain account name and password. The 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.

      > **Warning!**
      >
      > If you are going to integrate Device Monitor with Traffic Monitor 5.5 or earlier use format: h`ost: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 is 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.

> **Warning!**
>
> Installing the 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 a virtual printer press **Install**.

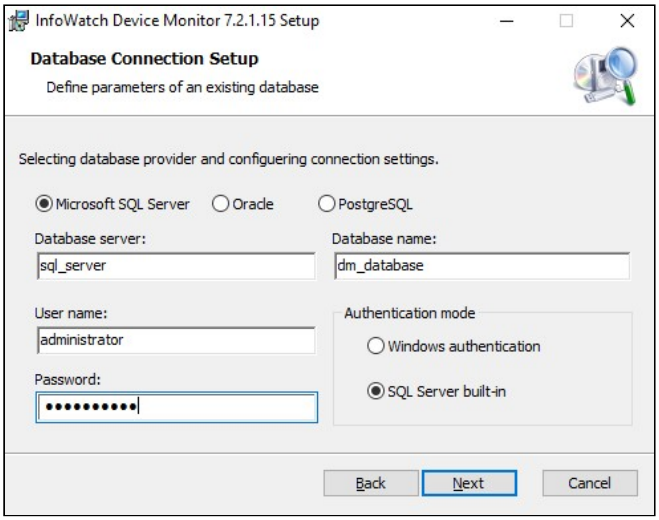
> **Note:**
>
> Signature installation may take a while (up to 30 minutes).

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
    Open the folder where Device Monitor distribution kit is kept. 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
        - Distribution service

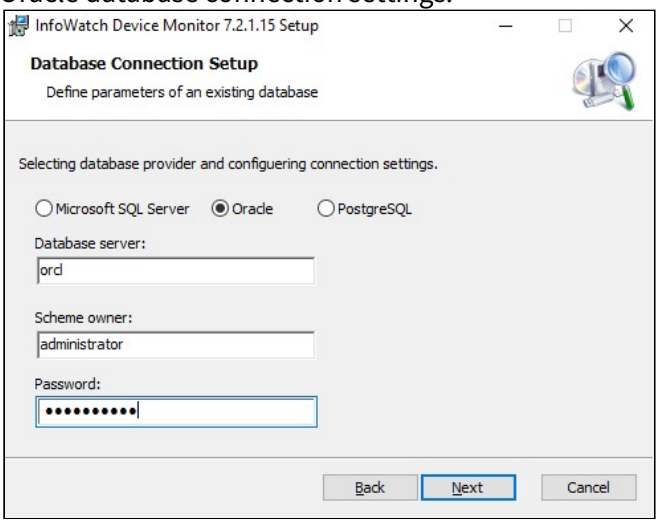
    You can change the list of components you want to install. All components are to be installed on one workstation by default. If you plan to use a Management Console or Distribution service on one workstation you do not need to install this feature:
    click **Management Console** or **Distribution service** and select **Entire feature will be unavailable** in the opened window. You can also change the folder to install the component: select this component in the list, click **Browse** and specify the needed location. When installing a Distribution service, a new Agents distribution kit will be automatically placed to distribution directory.
    Click **Next**.
    d. Configuring server settings
    Select the **Secondary server** as a **Type of installed server**.

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

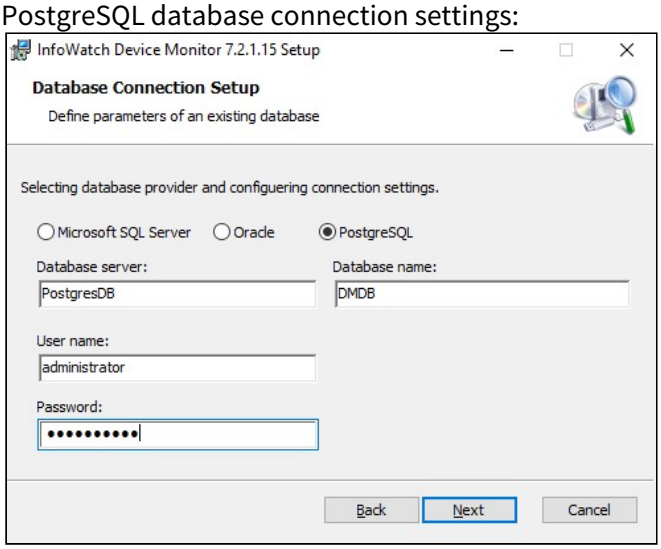
    e. Database connection setup
    Specify DBMS managing Device Monitor database and put in the rest connection parameters that were used while installing the primary server.
    Microsoft SQL Server connection settings
    If the account uses Windows authentication, and the database was created by a domain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



Oracle database connection settings:

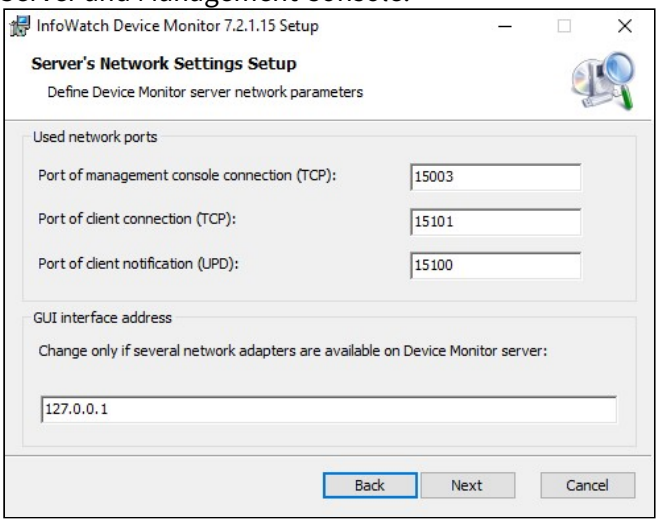


PostgreSQL database connection settings:



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. The 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

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);
- Automatic installation through InfoWatch Device Monitor Management Console (for details, see "*Infowatch Traffic Monitor. User Guide", "Active Directory Connecting and Synchronizing*" 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. If you are using VMWare Horizon VDI 8.0.0-16530 on your workstations, then disable the component ftapihook654.dll version 3.2.4.1. (see details in the article "VmWare Horizon VDI compatibility issues")
6. 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*);
7. 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.

8. If network connections settings (control panel) are not required to be used, disable it when creating InfoWatch Device Monitor Agent's distribution kit.
9. 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!

We highly recommend not installing InfoWatch Device Monitor Agents on computers with the same names. Such computers will be registered as a single computer, so the same policies will apply to them, the same events will be registered, etc.

Create an actual package to install Agent (see "Traffic Monitor. User Guide. Creating Installation Package") and write it to external device. The Agent can be installed by a user with local administrator rights on the computer.

Installing Device Monitor Agent to on the computer with OS Microsoft Windows using msi package followed by manual input of parameters:

1. **Running the Installation Wizard**
   Insert the external device containing Agent's distribution kit to computer drive. Then open the `Client` directory. In the catalog find and run the package for deploying on the required platform according to the parameters specified while packages forming. For example, `InfoWatch.DeviceMonitor.Client.7.2.0.x64.msi.cmd`.
   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 the 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 the parameters for connecting to the InfoWatch Device Monitor server:
   - **Server**. InfoWatch Device Monitor server name.
   - **Port**. Port number used for communication between InfoWatch Device Monitor Agent and Server (by default, port 15101 is specified).

   Click **Next**.

4. **Completing the installation**

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

Installing Device Monitor Agent to on the computer with OS Microsoft Windows using cmd package containing installation parameters:

1. **Enter Windows command line**
   Start the command line (cmd.exe) under the Administrator account.
2. **Run the script**
   a. Go to the catalog containing the installation script:
   `cd <path_to_script>`
   b. Run the script by entering its full name, for example:
   `InfoWatch.DeviceMonitor.Client.7.2.0.x64.msi.cmd`
   c. The installation without graphic interface will start in silent mode and without notifications. Wait till the installation is compele, then the log file with detailed information will be created.

Agent Installation via Software Distribution Tools

The corporate network administrator can perform Client centralized setup via software distribution tools. This section describes installation from Microsoft Active Directory.

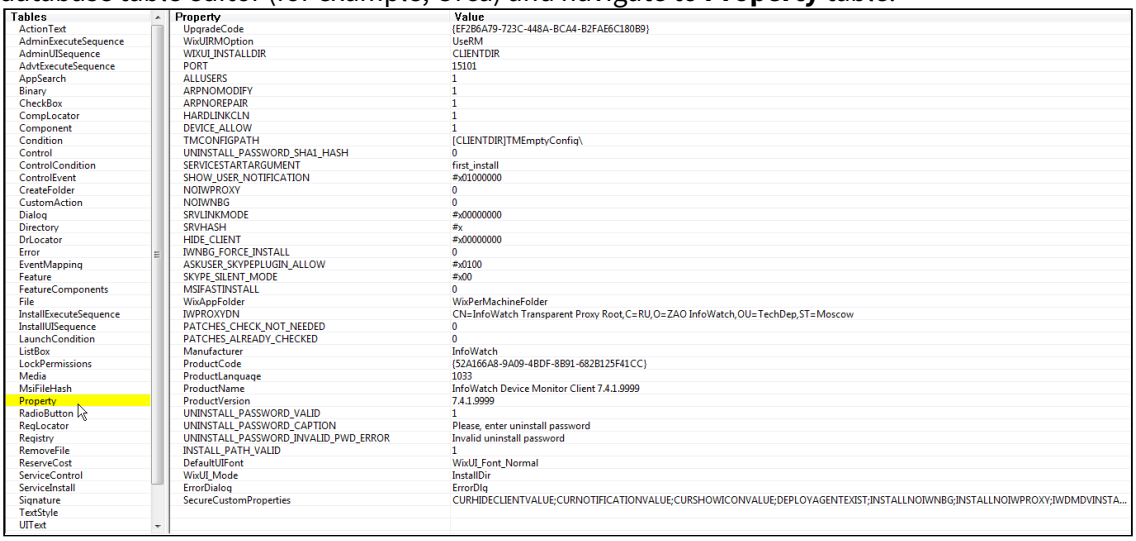
Agent installation from Microsoft Active Directory is carried out via group policy. To do so, you have to select a group policy that covers all target workstations. This policy may be assigned to:

- 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.

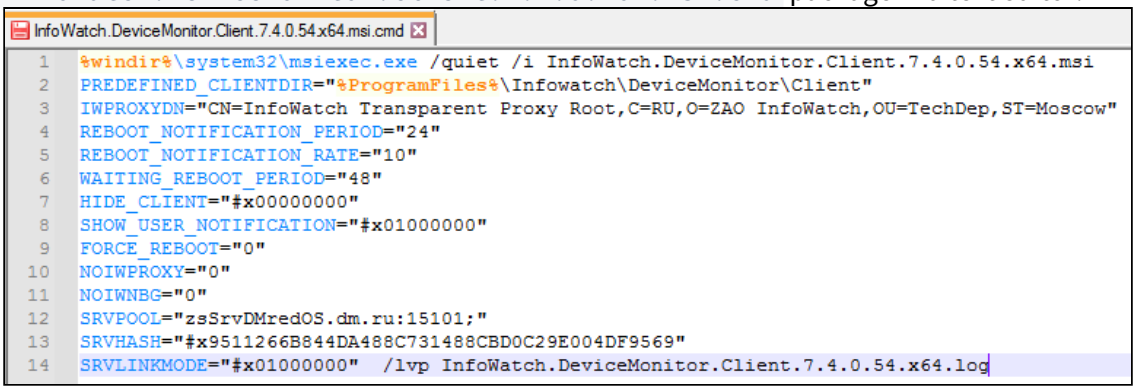
1. **Creating Installation Package**

a. Create `cmd` installation package, for example, `InfoWatch.DeviceMonitor.Client.7.2.0.x64.msi.cmd` as described in "*Infowatch Traffic Monitor. User Guide*", "Creating Installation Package" article).
b. Put the installation package to the network directory that can be read by all target computers within the domain.

2. **Creating Transform File**
   a. Open the `InfoWatch.DeviceMonitor.Client.7.2.0.x64.msi` installation file in a database table editor (for example, Orca) and navigate to **Property** table:

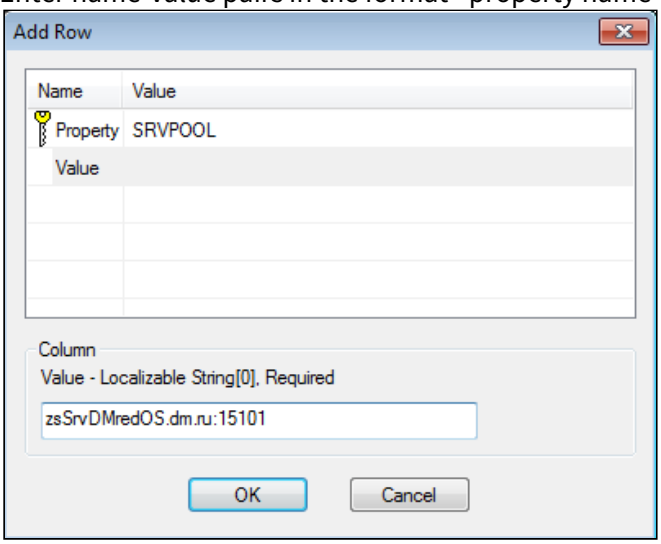


   b. In the menu bar, select **Transform** → **New Transform**
   c. Open the previously created `InfoWatch.DeviceMonitor.Client.7.2.0.x64.msi.cmd` package in a text editor:



   d. In the **Property** table, add missing properties or replace old property values with the new ones from the `cmd` package. To add a new property:
      i. Click on an empty row in the table.

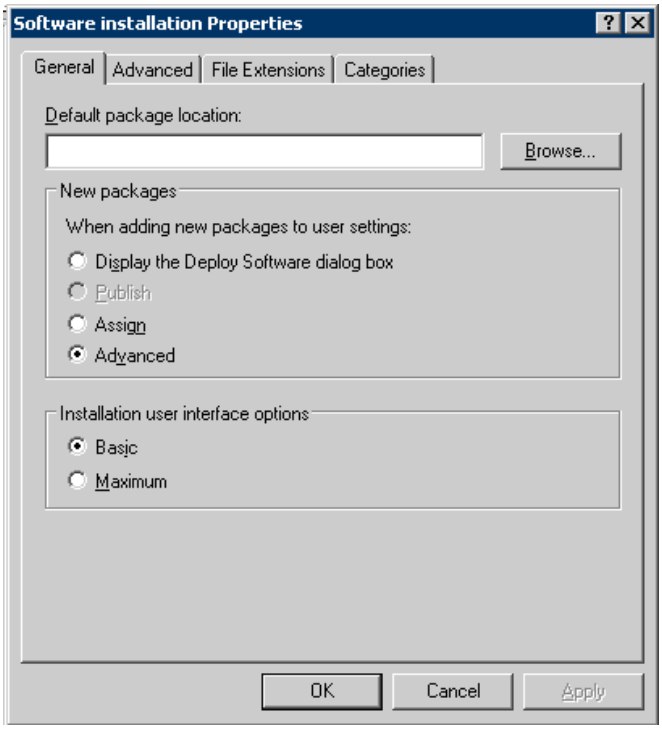
ii. Enter name-value pairs in the format <property name>=<"new value"> and click **OK**:



iii. To replace a property value, double-click the property value, enter the new value and press **Enter**.
Perform the steps above for all properties from the `cmd` package.

e. In the menu bar, select **Transform** → **Generate Transform**
f. Save the `mst` transform file.

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



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

4. **Preparing Agent installation task**

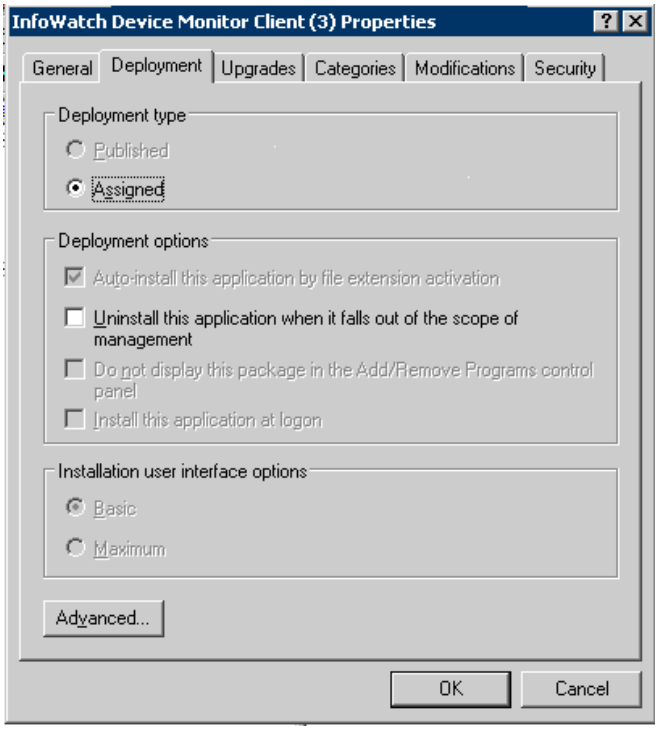
Agent installation task is created and configured on **Group Policy Object Editor** screen:

a. After opening **Group Policy Object Editor** box select **Software Settings** (**Computer Configuration** > **Software Settings**) in the console tree. Right-click the selected item and then select **New** > **Package**.

b. In the following **Open** dialog specify the `mst` transform file (first move the `msi` installation package to a network directory that is readable for all installation-target computers within the domain).

> **Note:**
>
> Some distribution systems allow you to specify deployment options. In such cases, you can pass the `InfoWatch.DeviceMonitor.Client.7.2.0.x64.msi.cmd` package directly to the distribution system.

c. Configure new package properties:
- Make sure all settings in **Deployment** tab comply with the following figure.



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

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

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

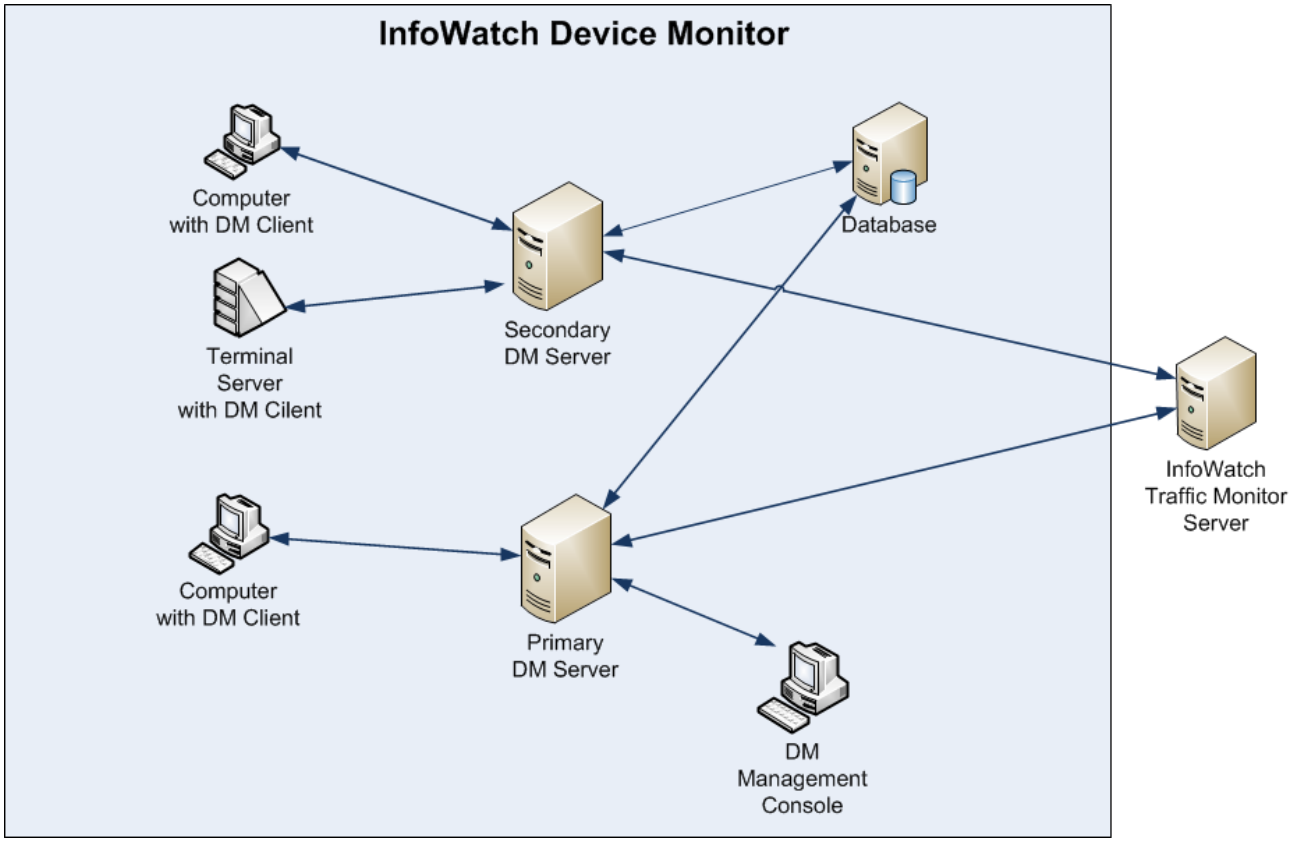
> **Important!**
>
> You can check if the Agent has been installed successfully in InfoWatch Device Monitor Management Console. All workstations the Agent has been successfully installed to must appear in the list in **Workstations** area. To view all managed workstations, click **Show all workstations**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

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 applications, retrieving data from agents and sending it to InfoWatch Traffic Monitor, distribution of deploy-agents to workstations
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
Distribution service	Getting and storing the new version of Agent's distibution kit
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. Deploy-agents Device Monitor are distributed from **base server** to **workstations**. Then, the workstations download Agent distributive from the closest distribution server. By default, the server is installed together with **Device Monitor server**. Several workstations can download the distributive simultaneously.
7. 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.
8. 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**

After the System is installed, please change the passwords:

- of `oracle` or `postgres` user (depends on which DB you are using);
- of Linux account (see details in the document "Traffic Monitor. Administration guide", "Changing the reset password").

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

Parameters of Traffic Monitor database:

`oinstall` - a group of the Oracle DBMS installation owner, which includes the following users:

- `iwtm`, `oracle` - for Oracle DB

- `iwtm`, `root` - for PostgreSQL DB

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:

Accounts which are available after starting:

- `sqlplus` - for Oracle;
- `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`	`iwtm_linux`	`xxXX1234`

Purpose	Oracle account name	PostgreSQL account name	Password
Account for Management Web Console to access the database	`iwtm_web`	`iwtm_web`	`xxXX1234`
Account for the monitoring subsystem (Nagios) to access the database	`iwtm_nagios`	`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!

Traffic Monitor can be updated to version 7.2 from versions 6.10.x, 7.0.x and 7.1.x. 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 a storage from which programs can be installed or updated. Before using the repository, you need to connect the repository so that the operating system could access it.

You can find a Guide on how to work with the repository on the Red Hat Enterprise Linux official website.

Warning!

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

Warning!

During the update, events are neither intercepted nor analyzed.

Примечание:

During IW Traffic Monitor update, the operations that require sysdba rights will be performed:

Oracle DBMS

- iwtm_logon_trg trigger creation that is used to provide iwtm_linux and iwtm_web users access to objects of iwtm scheme;
- Creation of sp_iwtm_execute_os_command procedure to run OS commands when creating, removing, archiving and restoring table space files;
- Setting user profile by default (password lifetime, password change limit and connection attempts limit);
- Setting sevice windows of dbms_scheduler;
- Disabling access to XDB using http protocol;
- Disabling dispatcher, as a particular server is used;
- Providing iwtm user with
    - DB installation, update and uninstallation rights;
    - Daily tablespaces creation, removing, archiving and restoring rights;
    - Rights that are used in InfoWatch Traffic Monitor code;
    - Rights to access DB statistics.

PostgreSQL DBMS

- Creation of wraper function to read files, stop and break sessions, create table spaces and provide iwtm with rights for them;
- Removing all views and functions from iwtm scheme in order to create the required ones later during update to a new version;
- Providing iwtm user with
    - Rights to create DB objects;
    - Rights to install, update, ininstall DB scheme;
    - Rights to create, remove, archive and restore table spaces;
    - Rights to clear postgres server statistics that are used in pgstat diagnostics script;
    - Rights for statistic views and tables to collect statistics of DB operation;
    - Rights that are used in InfoWatch Traffic Monitor code;
    - Rights to view DB statistics;
    - Rights for pgagent scheme to create and manage jobs.

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:

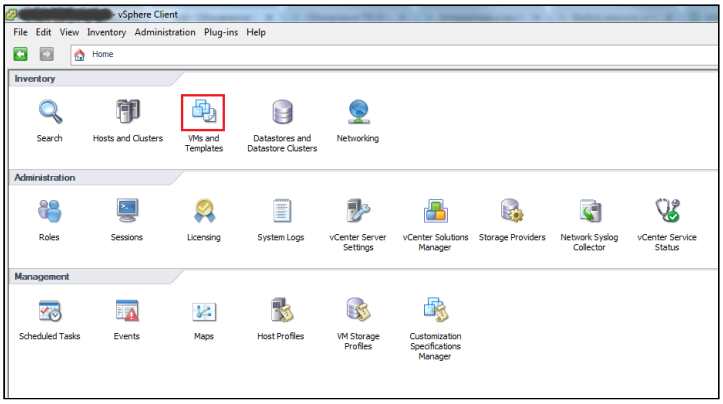
- the System installation type (it can be *All-in-one* or *Distributed installation*) - this information is required to choose the right instruction for the update;
- which DBMS is used (Oracle or PostgreSQL) - this information is required for updating the database schema and server components;
- the 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 actions:

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).

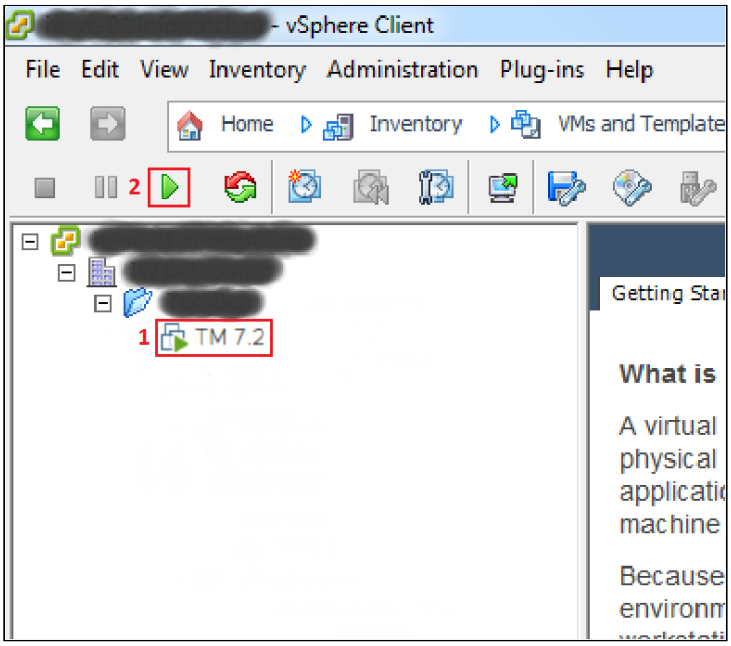
    > **Note:**
    >
    > This instruction contains examples of working with a virtual server in the client application of one of the most common virtualization environments - VMware vSphere (VMware vSphere Client).
    >
    > In frameworks, you can see interface areas that you need to click in the specified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

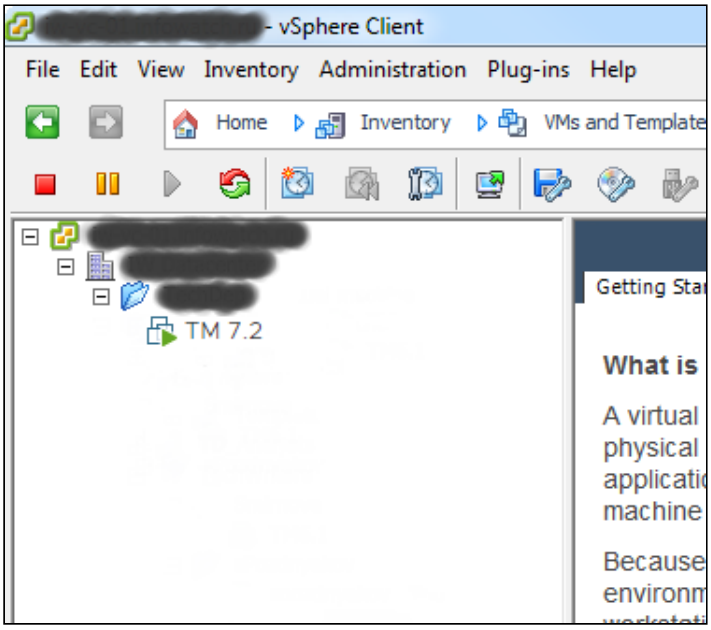


Consistently expand all the nodes on the left side of the workspace until you see the required virtual server.

Turn on the virtual server:



Some time later, 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".

> **Warning!**
>
> Traffic Monitor and the Crawler subsystem are compatible within the same version.
>
> **Example**:
> Crawler version 7.0.2 works with Traffic Monitor 7.0.5, that is they are compatible within version 7.0.x.
> Crawler version 7.0.5 (7.0.x) is not compatible with Traffic Monitor 7.1.0 (7.2.x).
>
> To enable compatibility, update the Crawler subsystem to the corresponding version of Traffic Monitor following the instruction.

> **Note:**
>
> After the System is updated, pre-installed privileges 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 Traffic Monitor to version 7.2, we recommend updating the Device Monitor server first.

The Traffic Monitor installer can work in two modes involving user to update the System:

- text mode in server console;
- graphical mode.

The updating steps and its sequence is similar in both modes.

Silent mode is also available to reduce user's role.

Regardless the selected mode of update, the Management console or server terminal is required to update the System.

During the update all the Traffic Monitor packages will be delivered, but after update is over the installer will start only the services which were not disabled before the update.

Note:

In case the service was disabled, it will **not** be started after updating.

In case the service was stopped, it will be started after updating.

New services statuses will comply with statuses of initial installation.

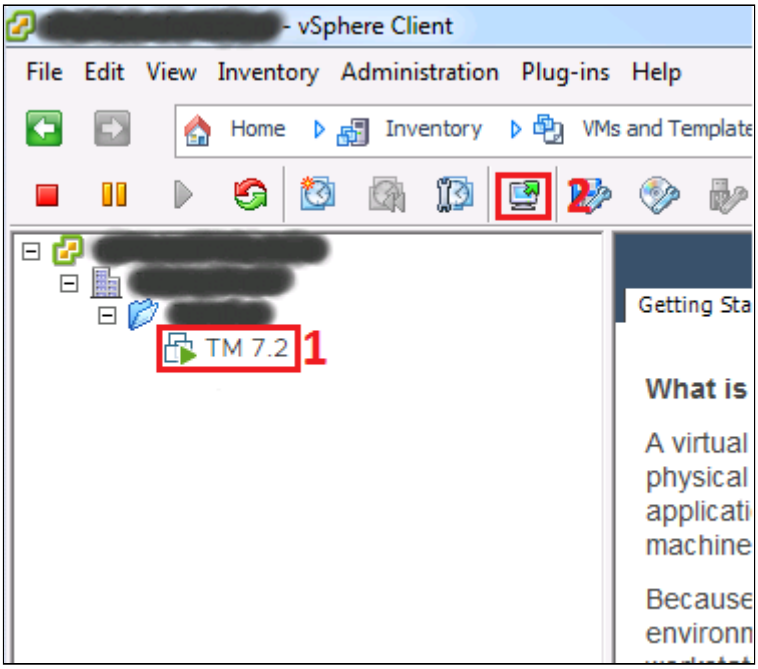
If you want to use the Autolinguist technology, then, after the update, run the following commands on the server where Autolinguist is installed (Web console template):

```
iwtm enable text_autoling
iwtm start text_autoling
```

The packages unpack will start not when the installer will be started, but directly before the updating.

Before updating 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 the **Launch Virtual Machine Console** command (see an example below).

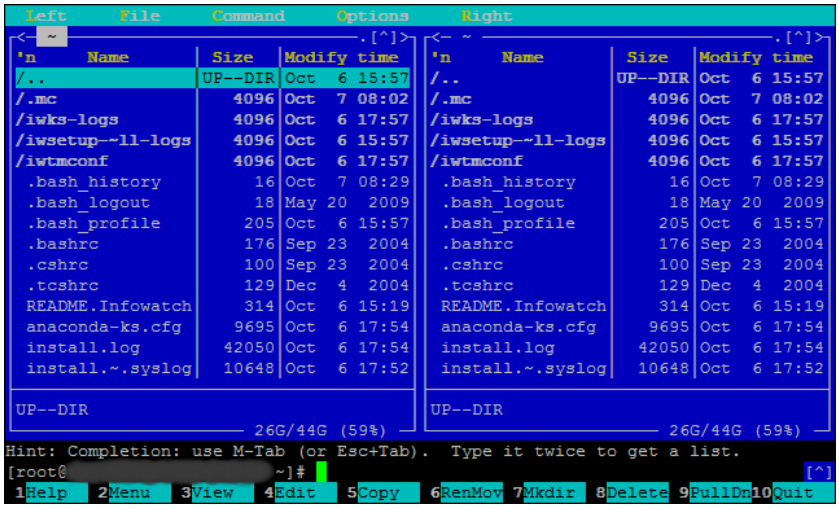


A window with the server console will open.

2. To log into the System, enter login and password (you should enter as a **root** user).

> **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, we recommend using the Screen utility. Thus you can avoid problems in case of a lost connection with the server being updated. 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 the screen again;
> - `screen -r name` - connect to a specific screen with «name»;
> - `exit` - exit screen (to be input within the screen window).

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



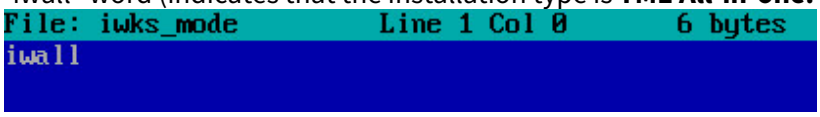
The screen will display a window of *Midnight Commander* file manager where you can view files. You can navigate in the file manager using keyboard arrows and the **Enter** key or with a mouse. Besides, you can enter commands at the command line which is displayed in the lower part of the screen (for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

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

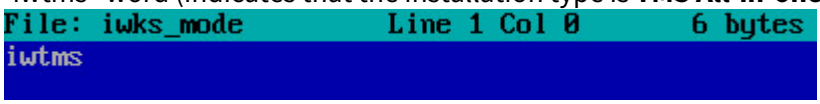


> **Note:**
>
> If **iwks_mode** file is missing in the directory, you need to create it. For this, enter the command:
>
> ```
> touch iwks_mode
> ```

5. 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**.

6. To see the number of Traffic Monitor version go to `/opt/iw/tm5/version`.
   Depending on the Traffic Monitor version that will be updated together with the System, further steps can differ.
7. 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.
>
> After update is complete the parameter of system unit files will be set to default values.

> **Attention!**
>
> In case an error occurs and you need to restore your database and restart the update from the last successfully completed step, we recommend to perform the following actions:
>
> 1. **Database and indexes 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** only (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.

Backup copies should be copied into their **original directories**, and **rights**, **users** and **groups should not be changed**.

a. To stop Traffic Monitor services enter the command:
`service iwtm stop` - for the version 6.10
`iwtm stop` - for the versions starting from 7.0
b. Enter the command:
`service iwtm-php-fpm stop` - for the version 6.10
`systemctl stop iwtm-php-fpm` - for the versions starting from 7.0
c. Perform the backup:
    i. Depending on the database you are using and the version of Traffic Monitor, enter the command to stop the database:
        - for **Oracle DBMS**
            - `service oracle stop` - for Traffic Monitor version 6.10;
            - `systemctl stop oracle` - for Traffic Monitor version starting from 7.0.
        - for **PostgreSQL DBMS**
            - `service postgresql-9.6 stop` - for the version 6.10;
            - `systemctl stop postgresql-9.6` - for the versions starting from 7.0.
    ii. Create your database backup. By default, the database is stored in the directories **`/u01`**, **`/u02`** etc.
    Store the database backup copies either on a separate section of the server or on another server or on an external device.

    Note:

    To specify the directories that contain the database, check the file content:

    - /opt/iw/tm5/csw/oracle/database.conf (for **Oracle DBMS**)
    - /opt/iw/tm5/csw/postgres/database.conf (for **PostgreSQL DBMS**)

    iii. Perform indexes backup. To do this:
        1. Go to the directory `/opt/iw/tm5/etc` and open to view the file **`indexer.conf`**.
        2. In the parameter `"SphinxBaseDir"` you can see the path to the directorty that contains the indexes. In the parameter `"ArchiveDir"` you can see a relative path to indexes archive. The path is specified relating to the content of `"NookDir"` parameter.
        Copy the directories with indexes and indexes archives either on a separate section of the server or on another server or on an external device.
    iv. Create the backup of `iw_adlibitum` service configuration. To do this:
        1. Go to the directory `/opt/iw/tm5/etc` and open the file **`adlibitum. conf`** to view.

2. In the parameter `"ConfigDir"` you can see a relative path to the directory that contains the configuration of `iw_adlibitum` service. The path is specified relating to the content of `"NookDir"` parameter.
   Copy the directory with the configuration either on a separate section of the server or on another server or on an external device.

2. **Backup configuration of the environment**

   You are required to consider the specifics of backing up from the **Warning** note in the previous step. Go to these addresses and copy the files:

   - **For Oracle DBMS:**
     - `/opt/iw/tm5/etc/oracle.conf`
     - `/etc/default/iwtm`
     - `/etc/profile.d/iw-oracle-env.sh`
     - `/etc/logrotate.d/iwtm-oracle-conf-server`
     - `/opt/iw/tm5/etc/oracle.conf`
     - `/opt/iw/tm5/etc/iw-oracle_client.sh`
     - `/opt/iw/tm5/etc/iw-oracle_server.sh`
   - **For PostgreSQL DBMS:**
     - `/etc/default/iwtm`
     - `/etc/profile.d/iw-postgresql-env.sh`
     - `/etc/profile.d/iw-postgresql-client-env.sh`
     - `/etc/sudoers.d/iw-pgagent`
     - `/etc/pgagent/pgagent-9.6.conf`
     - `/opt/iw/tm5/etc/iw-postgresql_server.sh`
     - `/opt/iw/tm5/etc/iw-postgresql_client.sh`
     - `/opt/iw/tm5/etc/iwtm-postgres.conf`
     - `/opt/iw/tm5/etc/postgres.conf`

Depending on the version installed, choose the instruction:

- Updating the System from version 6.10;
- Updating the System from version 7.0 and 7.1.

Warning!

To update the System from version 6.11, you should first update the System to version 7.0 using the corresponding instruction.

- Updating the System with a new installation and data backup (for PostgreSQL DBMS).

Updating the System from version 6.10

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 official instruction.
We strongly recommend backing up the System, cloning it, and updating 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`** (where x.x.x.xxx is a number of build);
      - **`iwtm-postgresql-13.2-x.xx.x.tar.gz`** - if you use PostgreSQL DBMS;
      - **`iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz`** - if you use Oracle DBMS;

   b. ISO-image of a 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 of the System to be updated.

   As per our example:
   - **`iwtm-installer-7.2.0.208-rhel7`**;
   - **`iwtm-postgresql-13.2-7.2.0.tar.gz -`** if you use PostgreSQL DBMS;
   - **`iwtm-oracle-19.0.0.0.0-7.2.0.tar.gz -`** if you use Oracle DBMS;
   - **`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-7.2.0.208-rhel7`

   > **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.

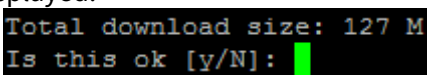
6. To exit the file manager (is required to better control command execution), enter the command:
   `exit`
7. To stop services of the Traffic Monitor server, enter the command:
   `service iwtm stop && chkconfig iwtm off`
8. Depending on DBMS being used, enter the command to stop the DB:
   For **Oracle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

   For **PostgreSQL DBMS**:
   - `service postgresql-9.6 stop && chkconfig postgresql-9.6 off`
9. Enter the command:
   - `service iwtm-php-fpm stop && chkconfig iwtm-php-fpm off`
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. Enter the command to stop the service:
    s`ervice 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 the repository in the guide on Red Hat Enterprise Linux official website.

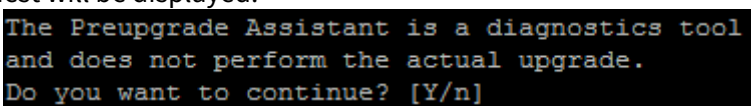
The following request will be displayed:



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.
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 the 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:



    To continue, type **Y** and press **Enter**.
19. Wait until the utility completes the job. The results of the chedk 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.
20. Delete the `dkms` package by running the command:
    `rpm -ev --nodeps dkms`

Warning!

Non-compliance may cause the OS updating error.

21. 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), specifying additional parameter `--cleanup-post`
Our example command:
`redhat-upgrade-tool --iso /root/rhel-server-7.6-x86_64-dvd.iso --cleanup-post`
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 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 restart the server:
`reboot`
The updating continues after the server is rebooted.
23. Wait until the updated System is loaded and log in again. For this, take 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 files .conf and .conf.rpmnew").
Traffic Monitor configuration files located in the `/opt/iw/tm5/etc` directory will be merged automatically when starting the installer.

> **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!

During the update, do not change `web.conf`, `database.conf`, `consul.json` files.

26. 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.
27. Enter the command to go to the directory containing Traffic Monitor distributives:
    `cd /root`

Note:

Before udating the System we recommend starting the DB service in case it was stopped earlier.
Depending on DBMS being used, enter the command to start the DB:
For **Oracle DBMS**:

- `service oracle start`

For **PostgreSQL DBMS**:

- `service postgresql-9.6 start`

28. Automatic merging of Traffic Monitor configuration files of the old and new versions is implemented in the installer. By default, this action is enabled.

Warning!

Automatic merging applies only to Traffic Monitor configuration files with the `.conf` extension that are located in the `/opt/iw/tm5/etc` directory.
Before merging, backup copies for source configuration files are created in the `/opt/iw/tm5/etc_conf_backup_<date_time>` directory. An example of the directory name: `/opt/iw/tm5/etc_conf_backup_11.08.2021_09:26:33`.
After merging, files with the `.rpmnew` extension, which relate to merged configuration files, will be deleted.
All steps will be logged in the `/var/log/infowatch/iwtm-install-<version>-<date>_<time>.log` file. An example of the log file name: `/var/log/iwtm-install-7.2.0.231-2021-08-19_09-56-25.log`.
You can also find information on the merge process in the `/var/log/infowatch/config_merge/` directory.
If during operations with a configuration file, some errors occur, the process is not stopped and other files are merged. Records concerning the errors will be added to the log file.

Start the installer using one of the modes:
Updating in text mode using server console

To update Traffic Monitor using server console, take the following steps:

a. Start the Traffic Monitor installer running the command:
   `./iwtm-installer-x.x.x.xxx-rhel7`
   Our example command:
   `./iwtm-installer-7.2.0.208-rhel7`

Preparations will be made to start the updating. At this stage the unpacking of Traffic Monitor files is not being performed.

Note:

Before starting the installation a warning about wrong owner of files may be displayed.

```
Found wrong owner of files in directory /opt/iw/tm5. The list of files with the wrong owner can be viewed in
 file /tmp/installbuilder_installer.log

Press 'Yes' to automatically fix incorrect file owner.

Press 'No' to abort installation and fix incorrect file owners manually. Also to fix incorrect file owners y
ou can use utility /tmp/iwtm_installer/scripts/check_iwtm.sh
                    [Y/n]:
```

Type **Y** and press **Enter** to change the owner of files and continue running.

Otherwise, you can enter **N** and press **Enter**, then make corrections manually or using `/tmp/iwtm_installer/scripts/check_iwtm.sh` script and start the installer again.

Warning!

If available configured OS repositories are missing, the preparation process will stop with the following error message:

```
[root@spopov-rhel7-713 ~]# ./iwtm-installer-7.2.1.280-rhel7

Preparing installation.../Warning: Failed to prepare installation:
Missing OS repos or unsupported OS. Please mount and/or enable OS packages
repository and try once again.

For details refer to
/var/log/infowatch/install/iwtm-installation_20211007114106.log or
/tmp/installbuilder_installer_11672.log if the first doesn't exist
Press [Enter] to continue:
```

To fix this error press **Enter** to exit, connect the standard RHEL repository, EPEL repository and restart the installer.

For more details on the error refer to the log files, specified in the error message.

After this finished, a welcoming window will be displayed:

```
Welcome to the Traffic Monitor Setup Wizard.

-------------------------------------------------------------------------------
Confirm Infowatch Traffic Monitor Update


InfoWatch Traffic Monitor upgrade from 6.10.12.784 to 7.2.0.208 is available
Database postgresql upgrade from 9 to 13 is available

Would you like to continue?


Note: database upgrade can take a long time and cannot be skipped



 [Y/n]:
```

This will contain all available updates for Traffic Monitor and DBMS.

b. To continue, type **Y** and press **Enter**. To exit the installer type **N** and press **Enter**.

> **Note:**
>
> When updating via server console you can see the default value which is specified in square brackets as a figure or a capital letter next to input field. This value will be used in case of leaving the field empty and pressing **Enter**

c. Confirm the Traffic Monitor services and database were stopped. Steps to confirm the stop and to select a mode will be missed in case the services were stopped manually before starting the installer.

d. Select a mode to stop Traffic Monitor:
   - `Quick stop` - quick stop without events processing;
   - `Waiting for stop` - wait till the current processing of events is finished `;`
   - `Waiting for emptying file queues -` wait till all the events are processed and all the file queues are empty before stopping.

   To make a choice please enter the figure specified next to option selected, and press **Enter**.

   > **Note:**
   >
   > In case `Quick stop` is selected, the stopped services will have `failed` status before the update.

e. If you've selected `Quick stop` or `Waiting for stop`, events can be sent to error queue after Traffic Monitor resumes the work.
   To continue type **Y** and press **Enter**.
   While stopping an events proessing progress will be displayed.

f. After the services are stopped, a message to start the updating and query to continue will be displayed.

```
Setup is now ready to begin upgrading Traffic Monitor on your computer.

Do you want to continue? [Y/n]:
```

To start the updating type **Y** and press **Enter**.
The unpacking of Traffic Monitor updating files will start. Implementation progress will be displayed.

```
Please wait while Setup upgrades Traffic Monitor on your computer.

 >Upgrading
 0% _____________ 50% _____________ 100%
 ########################################
Upgrading Traffic Monitor packages...done
```

The process may take some time.

> **Note:**

If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

g. When updating is successfully completed you can delete the packages created to install the System.
   This data is recommended to delete.
h. Before completeting the update the installer will offer starting the services which were stopped.

> **Warning!**
>
> After update is complete Nagios monitoring system configuration will be changed to default values. In case you've edited Nagios configuration files before the update, its copies will be created in `/etc/infowatch/nagios/iwmon` as `.saved` files. Before starting the Traffic Monitor services move the configuration from `.saved` files to corresponding new configuration files.
>
> After the update to manage the monitoring system use iwtm-nagios service.
>
> For example, to check Nagios status use the command:
>
> ```
> systemctl status iwtm-nagios
> ```

If you do not run the services, to recover the System's efficiency you should run it later manually.

> **Note:**
>
> If Consul service is configured incorrectly, the following warning message will be displayed:
>
> ```
> \Warning: You should run 'iwtm start' command manually after fixing problems with
> Consul.
> Press [Enter] to continue:
> ```
>
> To finish installation press **Enter**.
>
> **For correct work of System check and configure Consul service cluster**
>
> i. Start Consul service with the command:
>   `systemctl start iwtm-consul`
>   To check the service status enter the command:
>   `systemctl status iwtm-consul`
> ii. To check Consul enter the command:
>   1. To display IP address of main server (leader) of cluster:
>   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
>   2. To display information about cluster members:
>   `consul members`
> iii. If the IP address of cluster leader is not displayed, configure cluster of Consul service.
>   After configuration is complete, repeat checking (step ii).

If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

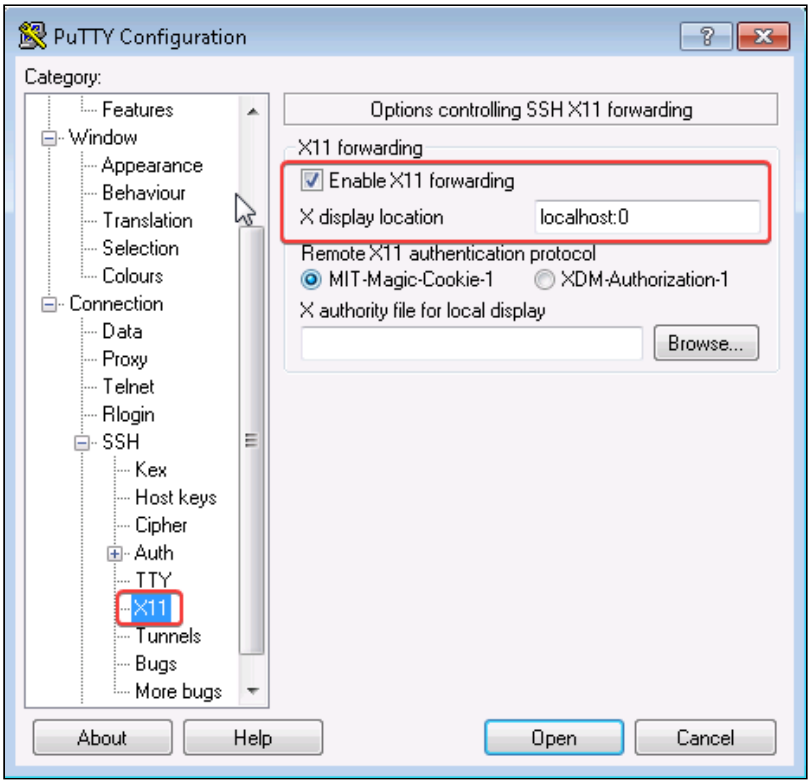
i. Wait till completion of installer opeartion.

Updating in graphical mode

X Window System uses a client - server model. To run the installer in the graphical mode **X11 Forwarding** is used to forward the graphical output of remote system. This let you work directly with Linux graphical applications on the computer which is connected to server. This mode is implemented via SSH connection.

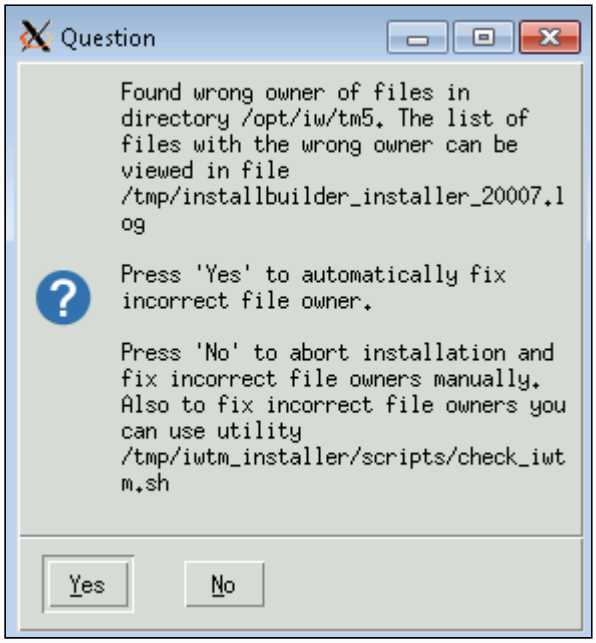
To update Traffic Monitor using graphical mode of installation, take the folowing steps:

a. On the server, where Traffic Monitor components are planned to update:
   i. Install `xauth` utility using the command:
   `yum install xauth`
   ii. In `/etc/ssh/sshd_config` configuration file uncomment the line "`X11Forwarding yes`". To do this, delete `#` placed before the line.
   iii. Save changes in configuration file.
   iv. Restart SSH service using the command:
   `systemctl restart sshd`
b. On the computer, where the graphical mode is to be used:
   i. To connect to Traffic Monitor installation server you will require a SSH client with enabled X11 Forwarding option, e.g. PuTTY.
   ii. To start the installer in the graphical mode you will require an application configured to access to X Window System, for example:
      - Xming application - for OS MS Windows;
      - Gnome 3 shell - for OS Linux.
c. Run the application client which was previously configured to access to X Window System.
d. Connect to server, where Traffic Monitor components are planned to install, using selected SSH client.
   Example of PuTTY configuration window used to connect



e. Run the installer using the command:
`./iwtm-installer-x.x.x.xxx-rhel7`
As per our example:
`./iwtm-installer-7.2.0.208-rhel7`
Preparations will be made to start the installation. At this stage the unpacking of files is not being performed.

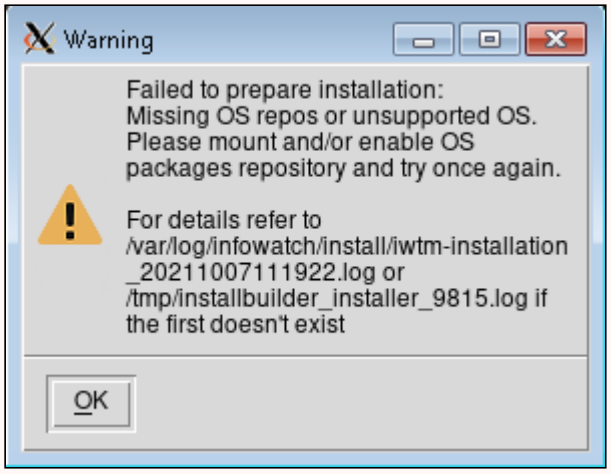
> **Note:**
>
> Before starting the installation a warning about wrong owner of files will be displayed.



Press **Yes** to change the owner of files and continue running.
Otherwise, you can enter **N** and press **Enter**, then make corrections manually or using `/tmp/iwtm_installer/scripts/check_iwtm.sh` script and start the installer again.

Warning!

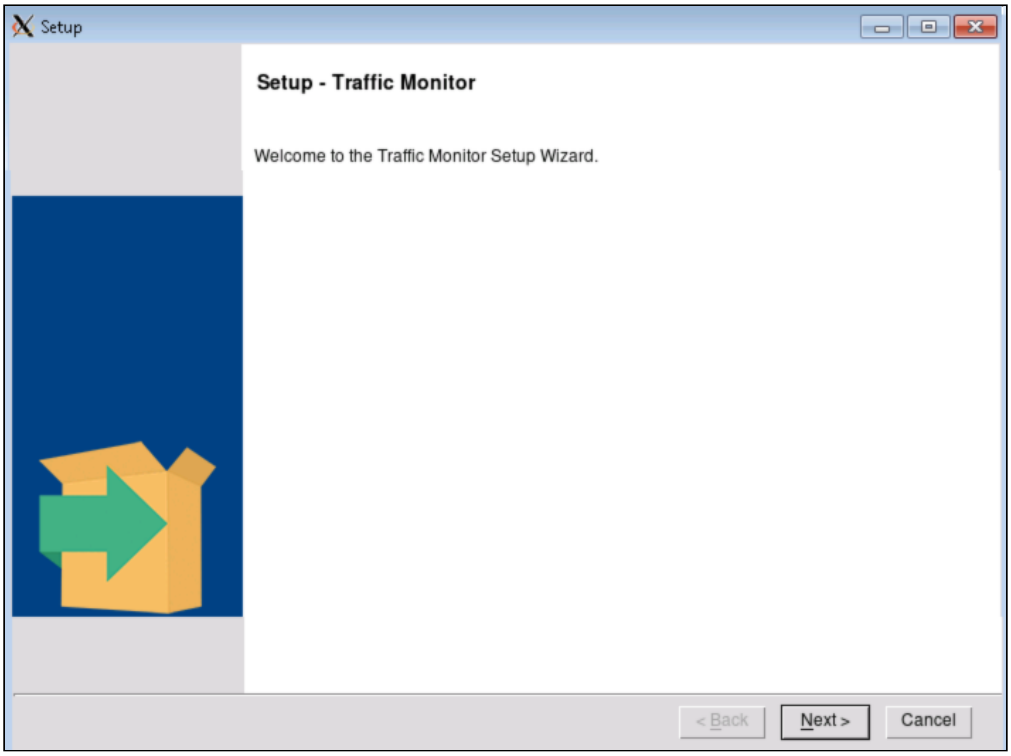
If available configured OS repositories are missing, the preparation process will stop with the following error message:



To fix this error press **OK** to exit, connect the standard RHEL repository, EPEL repository and restart the installer.

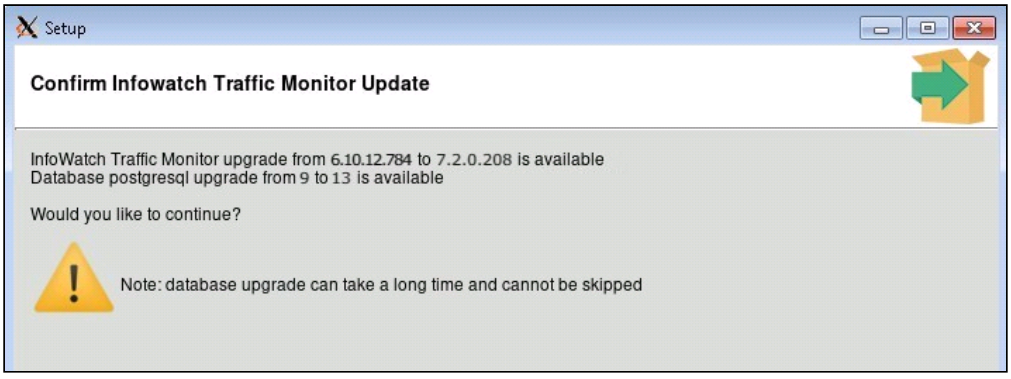
For more details on the error refer to the log files, specified in the error message.

After finishing, a window to install Traffic Monitor will be displayed:



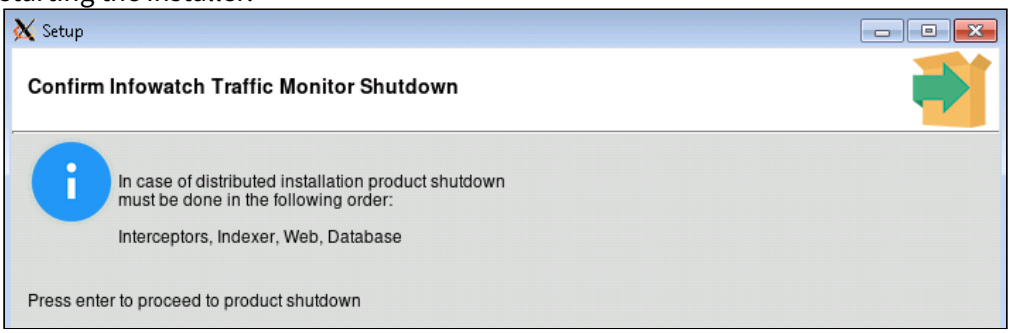
To go to the next parameter press **Next** button, to go back press - **Back**. To exit the installer press **Cancel** button.

f. The next window will contain data related to availabe upgrades for Traffic Monitor and DBMS.

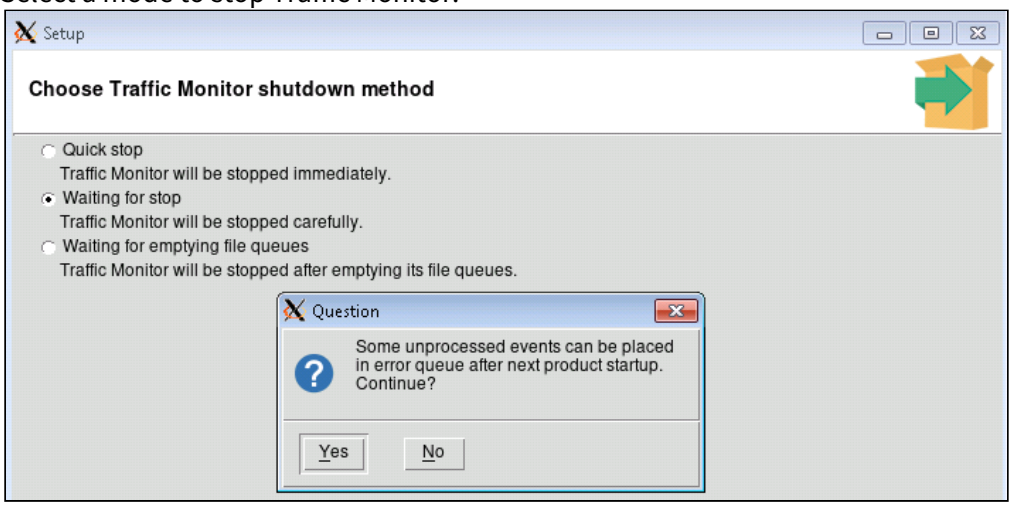


To continue press **Next**.

g. Confirm the Traffic Monitor services and database were stopped. Steps to confirm the stop and to select a mode will be missed in case the services were stopped manually before starting the installer.



h. Select a mode to stop Traffic Monitor:



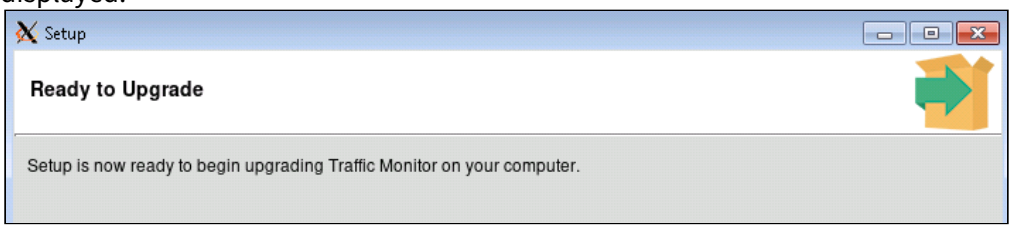
- `Quick stop -` quick stop without events processing;
- `Waiting for stop -` wait till the current processing of events is finished;
- `Waiting for emptying file queues -` wait till all the events are processed and all the file queues are empty before stopping.

  To select click in the checkbox next to required value and press **Next** button.

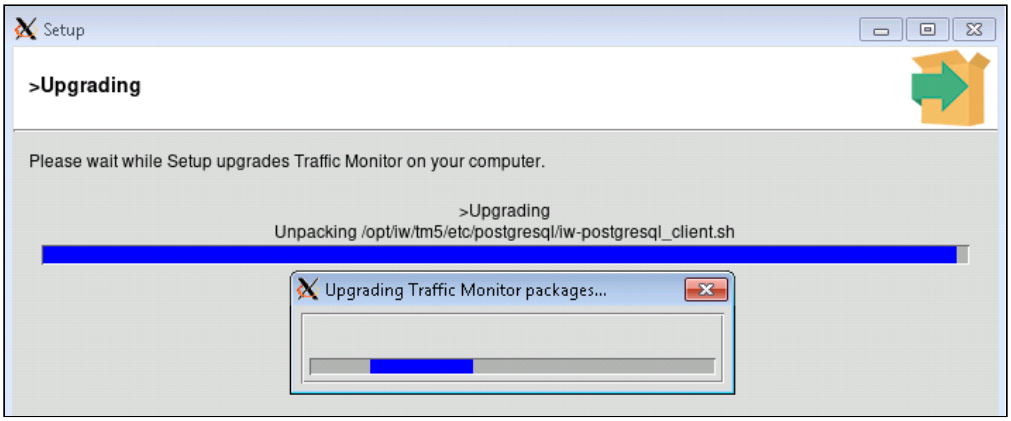
> **Note:**
>
> In case `Quick stop` is selected, the stopped services will have `failed` status before the update.

i. If you've selected `Quick stop` or `Waiting for stop`, events can be sent to error queue after Traffic Monitor resumes the work.
   To continue press **Yes** button.
   While stopping an events proessing progress will be displayed.

j. After the services are stopped, a message to start the updating and query to continue will be displayed.



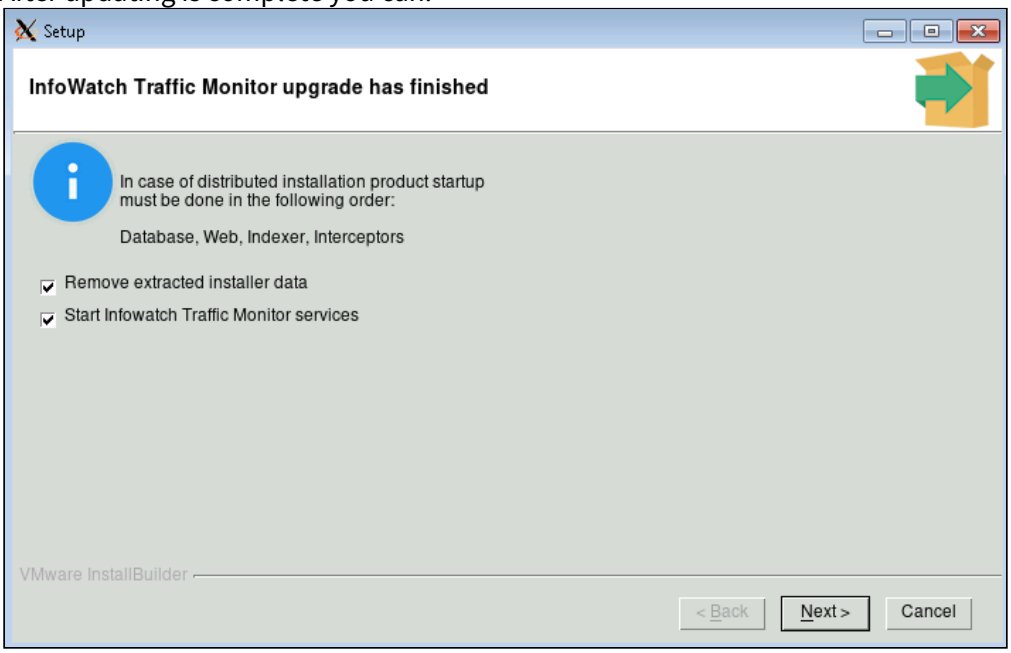
   To start the updating press **Yes** button.
   The unpacking of Traffic Monitor updating files will start. Implementation progress will be displayed.



The process may take some time.

> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

k. After updating is complete you can:



- `Remove exctracted installer data –` when updating is successfully completed you can delete the packages created to install the System. This data is recommended to delete.
- `Remove exctracted installer data –` when updating is successfully completed you can delete the packages created to install the System. This data is recommended to delete.
  To select click in the checkboxes next to required values and press **Next** button.

> **Warning!**

After update is complete Nagios monitoring system configuration will be changed to default values. In case you've edited Nagios configuration files before the update, its copies will be created in `/etc/infowatch/nagios/iwmon` as `.saved` files. Before starting the Traffic Monitor services move the configuration from `.saved` files to corresponding new configuration files.

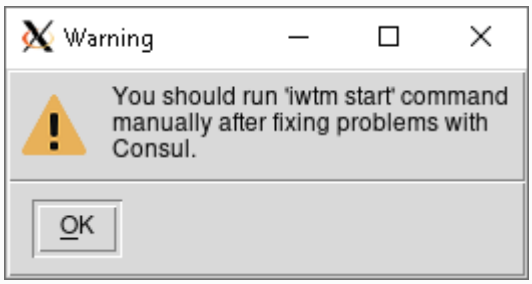
After the update to manage the monitoring system use iwtm-nagios service.

For example, to check Nagios status use the command:

```
systemctl status iwtm-nagios
```

Note:

If Consul service is configured incorrectly, the following warning message will be displayed:



To finish installation press **OK**.

For correct work of System check and configure Consul service cluster

i. Start Consul service with the command:
`systemctl start iwtm-consul`
To check the service status enter the command:
`systemctl status iwtm-consul`

ii. To check Consul enter the command:
   1. To display IP address of main server (leader) of cluster:
   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   2. To display information about cluster members:
   `consul members`

iii. If the IP address of cluster leader is not displayed, configure cluster of Consul service.
After configuration is complete, repeat checking (step ii).

If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

l. To finalise the installation press **Next**.
Wait till completion of installer opeartion.

Updating in silent mode

To reduce a user's role in the System updating process there is a silent mode of installation. In this mode Traffic Monitor can be updated using default parameters.

An options file is realized to be used as a parameter file. In this file you can set required installation parameters. When starting the installation via parameter file, the values specified in this file will be considered the default parameters.

4.1.1 Parameter file (option file)

The file contains the following parameters description:

`<parameter's_name>=<parameter's_value>`

You may leave comments using #.

Parameter file example:

```
# This file is just an example
fix_incorrect_file_owners=1
cleanup_way=clean_fq
start_services_after_upgrade=1
```

The example above contains the parameters as follows:

- change wrong owner of files to correct one;
- before stopping the services wait until all events are processed and the queues are cleared;
- run the services after update.

Warning!

The parameters which are not specified in the file will have the default values. The full list of parameters is specified in the table below.

To use the parameter file go to installer directory and run it using `--optionfile` specifying the file which was previosly created.

Example of using parameter file:

```
./iwtm-installer-7.2.0.208-rhel7 --optionfile /some_directory/option-file-example
```

An alternative way to use: give the parameter file the same name the installer has, but use `.options` extension and copy it to installer directory. In this case the running installer will consider the file parameters the default values.

4.1.2 Silent mode installation

To update the System in silent mode use `--mode unattended` option.

Level of interaction with user is set by `--unattendedmodeui` parameter, which has the following values:

- `none` - no information displayed while updating and no interaction is required;
- `minimal` - status of implementation is displayed while updating, no interaction is required;

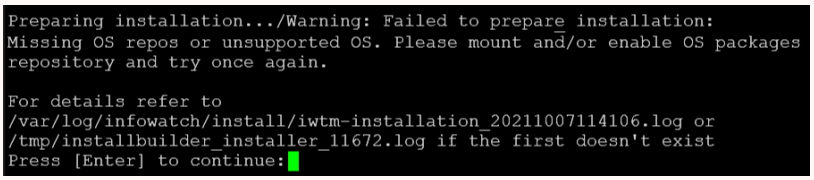
- `minimalWithDialogs` - status of implementation is displayed while updating, pop-up windows can be displayed and interaction with user can be required.

Example of installer running command in silent mode with no user assistance and using parameter file:

```
./iwtm-installer-7.2.0.208-rhel7 --optionfile /some_directory/option-file-example --mode unattended --unattendedmodeui minimal
```

Warning!

If available configured OS repositories are missing, the preparation process will stop with the following error message:



To fix this error press **Enter** to exit, connect the standard RHEL repository, EPEL repository and restart the installer.

For more details on the error refer to the log files, specified in the error message.

Note:

In case the process is over with no errors, the packages created for installation will be removed by installer. If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

Note:

If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

Note:

If Consul service is configured incorrectly, the following warning message will be displayed:



To finish installation press **Enter**.

For correct work of System check and configure Consul service cluster

a. Start Consul service with the command:
`systemctl start iwtm-consul`
To check the service status enter the command:

`systemctl status iwtm-consul`

b. To check Consul enter the command:
   i. To display IP address of main server (leader) of cluster:
   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   ii. To display information about cluster members:
   `consul members`
c. If the IP address of cluster leader is not displayed, configure cluster of Consul service.
   After configuration is complete, repeat checking (step ii).

If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

4.1.3 Full composition of parameter file

The table below contains full list of possible parameters used for update and their default values.

Name	Default value	Valid values	Description	Note
`force_upgrade`	`0`	`0,1`	Forcible switch to updating mode, even if the versions do not match	
`fix_incorrect_file_owners`	`0`	`0,1`	The parameter defines if the wrong owner of files should be changed before the update	If the files to be updated have a wrong owner, the update will be interrupted
`cleanup_way`	`wait_stop`	`quick_stop`, `wait_stop`, `clean_fq`	Select the mode to stop services: • `quick_stop` (no events processing); • `wait_stop` (wait until current events processing is complete);	All events processing and file queues clearing mode (`clean_fq`) is available only when interception components are installed on server. In case this mode was selected but there is a lack of interception components on server, the current events processing mode will be used (`wait_stop`)

Name	Default value	Valid values	Description	Note
			• `clean_fq` - (before stopping wait until all events are processed and the queues are cleared)	
`start services after_upgrade`	`1`	`0,1`	The parameter defines if the installer should run the services after update	After update is complete Nagios monitoring system configuration will be changed to default values. In case you've edited Nagios configuration files before the update, its copies will be created in `/etc/infowatch/nagios/iwmon` as `.saved` files. Before starting the Traffic Monitor services move the configuration from `.saved` files to corresponding new configuration files. After the update to manage the monitoring system use iwtm-nagios service. For example, to check Nagios status use the command: `systemctl status iwtm-nagios`

29. 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").

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

30. Enter the command to call the file manager again:
`mc`
31. Create a backup file for `/opt/iw/tm5/etc/scripts/iwssid.lua`.

32. In this directory rename the file **`iwssid.lua.rpmnew`** to **`iwssid.lua`**.
33. In case **`iwssid.lua`** file was edited before the upgrade, you should relocate the interception configuration from its backup copy to `/opt/iw/tm5/etc/`**`luaengined.conf`** file and the rest customization elements should be relocated to the updated **`iwssid.lua`** file. Otherwise, both files are to be left with no changes.

> **Note:**
>
> All settings for Inline System are relocated to the configuration file `luaengined.conf`.

34. To exit the file manager:
    `exit`
35. If the installer operation was not over before, select the services running and finalise its update. If the installer completed operation with no services run you shoulв run thm manually or reboot the server to start all the services which were stopped.
    A command to reboot the server is as follows:

    `reboot`

> **Warning!**
>
> After the start, Traffic Monitor connects to DB and loads the configuration file `cas_config.xml`. from it. Depending on size of the file, its loading may take some time.
>
> During the loading process, the System may record error messages in log files:
>
> **/opt/iw/tm5/log/cas_config_compiler.log**
>
> **Error record of a type**
>
> ```
> 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
```

When `cas_config.xml` file loading is complete the System will stop recording errors and will operate normally.

If the System keeps recording errors for a long time, check the connection to the DB.

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

Warning!

Before removal the list of packages to remove will be displayed as well as query to confirm. Check packages for the ones which name is started with " `iwtm-` ". In case such kind of packages are found, **cancel the removal and miss this action**.

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

37. Enter the command to clear cash of packages manager:
`yum clean all`
38. Enter the command to clear cash:
`redis-cli flushall`
39. Enter the command to test processes' start:

```
iwtm status
```

A list of processes and their statuses will be displayed

Note:

If the Crawler subsystem is a part of the 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 All-in-one server is complete. The version of the System 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 the instructions in this section.

Note:

After the DBMS was successfully update you can remove files which belongs to previous versions.

This can be done **only after** the System is completely updated and check is performed.

Before removing the files, please make sure that:

- the services arranged for this System are running and working;
- the Management concole contains no errors at System state section;
- old events are placed to DB. You can check this on Events section, using a query with corresponding date of interception;
- new events are sent to DB.

To remove the files run the following command:

- if you use PostgreSQL DBMS:
  `yum erase postgresql96*`
  `/u01/postgres/tmp/delete_old_cluster.sh`
- if you use Oracle DBMS:
  `su - "oracle" -c "rm -rf ${ORACLE_HOME}.backup"`

Warning!

If you have configured automatic synchronizations with LDAP servers, to guarantee the download of essences after update is completed, you shoulв run the synchronising manually (for more details please see "*Infowatch Traffic Monitor. User guide*",

"Running Synchronization with Server Manually" article).

Note:

To display data correctly via Management console you should delete the cache in the browser you use. This can be done using the browser standard tools.

Updating the System from version 7.0 and 7.1

Warning!

We strongly recommend backing up the System, cloning it, and updating on this particular testing machine.

To upgrade the System, please take the following actions:

1. Copy the following files which are a part of InfoWatch Traffic Monitor distribution kit to `/root` directory:
   - **`iwtm-installer-x.x.x.xxx-rhel7.run`** (where x.x.x.xxx is the build number)
   - **`iwtm-postgresql-13.2-x.xx.x.tar.gz`** - if you use PostgreSQL DBMS;
   - **`iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz -`** if you use Oracle DBMS.

   As per our example:
   - **`iwtm-installer-7.2.0.208-rhel7`**;
   - **`iwtm-postgresql-13.2-7.2.0.tar.gz`** - if you use PostgreSQL DBMS;
   - **`iwtm-oracle-19.0.0.0.0-7.2.0.tar.gz`** - if you use Oracle DBMS.

2. To make the file **`iwtm-installer-x.x.x.xxx-rhel7`** executable, enter the command:
`chmod u+x /root/iwtm-installer-x.x.x.xxx-rhel7`
Our example command:
`chmod u+x /root/iwtm-installer-7.2.0.208-rhel7`

> **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**.

3. Connect external or local Red Hat Enterprise Linux 7 repositories. You can find instructions on how to configure local repository at the Red Hat Enterprise Linux official web page.
4. To update packages, enter:
`yum upgrade`
The following request will be displayed:

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

To continue, type **Y** and then press **Enter**.
5. Enter the command to go to Traffic Monitor distribution kit directory:
`cd /root`

> **Note:**
>
> Before starting the update, you are recommended to start the database service, in case it was stopped before. In accordance with DBMS used please type the command to run:
>
> - `systemctl start oracle` (for **Oracle DBMS**)
> - `systemctl start postgresql-9.6` (for **PostgreSQL DBMS**)

6. Automatic merging of Traffic Monitor configuration files of the old and new versions is implemented in the installer.

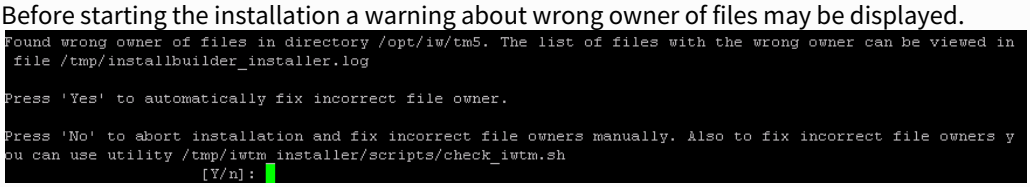
> **Warning!**
>
> Automatic merging applies only to Traffic Monitor configuration files with the **`.conf`** extension that are located in the `/opt/iw/tm5/etc` directory.
> Before merging, backup copies for source configuration files are created in the `/opt/iw/tm5/etc_conf_backup_<date_time>` directory. An example of the directory name: `/opt/iw/tm5/etc_conf_backup_11.12.2020_09:26:33`.
> After merging, files with the **`.rpmnew`** extension, which relate to merged configuration files, will be deleted.
> All steps will be logged in the `/var/log/infowatch/iwtm-install-<version>-<date>_<time>.log` file. An example of the log file name: `/var/log/iwtm-install-7.1.0.231-2020-11-19_09-56-25.log`.
> You can also find information on the merge process in the `/var/log/infowatch/`

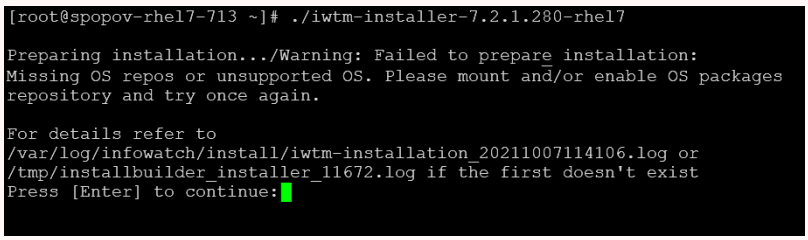
`config_merge/` directory.
If during operations with a configuration file, some errors occur, the process is not stopped and other files are merged. Records concerning the errors will be added to the log file

Run the installer using one of the modes:
Updating in text mode using server console

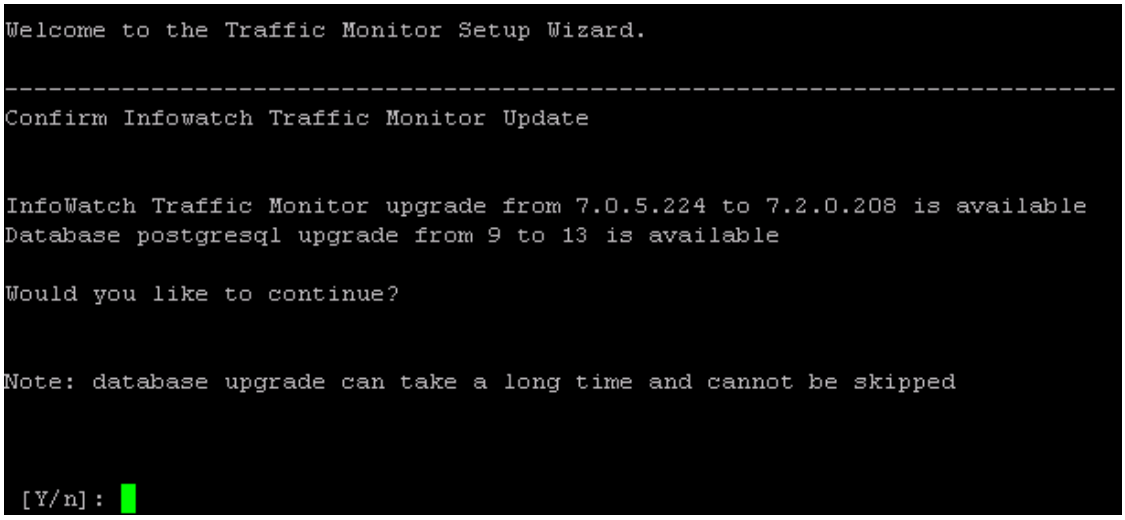
To update Traffic Monitor using server console, take the following steps:

a. Start the Traffic Monitor installer running the command:
`./iwtm-installer-x.x.x.xxx-rhel7`
Our example command:
`./iwtm-installer-7.2.0.208-rhel7`
Preparations will be made to start the updating. At this stage the unpacking of Traffic Monitor files is not being performed.

> **Note:**
>
> Before starting the installation a warning about wrong owner of files may be displayed.
>
> 
>
>
> Type **Y** and press **Enter** to change the owner of files and continue running.
>
> Otherwise, you can enter **N** and press **Enter**, then make corrections manually or using `/tmp/iwtm_installer/scripts/check_iwtm.sh` script and start the installer again.

> **Warning!**
>
> If available configured OS repositories are missing, the preparation process will stop with the following error message:
>
> 
>
>
> To fix this error press **Enter** to exit, connect the standard RHEL repository, EPEL repository and restart the installer.
>
> For more details on the error refer to the log files, specified in the error message.

After this finished, a welcoming window will be displayed:



It will contain all available updates for Traffic Monitor and DBMS.

b. To continue, type **Y** and press **Enter**. To exit the installer type **N** and press **Enter**.

> **Note:**
>
> When updating via server console you can see the default value which is specified in square brackets as a figure or a capital letter next to input field. This value will be used in case of leaving the field empty and pressing **Enter**

c. Confirm the Traffic Monitor services and database were stopped. Steps to confirm the stop and to select a mode will be missed in case the services were stopped manually before starting the installer.

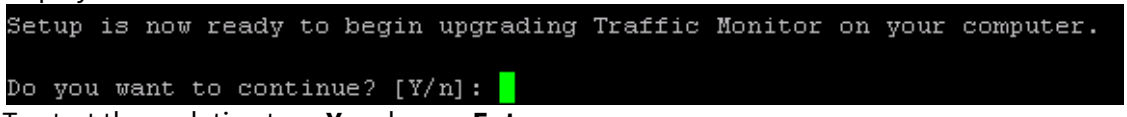
d. Select a mode to stop Traffic Monitor:
   - `Quick stop -` quick stop without events processing;
   - `Waiting for stop -` wait till the current processing of events is finished `;`
   - `Waiting for emptying file queues -` wait till all the events are processed and all the file queues are empty before stopping.

   To make a choice please enter the figure specified next to option selected, and press **Enter**.

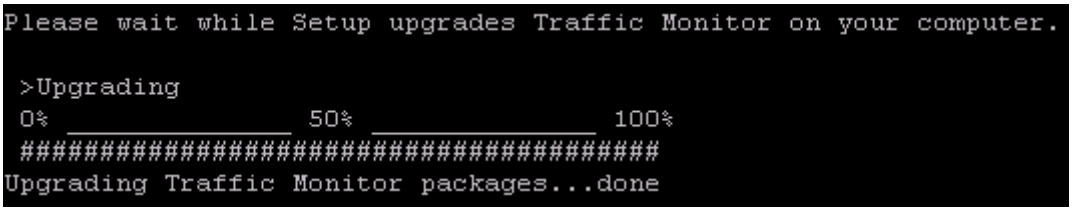
> In case `Quick stop` is selected, the stopped services will have `failed` status before the update.

e. If you've selected `Quick stop` or `Waiting for stop`, events can be sent to error queue after Traffic Monitor resumes the work.
   To continue type **Y** and press **Enter**.
   While stopping an events proessing progress will be displayed.

f. After the services are stopped, a message to start the updating and query to continue will be displayed.



To start the updating type **Y** and press **Enter**.
The unpacking of Traffic Monitor updating files will start. Implementation progress will be displayed.



The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

g. When updating is successfully completed the installer will offer starting the services which were stopped.

> **Warning!**
>
> After update is complete Nagios monitoring system configuration will be changed to default values. In case you've edited Nagios configuration files before the update, its copies will be created in `/etc/infowatch/nagios/iwmon` as `.saved` files. Before starting the Traffic Monitor services move the configuration from `.saved` files to corresponding new configuration files.
>
> After the update to manage the monitoring system use iwtm-nagios service.
> For example, to check Nagios status use the command:
> `systemctl status iwtm-nagios`

If you do not run the services, to recover the System's efficiency you should run it later manually.

> **Note:**
>
> If Consul service is configured incorrectly, the following warning message will be displayed:
>
> 
>
>
> To finish installation press **Enter**.
>
> **For correct work of System check and configure Consul service cluster**
>
> i. Start Consul service with the command:
> `systemctl start iwtm-consul`
> To check the service status enter the command:
> `systemctl status iwtm-consul`
> ii. To check Consul enter the command:
> 1. To display IP address of main server (leader) of cluster:
> `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`

2. To display information about cluster members:
   `consul members`

iii. If the IP address of cluster leader is not displayed, configure cluster of Consul service.
After configuration is complete, repeat checking (step ii).

If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

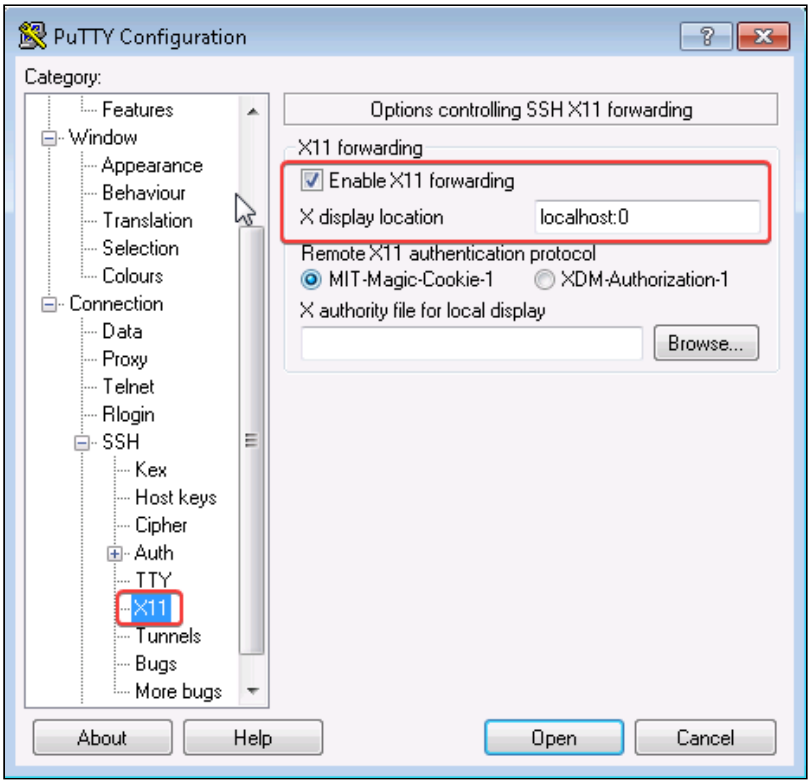
h. Before completeting the update the installer will offer deleting the packages created to update the System.
When update is successfully completed, this data is recommended to delete.
i. Wait till completion of installer opeartion.

Updating in graphical mode

X Window System uses a client - server model. To run the installer in the graphical mode **X11 Forwarding** is used to forward the graphical output of remote system. This let you work directly with Linux graphical applications on the computer which is connected to server. This mode is implemented via SSH connection.

To update Traffic Monitor using graphical mode of installation, take the folowing steps:

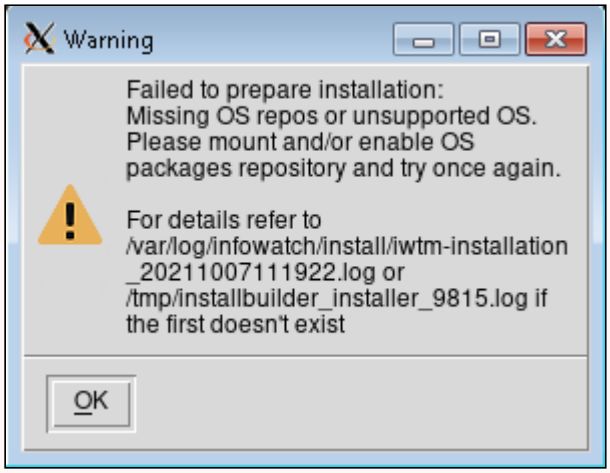
a. On the server, where Traffic Monitor components are planned to update:
   i. Install `xauth` utility using the command:
   `yum install xauth`
   ii. In `/etc/ssh/sshd_config` configuration file uncomment the line "`X11Forwarding yes`". To do this, delete `#` placed before the line.
   iii. Save changes in configuration file.
   iv. Restart SSH service using the command:
   `systemctl restart sshd`
b. On the computer, where the graphical mode is to be used:
   i. To connect to Traffic Monitor installation server you will require a SSH client with enabled X11 Forwarding option, e.g. PuTTY.
   ii. To start the installer in the graphical mode you will require an application configured to access to X Window System, for example:
      - Xming application - for OS MS Windows;
      - Gnome 3 shell - for OS Linux.
c. Run the application client which was previously configured to access to X Window System.
d. Connect to server, where Traffic Monitor components are planned to install, using selected SSH client.
Example of PuTTY configuration window used to connect



e. Run the installer using the command:
`./iwtm-installer-x.x.x.xxx-rhel7`
As per our example:
`./iwtm-installer-7.2.0.208-rhel7`
Preparations will be made to start the installation. At this stage the unpacking of files is not being performed.

> **Note:**
>
> Before starting the installation a warning about wrong owner of files will be displayed.
>
> Press **Yes** to change the owner of files and continue running.
>
> Otherwise, you can enter **N** and press **Enter**, then make corrections manually or using `/tmp/iwtm_installer/scripts/check_iwtm.sh` script and start the installer again.

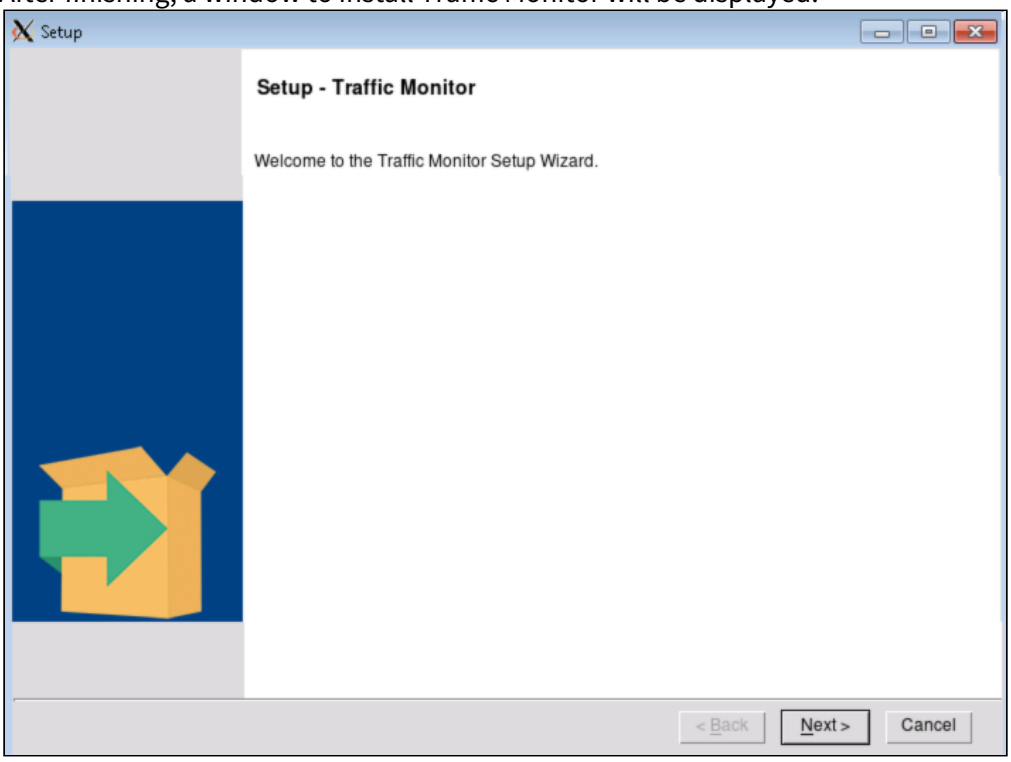
> **Warning!**
>
> If available configured OS repositories are missing, the preparation process will stop with the following error message:



To fix this error press **OK** to exit, connect the standard RHEL repository, EPEL repository and restart the installer.

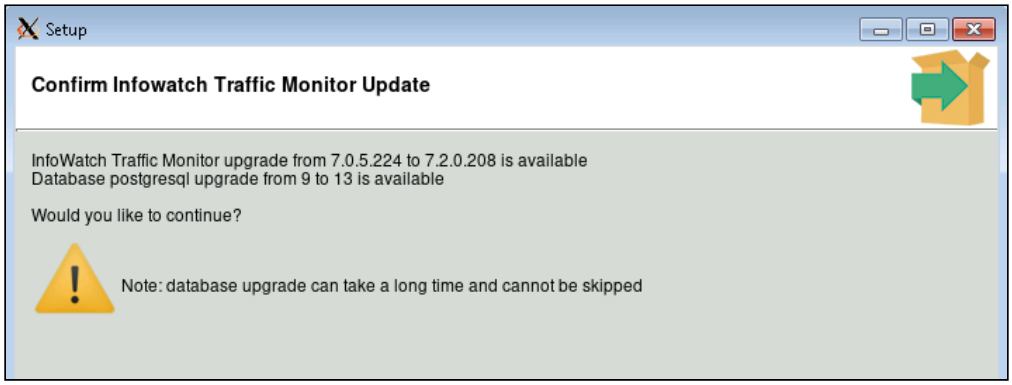
For more details on the error refer to the log files, specified in the error message.

After finishing, a window to install Traffic Monitor will be displayed:



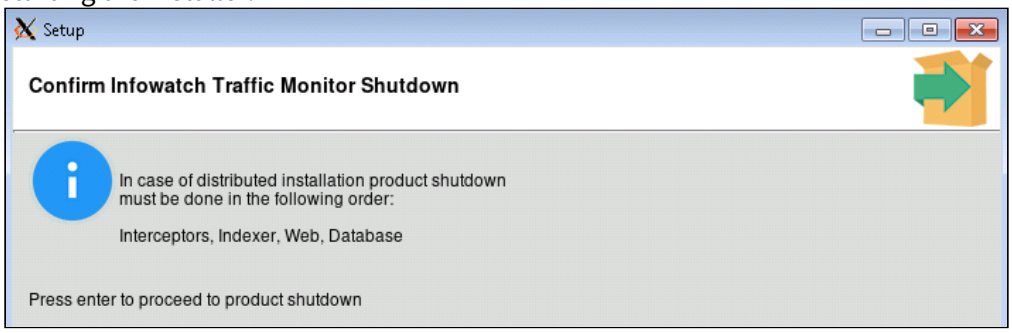
To go to the next parameter press **Next** button, to go back press - **Back**. To exit the installer press **Cancel** button.

f. The next window will contain data related to availabe upgrades for Traffic Monitor and DBMS.

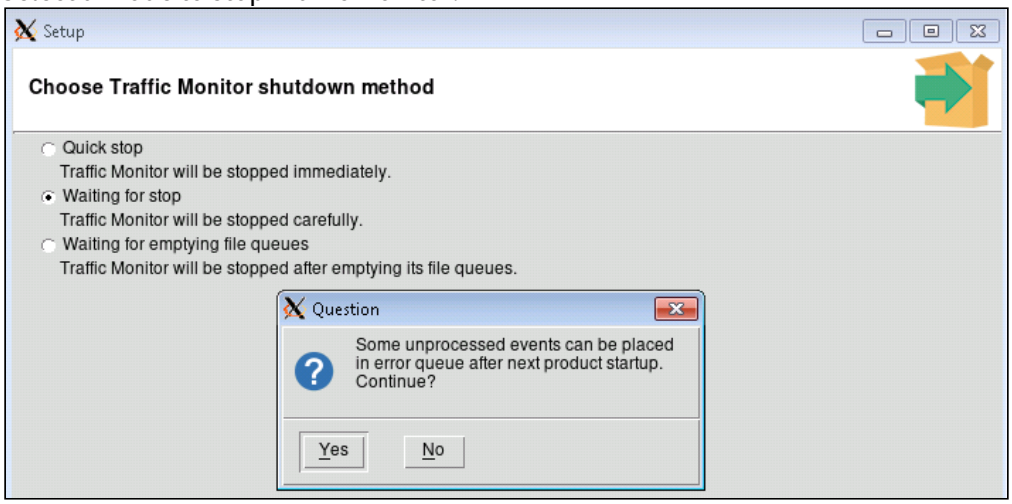


To continue press **Next**.

g. Confirm the Traffic Monitor services and database were stopped. Steps to confirm the stop and to select a mode will be missed in case the services were stopped manually before starting the installer.



h. Select a mode to stop Traffic Monitor:



- `Quick stop –` quick stop without events processing;
- `Waiting for stop –` wait till the current processing of events is finished;
- `Waiting for emptying file queues –` wait till all the events are processed and all the file queues are empty before stopping.

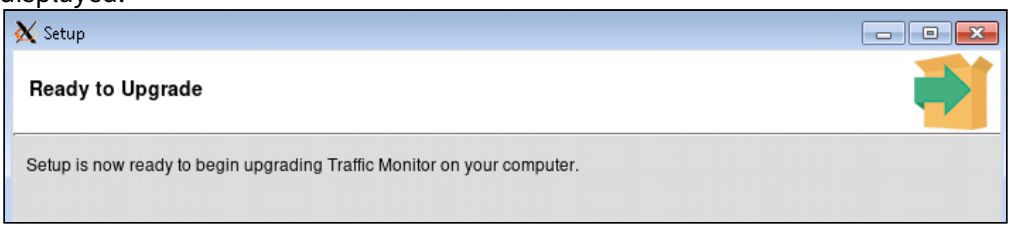
To select click in the checkbox next to required value and press **Next** button.

> **Note:**

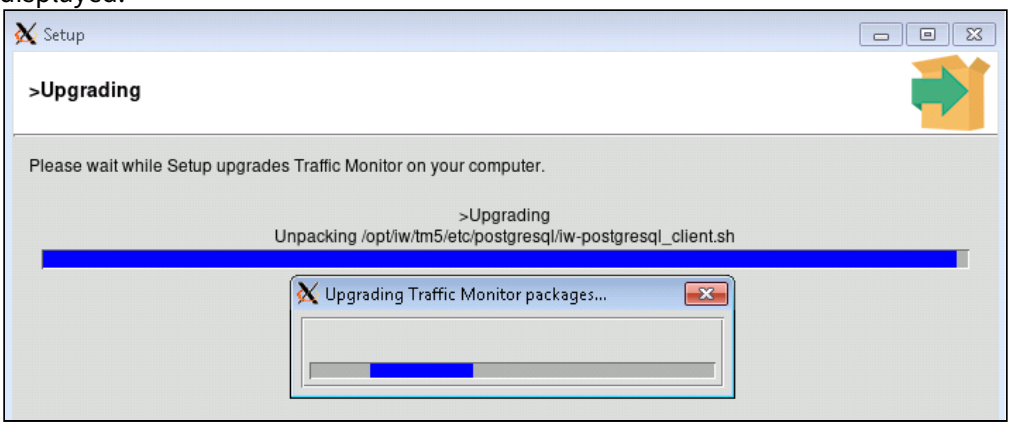
In case `Quick stop` is selected, the stopped services will have `failed` status before the update.

i. If you've selected `Quick stop` or `Waiting for stop`, events can be sent to error queue after Traffic Monitor resumes the work.
To continue press **Yes** button.
While stopping an events proessing progress will be displayed.

j. After the services are stopped, a message to start the updating and query to continue will be displayed.



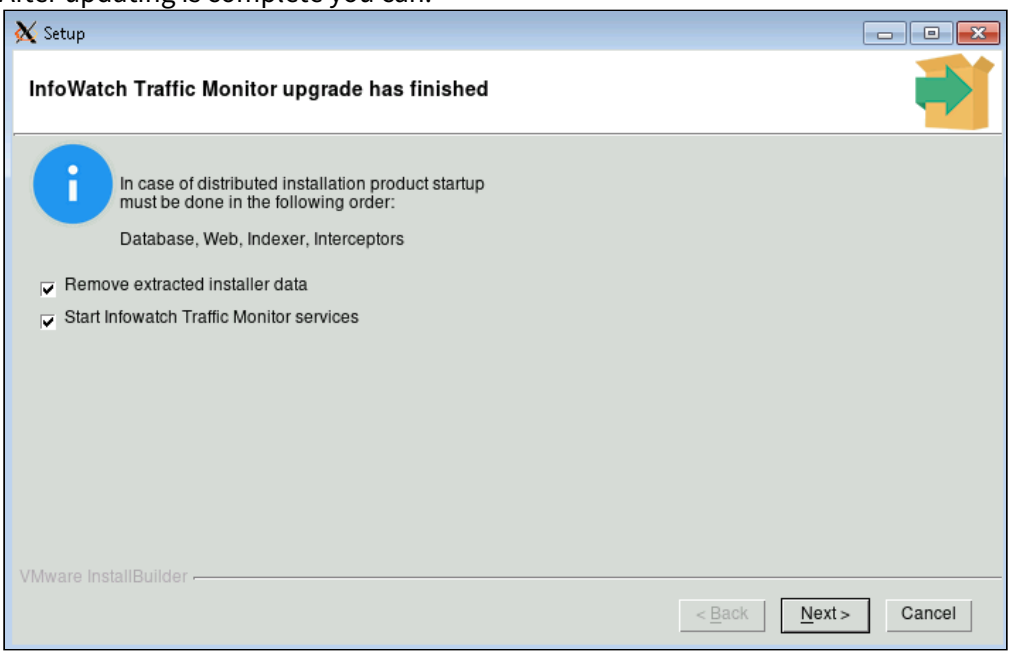
To start the updating press **Yes** button.
The unpacking of Traffic Monitor updating files will start. Implementation progress will be displayed.



The process may take some time.

If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

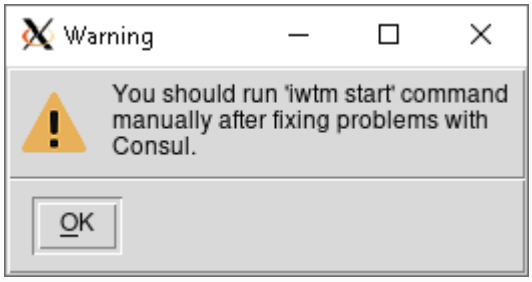
k. After updating is complete you can:



- **`Remove exctracted installer data -`** when updating is successfully completed you can delete the packages created to install the System. This data is recommended to delete.
- **`Remove exctracted installer data -`** when updating is successfully completed you can delete the packages created to install the System. This data is recommended to delete.
  To select click in the checkboxes next to required values and press **Next** button.

> **Warning!**
>
> After update is complete Nagios monitoring system configuration will be changed to default values. In case you've edited Nagios configuration files before the update, its copies will be created in `/etc/infowatch/nagios/iwmon` as `.saved` files. Before starting the Traffic Monitor services move the configuration from `.saved` files to corresponding new configuration files.
>
> After the update to manage the monitoring system use iwtm-nagios service.
>
> For example, to check Nagios status use the command:
>
> ```
> systemctl status iwtm-nagios
> ```

> **Note:**
>
> If Consul service is configured incorrectly, the following warning message will be displayed:



To finish installation press **OK**.

For correct work of System check and configure Consul service cluster

i. Start Consul service with the command:
`systemctl start iwtm-consul`
To check the service status enter the command:
`systemctl status iwtm-consul`

ii. To check Consul enter the command:
    1. To display IP address of main server (leader) of cluster:
    `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
    2. To display information about cluster members:
    `consul members`

iii. If the IP address of cluster leader is not displayed, configure cluster of Consul service.
After configuration is complete, repeat checking (step ii).

If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

l. To finalise the installation press **Next**.
Wait till completion of installer opeartion.

Updating in silent mode

To reduce a user's role in the System updating process there is a silent mode of installation. In this mode Traffic Monitor can be updated using default parameters.

An options file is realized to be used as a parameter file. In this file you can set required installation parameters. When starting the installation via parameter file, the values specified in this file will be considered the default parameters.

4.1.4 Parameter file (option file)

The file contains the following parameters description:

`<parameter's_name>=<parameter's_value>`

You may leave comments using #.

Parameter file example:

```
# This file is just an example
```

```
fix_incorrect_file_owners=1
cleanup_way=clean_fq
start_services_after_upgrade=1
```

The example above contains the parameters as follows:

- change wrong owner of files to correct one;
- before stopping the services wait until all events are processed and the queues are cleared;
- run the services after update.

Warning!

The parameters which are not specified in the file will have the default values. The full list of parameters is specified in the table below.

To use the parameter file go to installer directory and run it using `--optionfile` specifying the file which was previosly created.

Example of using parameter file:

```
./iwtm-installer-7.2.0.208-rhel7 --optionfile /some_directory/option-file-example
```

An alternative way to use: give the parameter file the same name the installer has, but use `.options` extension and copy it to installer directory. In this case the running installer will consider the file parameters the default values.

4.1.5 Silent mode installation

To update the System in silent mode use `--mode unattended` option.

Level of interaction with user is set by `--unattendedmodeui` parameter, which has the following values:

- `none` - no information displayed while updating and no interaction is required;
- `minimal` - status of implementation is displayed while updating, no interaction is required;
- `minimalWithDialogs` - status of implementation is displayed while updating, pop-up windows can be displayed and interaction with user can be required.

Example of installer running command in silent mode with no user assistance and using parameter file:

```
./iwtm-installer-7.2.0.208-rhel7 --optionfile /some_directory/option-file-example --mode
unattended --unattendedmodeui minimal
```

Warning!

If available configured OS repositories are missing, the preparation process will stop with the following error message:

```
[root@spopov-rhel7-713 ~]# ./iwtm-installer-7.2.1.280-rhel7

Preparing installation.../Warning: Failed to prepare installation:
Missing OS repos or unsupported OS. Please mount and/or enable OS packages
repository and try once again.

For details refer to
/var/log/infowatch/install/iwtm-installation_20211007114106.log or
/tmp/installbuilder_installer_11672.log if the first doesn't exist
Press [Enter] to continue:
```

To fix this error press **Enter** to exit, connect the standard RHEL repository, EPEL repository and restart the installer.

For more details on the error refer to the log files specified in the error message.

Note:

In case the process is over with no errors, the packages created for installation will be removed by installer. If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

Note:

If Consul service is configured incorrectly, the following warning message will be displayed:

```
\Warning: You should run 'iwtm start' command manually after fixing problems with
Consul.
Press [Enter] to continue:
```

To finish installation press **Enter**.

a. Start Consul service with the command:
   `systemctl start iwtm-consul`
   To check the service status enter the command:
   `systemctl status iwtm-consul`
b. To check Consul enter the command:
   i. To display IP address of main server (leader) of cluster:
      `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   ii. To display information about cluster members:
      `consul members`
c. If the IP address of cluster leader is not displayed, configure cluster of Consul service.
   After configuration is complete, repeat checking (step ii).

If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

4.1.6 Full composition of parameter file

The table below contains full list of possible parameters used for update and their default values.

Name	Default value	Valid values	Description	Note
`force_upgrade`	`0`	`0,1`	Forcible switch to updating mode, even if the versions do not match	
`fix_incorrect_file_owners`	`0`	`0,1`	The parameter defines if the wrong owner of files should be changed before the update	If the files to be updated have a wrong owner, the update will be interrupted
`cleanup_way`	`wait_stop`	`quick_stop`, `wait_stop`, `clean_fq`	Select the mode to stop services: • `quick_stop` (no events processing); • `wait_stop` (wait until current events processing is complete); • `clean_fq` - (before stopping wait until all events are processed and the queues are cleared)	All events processing and file queues clearing mode (`clean_fq`) is available only when interception components are installed on server. In case this mode was selected but there is a lack of interception components on server, the current events processing mode will be used (`wait_stop`)
`start services after_upgrade`	`1`	`0,1`	The parameter defines if the installer should run the services after update	After update is complete Nagios monitoring system configuration will be changed to default values. In case you've edited Nagios configuration files before the update, its copies will be created in `/etc/infowatch/nagios/iwmon` as `.saved` files. Before starting the Traffic Monitor services move the

Name	Default value	Valid values	Description	Note
				configuration from `.saved` files to corresponding new configuration files. After the update to manage the monitoring system use iwtm-nagios service. For example, to check Nagios status use the command: systemctl status iwtm-nagios

7. 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".

8. Enter the command to call the file manager again:
`mc`
9. Create a backup file for `/opt/iw/tm5/etc/scripts/`**`iwssid.lua`**.
10. In this directory rename the file **`iwssid.lua.rpmnew`** to **`iwssid.lua`**.
11. In case **`iwssid.lua`** file was edited before the upgrade, you should relocate the interception configuration from its backup copy to `/opt/iw/tm5/etc/`**`luaengined.conf`** file and the rest customization elements should be relocated to the updated **`iwssid.lua`** file. Otherwise, both files are to be left with no changes.

> **Note:**
>
> All settings for Inline System are relocated to the configuration file `luaengined.conf`.

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

Warning!

After the start, Traffic Monitor connects to DB and loads the configuration file `cas_config.xml`. from it. Depending on size of the file, its loading may take some time.

During the loading process, 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
```

When `cas_config.xml` file loading is complete the System will stop recording errors and will operate normally.

If the System keeps recording errors for a long time, check the connection to the DB.

14. Enter the command to clear cash of packages manager:
    `yum clean all`
15. Enter the command to clear cash:
    `redis-cli flushall`

16. Enter the command to test processes' start:
`iwtm status`
A list of processes and their statuses will be displayed.

> **Note:**
>
> If the Crawler subsystem is a part of the 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 All-in-one server is complete. The version of the System 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 the instructions in this section.

> **Note:**
>
> After the DBMS was successfully update you can remove files which belongs to previous versions.
>
> This can be done **only after** the System is completely updated and check is performed.
>
> Before removing the files, please make sure that:
>
> - the services arranged for this System are running and working;
> - the Management concole contains no errors at System state section;
> - old events are placed to DB. You can check this on Events section, using a query with corresponding date of interception;
> - new events are sent to DB.
>
> To remove the files run the following command:
>
> - if you use PostgreSQL DBMS:
> `yum erase postgresql96*`
> `/u01/postgres/tmp/delete_old_cluster.sh`
> - if you use Oracle DBMS:
> `su - "oracle" -c "rm -rf ${ORACLE_HOME}.backup"`

> **Warning!**
>
> If you have configured automatic synchronizations with LDAP servers, to guarantee the download of essences after update is completed, you shoulв run the synchronising manually (for more details please see "*Infowatch Traffic Monitor. User guide",*
>
> "Running Synchronization with Server Manually" article).

> **Note:**

To display data correctly via Management console you should delete the cache in the browser you use. This can be done using the browser standard tools.

Updating the System with a new installation and data backup

Warning!

We strongly recommend backup the System and clone it and update on computer used for testing purposes.

If you do not plan to copy data and just mountain disk or data section we do recommend backing it up.

After installing a clear System instance you should configure the configuration files again. Please save it before updating the System again.

Note:

In case you have Crawler, please stop. This procedure is to be completed on the server, where subsystem is installed. Use OS Windows standard options: **Start - Control Panel - Administration Tools - Services**, then highlight the service from the list and click **Stop service**.

1. To stop Traffic Monitor services, enter the command:
   `service iwtm stop` - для версии 6.10
   `iwtm stop` - for the version 7.0 and later
2. Enter the command:
   `service iwtm-php-fpm stop` - для версии 6.10
   `systemctl stop iwtm-php-fpm` - для версии 7.0 и выше
3. Connect to Dtabase and check the number of events contained:
   a. To connect to DB server, enter the commands in console:
      `su - iwtm`
      `psql postgres iwtm -p 5433`
   b. Then enter the command:
      `select count(1) from object;`
   c. To exit enter the commandy:
      `\q`
   d. Enter the command:
      `exit`
4. Make copies of packages frominstalled product version repositories.
   The packages are located in directories as follows `/opt/distr/postgresql/iwtm-postgresql-9.6.19-<version_of_installed_Traffic_Monitor>` и `/opt/iw/distr/<version_of_installed_Traffic_Monitor>` .
   E.g., for Traffic Monitor 7.1.3 directories `/opt/distr/postgresql/iwtm-postgresql-9.6.19-7.1.3` и `/opt/iw/distr/7.1.3.385` .
   Copy the following folders:
   - `postgresql96-libs-9.6.19-1PGDG.rhel7.x86_64.rpm`
   - `postgresql96-9.6.19-1PGDG.rhel7.x86_64.rpm`
   - `postgresql96-server-9.6.19-1PGDG.rhel7.x86_64.rpm`
   - `pg_pathman96-1.5.11-2.el7.iw.x86_64.rpm`
   - `pg_stat_kcache96-2.1.3-1.rhel7.x86_64.rpm`

- `postgresql96-contrib-9.6.19-1PGDG.rhel7.x86_64.rpm`

5. Make DB, indexes, iw_adlibitum service reserve backup.
6. Install new version of Traffic Monitor.

> **Важно!**
>
> In case DB reserve copies are stored on external storages, do not comnnect them while installing the System. You should do this right before restoring and updating the database.
>
> When completing the installation do not remove the packages which were created by installer (section **Remove extracted installer data**).

7. To stop the services enter the commands:
   ```
   iwtm stop
   systemctl stop iwtm-php-fpm
   systemctl stop iwtm-nagios
   ```
8. Enter the command to stop the database:
   ```
   systemctl stop postgresql-13
   ```

> **Note:**
>
> To be able to restore the initial state of installation, copy the directories `u01` and `u02`.

9. To change access rights to the directires enter the commands:
   ```
   chmod 777 /var/log/infowatch/update
   ```
10. Copy reserve DB copy so that it was located the same way it was placed initially.
11. Go to `u01` directory using the command:
    ```
    cd /u01
    ```
12. To change the directory owner use the command:
    ```
    chown -R postgres:postgres postgres
    ```
13. Go to `u02` directory using the command:
    ```
    cd /u02
    ```
14. To change the directories owner use the commands:
    ```
    chown -R postgres:postgres arch
    chown -R postgres:postgres pgdata
    chown -R postgres:postgres pgdata1
    ```
15. Copy the packages from step 4 to directory on server to be updated and go to it.
16. Install the packages using the commands:
    ```
    rpm -i postgresql96-libs-9.6.19-1PGDG.rhel7.x86_64.rpm
    rpm -i postgresql96-9.6.19-1PGDG.rhel7.x86_64.rpm
    rpm -i postgresql96-server-9.6.19-1PGDG.rhel7.x86_64.rpm
    rpm -i pg_pathman96-1.5.11-2.el7.iw.x86_64.rpm
    rpm -i pg_stat_kcache96-2.1.3-1.rhel7.x86_64.rpm
    rpm -i postgresql96-contrib-9.6.19-1PGDG.rhel7.x86_64.rpm
    ```
17. Change the link to configuration file using the command:
    ```
    ln -sf /u01/postgres/iwtm-postgres.conf /opt/iw/tm5/etc/postgresql/iwtm-postgres.conf
    ```
18. Enter the command to go to directory with scripts:
    ```
    /tmp/iwtm_installer/scripts
    ```

19. Being in directory run the DBMS update script using the command of a type:
`./install_postgres.sh --distrib_path=<DBMS_ repository> --tm_version=<версия_нового_Traffic_Monitor> --update`
As per our example:
`./install_postgres.sh --distrib_path=/root --tm_version=7.2.0.208 --update`

> **Note:**
>
> In example above `iwtm-postgresql-13.2-x.xx.x.tar.gz` directory is located in `/root` directory.
> To verify the version of installed Traffic Monitor, enter the command:
> cat /opt/iw/tm5/version

20. After competing successfully the update enter the command to verify the DBMS services status:
`systemctl status postgresql-13`
21. Run the updating script of a type:
`./install_dbschema.sh --tm_version=<new_Traffic_Monitor_version> --db_type=postgres --update`
As per our example:
`./install_dbschema.sh --tm_version=<7.2.0.208 --db_type=postgres --update`
22. Complete the step 3 of current instruction to compare the number of events in DB before and after update.Copy reserve indexes and `iw_adlibitum` service configs so that the location was the same.
In case the initial location wasn't the default location you should specify it in configuration files. (see ciii and civ).
23. Run the commands:
`sudo -u iwtm touch /opt/iw/tm5/www/backend/protected/runtime/first_run`
`iwtm restart kicker`
24. Enyter the command to reboot the server:
`reboot`
Wait until the server is downloaded and authorise again completing steps 1-3 of current instruction before completing the update.
25. Enter the command to clear cache:
`redis-cli flushall`
26. Enetr the command to check the services status:
`iwtm status`
The list of services and its statuses will be displayed.

> **Note:**

При наличии в Системе подсистемы Краулер потребуется запустить службы указанной подсистемы (на сервере Краулер). Данная процедура выполняется на сервере, где установлена подсистема, стандартными средствами ОС Windows: **Пуск** - **Панель управления** - **Администрирование** - **Службы**, затем потребуется выделить службу в списке служб и нажать **Запуск службы**.

In case you have Crawler, you should run the service. This procedure is to be completed on the server, where subsystem is installed. Use OS Windows standard options: **Start - Control Panel - Administration Tools - Services**, then highlight the service from the list and click **Run service**.

Update of Traffic Monitor server All-in-one is compeleted. The new version number can be found in About System window of Traffic Monitor management consoleй. If you havy other servers or subsystems which are to be updated as well, use these instructions to do it. E

Примечание:

To display data correctly via Management console you should delete the cache in the browser you use. This can be done using the browser standard tools.

4.2 Updating TM in case of Distributed Installation

Warning!

Before updating the Traffic Monitor server to version 7.2 it is strongly recommended to update the DM server first.

Traffic Monitor installation kit starting from version 7.2 contains installation templates. Each template - is a set of components to be activated after the System is deployed. For more details please see "System Deployment Schemes and Installation Types".

There are four templates available to install:

- **Database**;
- **Indexer service**;
- **Web console**;
- **Traffic interceptors**.

Versions before 7.2 contained two types of servers:

- TM server (TME Node Server installation type), which is in accordance to current Web console and Interceptors templates;
- DBMS server (TME DB Server), which is is in accordance to current Database and Indexer templates.

All servers are to be updated, where Traffic Monitor components are installed.

The Traffic Monitor installer can work in two modes involving user to update the System:

- text mode in server console;
- graphical mode.

The updating steps and its sequence is similar in both modes.

Silent mode is also available to reduce user's role.

Regardless the selected mode of update, the Management console or server terminal is required to update the System.

During the update all the Traffic Monitor packages will be delivered, but after update is over the installer will start only the services which were not disabled before the update.

Note:

In case the service was disabled, it will **not** be started after updating.

In case the service was stopped, it will be started after updating.

New services statuses will comply with statuses of initial installation.

If you want to use the Autolinguist technology, then, after the update, run the following commands on the server where Autolinguist is installed (Web console template):

```
iwtm enable text_autoling
iwtm start text_autoling
```

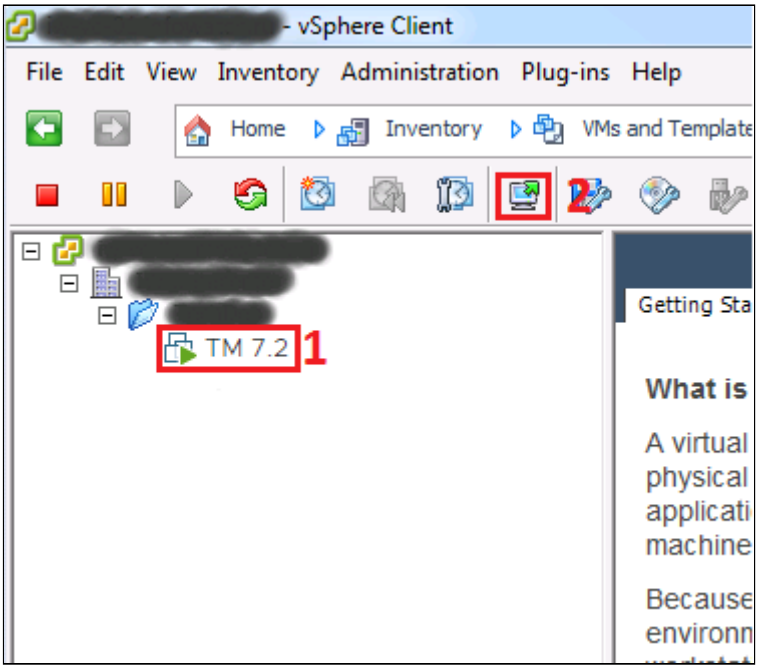
The packages unpack will start not when the installer will be started, but directly before the updating.

Warning!

Each server should have a unique correct FQDN.

Before updating 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 the **Launch Virtual Machine Console** command (see an example below).

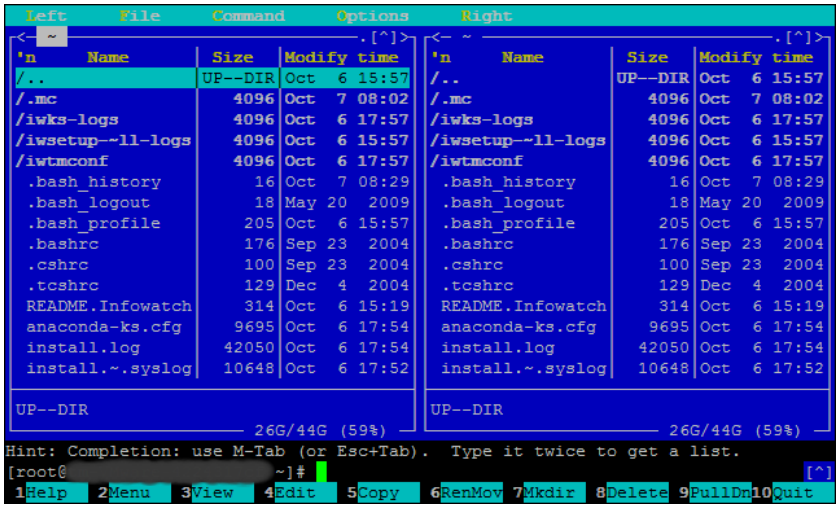


A window with the server console will open.

2. To log into the System, enter login and password (you should enter as a **root** user).

> **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, we recommend using the Screen utility. Thus you can avoid problems in case of a lost connection with the server being updated. 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 the screen again;
> - `screen -r name` - connect to a specific screen with Â«nameÂ»;
> - `exit` - exit screen (to be input within the screen window).

3. 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**.

4. 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`

5. Position the cursor on the **iwks_mode** fine and press **F3**.
Depending on the type of server the content of **iwks_mode** file will be displayed on the screen:
   - " `iwtm` " - indicates that the installation type is **TME Node server**;
   - " `iwdb` " - (indicates that the installation type is **TME DB server**.

Note:

If the file content is different:

1. press **F3** again.
2. press **F4**.
3. in the window that opens, delete all characters and depending on the System edition, 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**.

6. To see the number of Traffic Monitor version go to `/opt/iw/tm5/version`. Depending on the Traffic Monitor version that will be updated together with the System, further steps can differ.
7. 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.

After update is complete the systemd unit file parameters will return to default values.

Attention!

In case an error occurs and you need to restore your database and restart the update from the last successfully completed step, we recommend to perform the following actions:

1. **Database and indexes 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** only (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.

Backup copies should be copied into their **original directories**, and **rights**, **users** and **groups should not be changed**.

a. On TM server:
   i. To stop Traffic Monitor services enter the command:
   `service iwtm stop` - for the version 6.10
   `iwtm stop` - for the versions starting from 7.0
   ii. Enter the command:
   `service iwtm-php-fpm stop` - for the version 6.10
   `systemctl stop iwtm-php-fpm` - for the versions starting from 7.0
   iii. Create the backup of `iw_adlibitum` service. For this:
      1. Go to /opt/iw/tm5/etc and open the file **`adlibitum. conf`** to view.
      2. In "ConfigDir" parameter you can see a relative path to the directory where the configuration of `iw_adlibitum` service is. The path is specified in relation to the content of `"NookDir"` parameter.
      Copy the directory to a separate section of server or to another server or to an external device.

b. On DBMS server:
   i. Enter the command to stop the service `iw_indexer`: `service iwtm stopwait indexer` - for versions starting from 6.10
   `iwtm stop indexer` - for versions starting from 7.0
   ii. Depending on the DBMS you use and the version of Traffic Monitor, enter tha command to stop the database:
      - for **Oracle DBMS**
        - `service oracle stop` - for Traffic Monitor version 6.10;
        - `systemctl stop oracle` - for Traffic Monitor version starting from 7.0.
      - for **PostgreSQL DBMS**
        - `service postgresql-9.6 stop` - for Traffic Monitor version 6.10;
        - `systemctl stop postgresql-9.6` - for Traffic Monitor version starting from 7.0.
   iii. Create your database backup. By default, the database is stored in the directories **`/u01`**, **`/u02`** etc.
   Store the database backup copies either on a separate section of the server or on another server or on an external device.

   Note:

   To specify the directories that contain the database, check the file content:
   - /opt/iw/tm5/csw/oracle/database.conf (for **Oracle DBMS**)
   - /opt/iw/tm5/csw/postgres/database.conf (for **PostgreSQL DBMS**)

   iv. Perform indexes backup. To do this:
      1. Go to the directory `/opt/iw/tm5/etc` and open to view the file **`indexer.conf`**.

2. In the parameter `"SphinxBaseDir"` you can see the path to the directorty that contains the indexes. In the parameter `"ArchiveDir"` you can see a relative path to indexes archive. The path is specified relating to the content of `"NookDir"` parameter.
   Copy the directories with indexes and indexes archives either on a separate section of the server or on another server or on an external device.

2. **Backup configuration of environment**

   You are required to consider the specifics of backing up from the **Warning** note in the previous step. Go to these addresses and copy the files:

   - **For Oracle DBMS:**
     - `/opt/iw/tm5/etc/oracle.conf`
     - `/etc/default/iwtm`
     - `/etc/profile.d/iw-oracle-env.sh`
     - `/etc/logrotate.d/iwtm-oracle-conf-server`
     - `/opt/iw/tm5/etc/oracle.conf`
     - `/opt/iw/tm5/etc/iw-oracle_client.sh`
     - `/opt/iw/tm5/etc/iw-oracle_server.sh`
   - **For PostgreSQL DBMS:**
     - `/etc/default/iwtm`
     - `/etc/profile.d/iw-postgresql-env.sh`
     - `/etc/profile.d/iw-postgresql-client-env.sh`
     - `/etc/sudoers.d/iw-pgagent`
     - `/etc/pgagent/pgagent-9.6.conf`
     - `/opt/iw/tm5/etc/iw-postgresql_server.sh`
     - `/opt/iw/tm5/etc/iw-postgresql_client.sh`
     - `/opt/iw/tm5/etc/iwtm-postgres.conf`
     - `/opt/iw/tm5/etc/postgres.conf`

Depending on the version installed, choose the instruction:

- Updating the System above the version 6.10;
- Updating the System above the version 7.0 and 7.1.

> **Warning!**
>
> To update the System from version 6.11, you should first update the System to version 7.0 using the corresponding instruction.

- System upgrade with clear installation and data backup (for PostgreSQL DBMS).

Updating the System from version 6.10

> **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 official instruction.
We strongly recommend backing up the System, cloning it, and updating 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.

Steps of the update:

Step 1. Upgating all TM servers (TME Node Server)
Step 2. DBMS server update (TME DB Server)
Step 3. Checking Consul cluster
Step 4. Healthcheck 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), take the following steps as per each of them:

1. Copy files into the `/root` directory:
   a. The files from InfoWatch Traffic Monitor distributive:
      - **`iwtm-installer-x.x.x.xxx-rhel7`** (where x.x.x.xxx is a number of build);
      - **`iwtm-postgresql-13.2-x.xx.x.tar.gz`** - if you use PostgreSQL DBMS;
      - **`iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz`** - if you use Oracle DBMS;
   b. ISO-image of a 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 of the System to be updated.

   As per our example:
   - **`iwtm-installer-7.2.0.208-rhel7`** ;
   - **`iwtm-postgresql-13.2-7.2.0.tar.gz -`** if you use PostgreSQL DBMS;
   - **`iwtm-oracle-19.0.0.0.0-7.2.0.tar.gz -`** if you use Oracle DBMS;
   - **`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-7.2.0.208-rhel7`

   > **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. To stop interceptors enter the commands:
   ```
   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 file manager again:
   ```
   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 Traffic Monitor server services, enter the command:
   ```
   service iwtm stop && chkconfig iwtm off
   ```
8. Enter commands to stop services:
   ```
   service iwtm-php-fpm stop && chkconfig iwtm-php-fpm off
   service redis stop && chkconfig redis off
   service nginx stop && chkconfig nginx off
   service gearmand stop && chkconfig gearmand off
   service nagios stop && chkconfig nagios off
   service iwtm-consul stop && chkconfig iwtm-consul off
   ```
9. 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 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**.

10. After packages updating is completed, enter the command to reboot the server:
    `reboot`
    Wait until the server is loaded and log in again.
11. 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.
12. To disconnect repositories run the command:
    `yum-config-manager --disable \*`
13. Enter the command to clear the cash of the package manager:
    `yum clean all`
14. 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/` .

15. To run the utility, used to check 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]
```

    To continue, type **Y** and press **Enter**.
16. Wait until the utility completes the job. The results of the chedk 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.
17. 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.

18. 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), specifying additional parameter `--cleanup-post`
    Our example command:
    `redhat-upgrade-tool --iso /root/rhel-server-7.6-x86_64-dvd.iso --cleanup-post`
    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 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.

19. Enter the command to restart the server:
    `reboot`
    The updating continues after the server is rebooted.
20. Wait until the updated System is loaded and log in again. For this, take steps 1-3 of the instruction before updating.
21. To update the configuration of the Postfix mail server, enter the command:
    `postfix upgrade-configuration`
22. 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 files .conf and .conf.rpmnew").
    Traffic Monitor configuration files located in the `/opt/iw/tm5/etc` directory will be merged automatically when starting the installer.

> **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!

During the update, do not change **web.conf**, **database.conf**, **consul.json** files.

23. 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.
24. Enter the command to go to the directory containing Traffic Monitor distributives:
`cd /root`
25. Automatic merging of Traffic Monitor configuration files of the old and new versions is implemented in the installer. By default, this action is enabled.

Warning!

Automatic merging applies only to Traffic Monitor configuration files with the **.conf** extension that are located in the `/opt/iw/tm5/etc` directory.
Before merging, backup copies for source configuration files are created in the `/opt/iw/tm5/etc_conf_backup_<date_time>` directory. An example of the directory name: `/opt/iw/tm5/etc_conf_backup_11.08.2021_09:26:33`.
After merging, files with the **.rpmnew** extension, which relate to merged configuration files, will be deleted.
All steps will be logged in the `/var/log/infowatch/iwtm-install-<version>-<date>_<time>.log` file. An example of the log file name: `/var/log/iwtm-install-7.2.0.231-2021-08-19_09-56-25.log`.
You can also find information on the merge process in the `/var/log/infowatch/config_merge/` directory.
If during operations with a configuration file, some errors occur, the process is not stopped and other files are merged. Records concerning the errors will be added to the log file.

Start the installer using one of the modes:
Updating in text mode using server console

To update Traffic Monitor using server console, take the following steps:

a. Start the Traffic Monitor installer running the command:

./iwtm-installer-x.x.x.xxx-rhel7

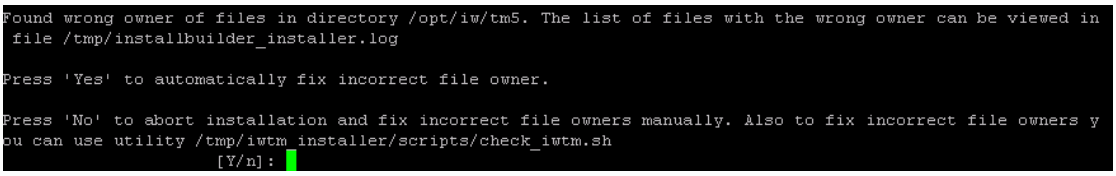
Our example command:

./iwtm-installer-7.2.0.123-rhel7

Preparations will be made to start the updating. At this stage the unpacking of Traffic Monitor files is not being performed.

Note:

Before starting the installation a warning about wrong owner of files may be displayed.

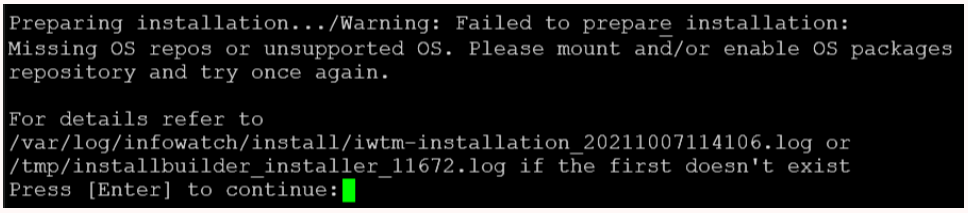


Type **Y** and press **Enter** to change the owner of files and continue running.

Otherwise, you can enter **N** and press **Enter**, then make corrections manually or using `/tmp/iwtm_installer/scripts/check_iwtm.sh` script and start the installer again.

Warning!

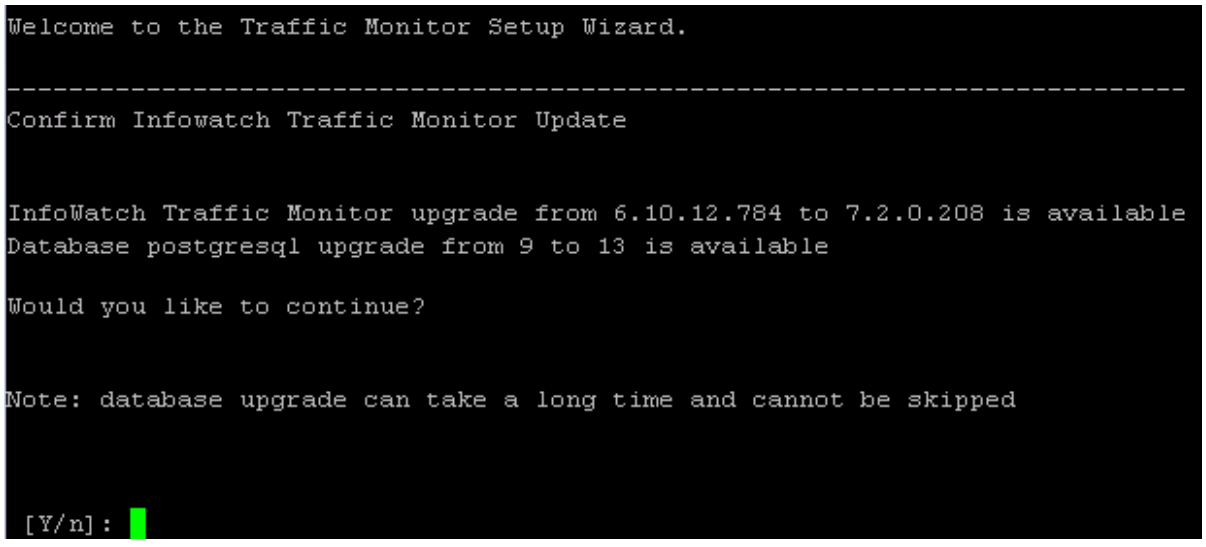
If available configured OS repositories are missing, the preparation process will stop with the following alert box:



To fix this error press **Enter** to dismiss, connect the standard RHEL repository, EPEL repository and restart the installer.

For more details on the error refer to the log files specified in the alert box.

After this finished, a welcoming window will be displayed:



This will contain all available updates for Traffic Monitor and DBMS.

b. To continue, type **Y** and press **Enter**. To exit the installer type **N** and press **Enter**.

> **Note:**
>
> When updating via server console you can see the default value which is specified in square brackets as a figure or a capital letter next to input field. This value will be used in case of leaving the field empty and pressing**Enter**

c. Confirm the Traffic Monitor services and database were stopped. Steps to confirm the stop and to select a mode will be missed in case the services were stopped manually before starting the installer.

> **Note:**
>
> In case all Traffic Monitor components are operating on few servers, they should be stopped in the following order:
>
> i. Interceptors
>
> ii. Indexer
>
> iii. Web console
>
> iv. Database

d. Select a mode to stop Traffic Monitor:

- `Quick stop` - quick stop without events processing;
- `Waiting for stop` - wait till the current processing of events is finished;
- `Waiting for emptying file queues –` wait till all the events are processed and all the file queues are empty before stopping. The mode is available only on servers with interception components.

> **Warning!**
>
> If interception and analysis components (`iw_cas` , `iw_pas`) are used on different servers, interceptors stopping and file queues cleaning can pend. You are recommended using different modes or stop the components manually.

To make a choice please enter the figure specified next to option selected, and press **Enter**.

> **Note:**
>
> In case `Quick stop` is selected, the stopped services will have `failed` status before the update.

e. If you've selected `Quick stop` or `Waiting for stop` , events can be sent to error queue after Traffic Monitor resumes the work.

To continue type **Y** and press **Enter**.
While stopping an events proessing progress will be displayed.
f. After the services are stopped, a message to start the updating and query to continue will be displayed.

```
Setup is now ready to begin upgrading Traffic Monitor on your computer.

Do you want to continue? [Y/n]:
```

To start the updating type **Y** and press **Enter.**
The unpacking of Traffic Monitor updating files will start. Implementation progress will be displayed.

```
Please wait while Setup upgrades Traffic Monitor on your computer.

 >Upgrading
 0% _____________ 50% _____________ 100%
 ########################################
Upgrading Traffic Monitor packages...done
```

The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

g. When updating is successfully completed you can delete the packages created to install the System.
This data is recommended to delete.
h. Before completeting the update the installer will offer starting the services which were stopped.

> **Note:**
>
> If Consul service is configured incorrectly, the following warning message will be displayed:
>
> ```
> \Warning: You should run 'iwtm start' command manually after fixing problems with
> Consul.
> Press [Enter] to continue:
> ```
>
> To finish installation press **Enter**.
>
> If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually after the checking described in step 3 of the instruction.

> **Warning!**
>
> Do not run services before the DBMS server is updated. You can wait and start the services after the server update or continue and update it later manually.

After update is complete Nagios monitoring system configuration will be changed to default values. In case you've edited Nagios configuration files before the update, its copies will be created in `/etc/infowatch/nagios/iwmon` as `.saved` files. Before starting the Traffic Monitor services move the configuration from `.saved` files to corresponding new configuration files.

After the update to manage the monitoring system use iwtm-nagios service.

For example, to check Nagios status use the command:

```
systemctl status iwtm-nagios
```

Updating in graphical mode

X Window System uses a client - server model. To run the installer in the graphical mode **X11 Forwarding** is used to forward the graphical output of remote system. This let you work directly with Linux graphical applications on the computer which is connected to server. This mode is implemented via SSH connection.

To update Traffic Monitor using graphical mode of installation, take the folowing steps:

a. On the server, where Traffic Monitor components are planned to update:

i. Install xauth utility using the command:

yum install xauth

ii. In `/etc/ssh/sshd_config` configuration file uncomment the line "`X11Forwarding yes`". To do this, delete `#` placed before the line.

iii. Save changes in configuration file.

iv. Restart SSH service using the command:

```
systemctl restart sshd
```

b. On the computer, where the graphical mode is to be used:

i. To connect to Traffic Monitor installation server you will require a SSH client with enabled X11 Forwarding option, e.g. PuTTY.

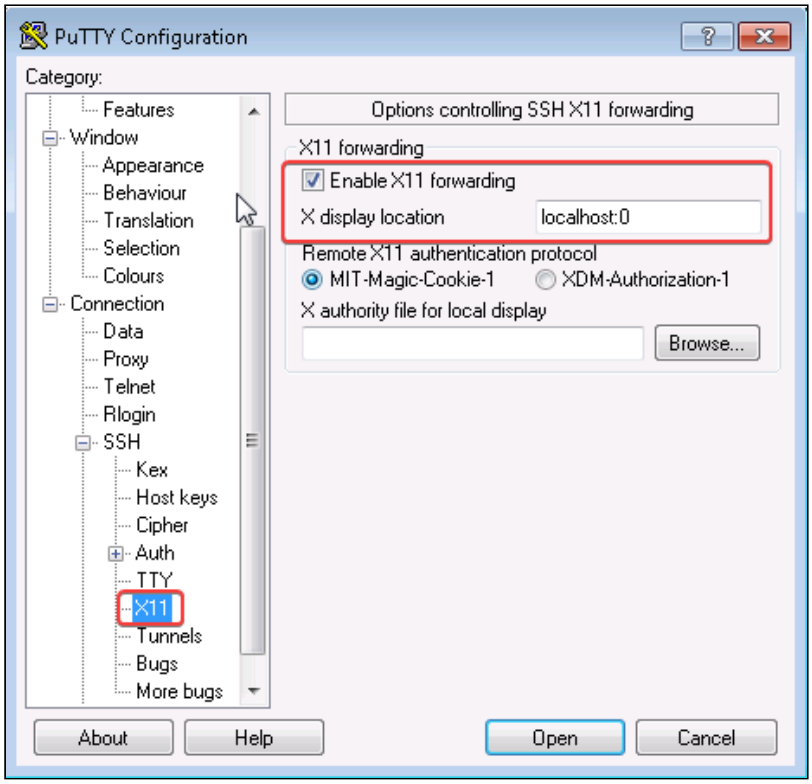
ii. To start the installer in the graphical mode you will require an application configured to access to X Window System, for example:

- Xming application - for OS MS Windows;
- Gnome 3 shell - for OS Linux.

c. Run the application client which was previously configured to access to X Window System.

d. Connect to server, where Traffic Monitor components are planned to install, using selected SSH client.

Example of PuTTY configuration window used to connect



e. Run the installer using the command:

./iwtm-installer-x.x.x.xxx-rhel7

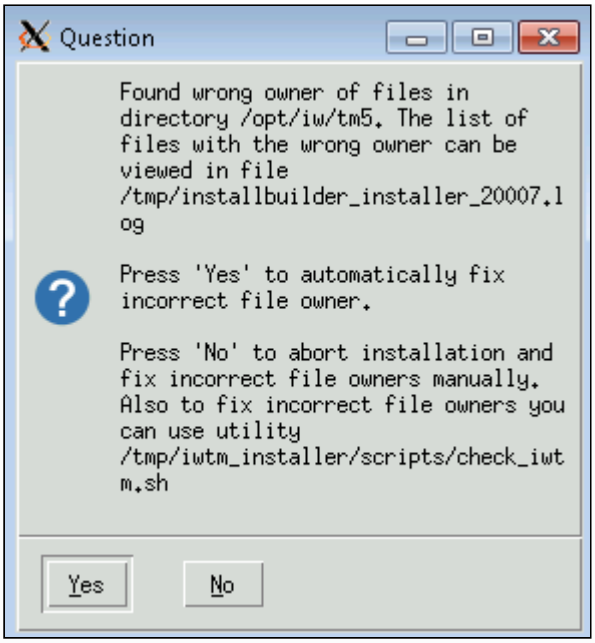
As per our example:

./iwtm-installer-7.2.0.123-rhel7

Preparations will be made to start the installation. At this stage the unpacking of files is not being performed.

Note:

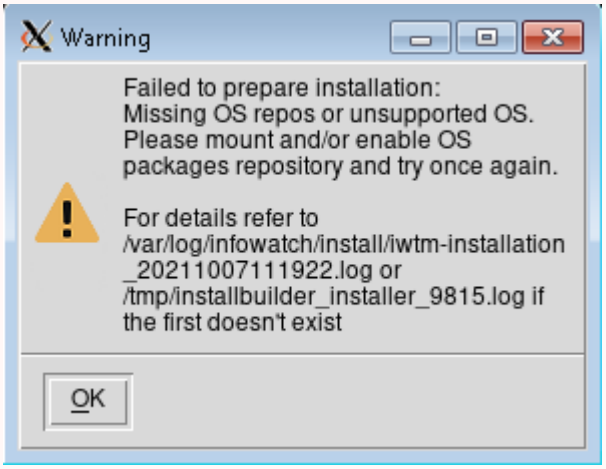
Before starting the installation a warning about wrong owner of files will be displayed.



Press **Yes** to change the owner of files and continue running.
Otherwise, you can enter **N** and press **Enter**, then make corrections manually or using `/tmp/iwtm_installer/scripts/check_iwtm.sh` script and start the installer again.

Warning!

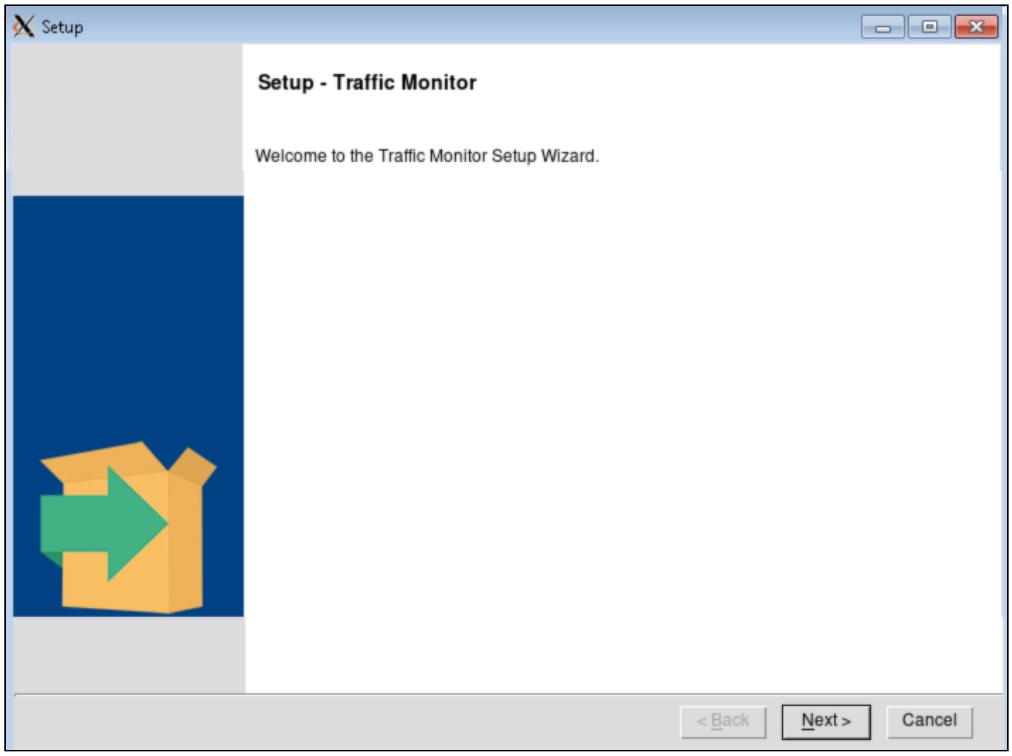
If available configured OS repositories are missing, the preparation process will stop with the following alert box:



To fix this error press **OK** to dismiss, connect the standard RHEL repository, EPEL repository and restart the installer.

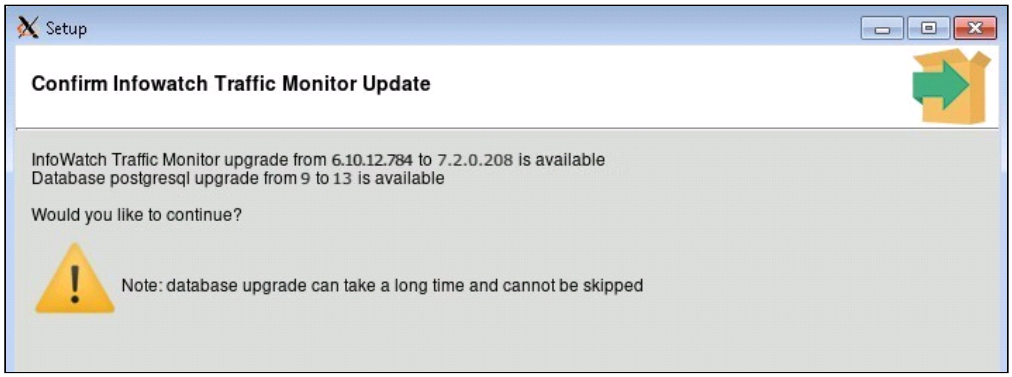
For more details on the error refer to the log files specified in the alert box.

After finishing, a window to install Traffic Monitor will be displayed:



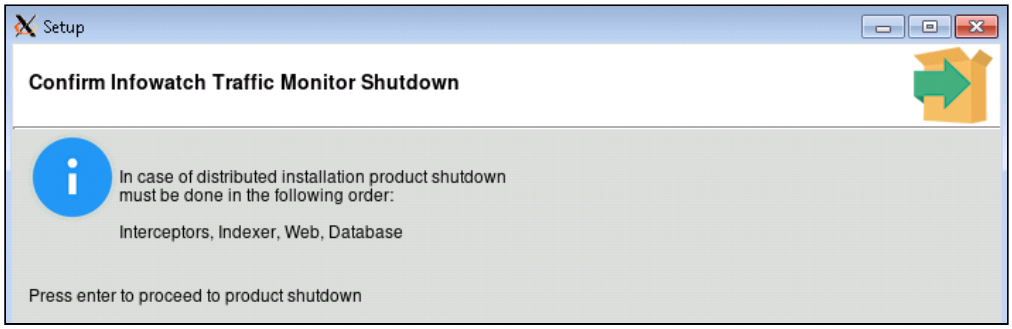
To go to the next parameter press **Next** button, to go back press - **Back**. To exit the installer press **Cancel** button.

f. The next window will contain data related to availabe upgrades for Traffic Monitor and DBMS.



To continue press **Next**.

g. Confirm the Traffic Monitor services and database were stopped. Steps to confirm the stop and to select a mode will be missed in case the services were stopped manually before starting the installer.



Note:

In case all Traffic Monitor components are operating on few servers, they should be stopped in the following order:

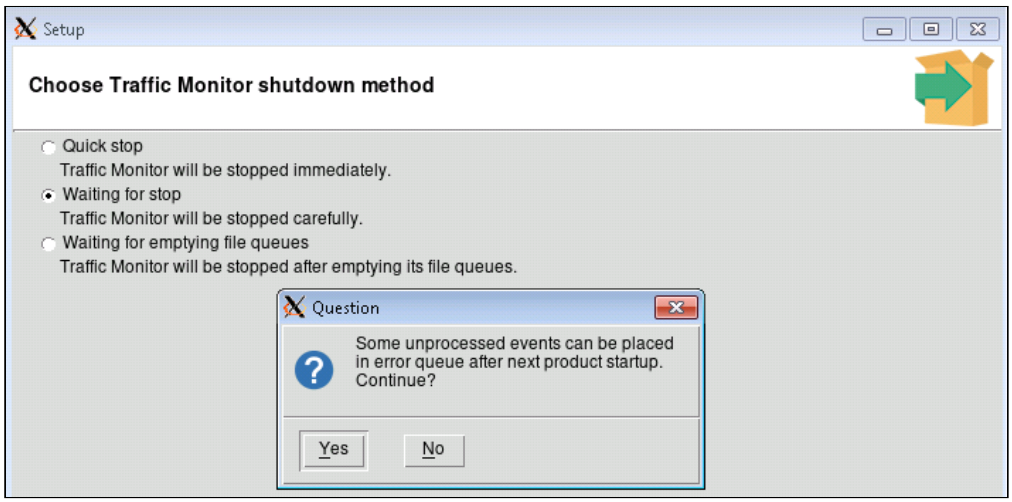
i. Interceptors

ii. Indexer

iii. Web console

iv. Database

h. Select a mode to stop Traffic Monitor:



- `Quick stop –` quick stop without events processing;
- `Waiting for stop –` wait till the current processing of events is finished;
- `Waiting for emptying file queues` - wait till all the events are processed and all the file queues are empty before stopping.

Warning!

If interception and analysis components (`iw_cas` , `iw_pas`) are used on different servers, interceptors stopping and file queues cleaning can pend. You are recommended using different modes or stop the components manually.

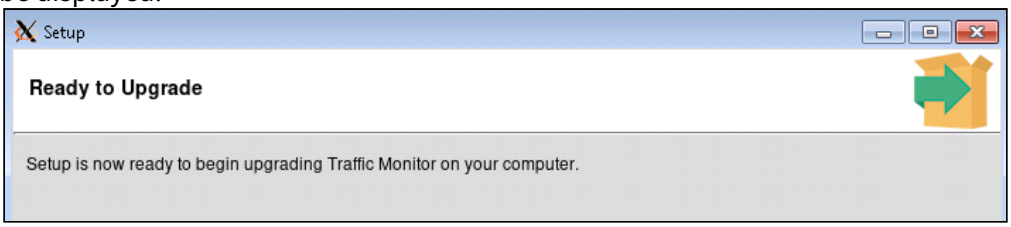
To select click in the checkbox next to required value and press **Next** button.

Note:

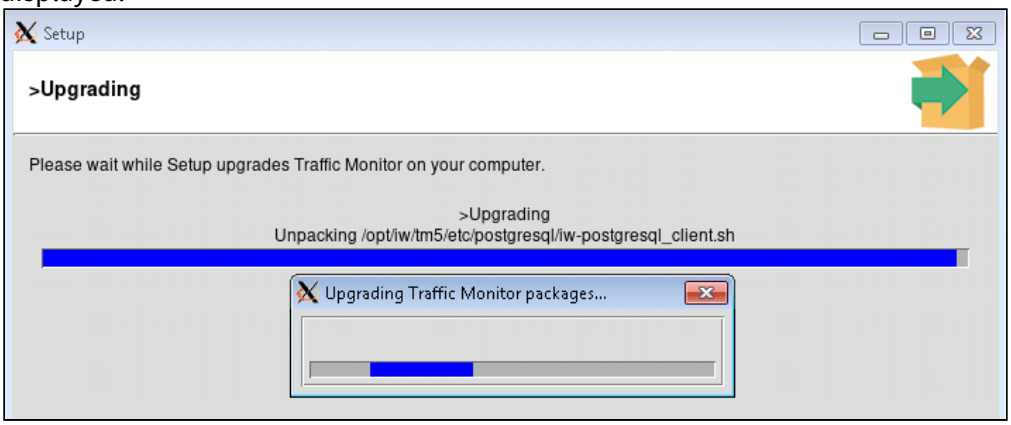
In case `Quick stop` is selected, the stopped services will have `failed` status before the update.

i. If you've selected `Quick stop` or `Waiting for stop` , events can be sent to error queue after Traffic Monitor resumes the work.
To continue press **Yes** button.

While stopping an events proessing progress will be displayed.
j. After the services are stopped, a message to start the updating and query to continue will be displayed.



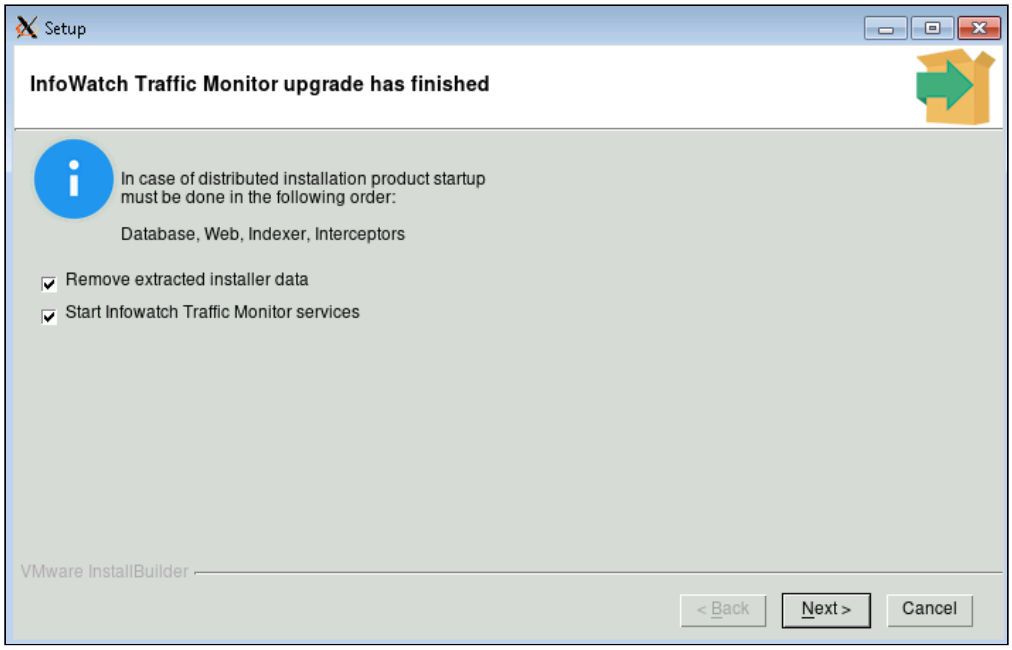
To start the updating press **Yes** button.
The unpacking of Traffic Monitor updating files will start. Implementation progress will be displayed.



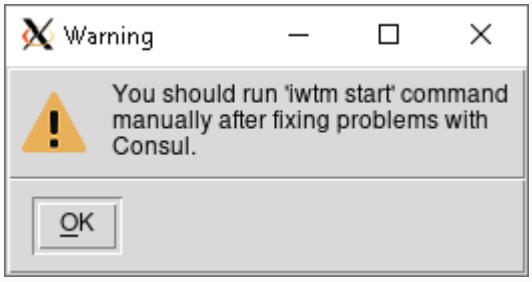
The process may take some time.

> **Note:**
>
> If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

k. After update is complete you can:



- **`Remove exctracted installer data -`** when updating is successfully completed you can delete the packages created to install the System. This data is recommended to delete.
- **`Start Infowatch Traffic Monitor services`** - start the services which were stopped. If you do not run the services, to recover the System's efficiency you should run it later manually.
  To select click in the checkboxes next to required values and press **Next** button.

> **Note:**
>
> If Consul service is configured incorrectly, the following warning message will be displayed:
>
> 
>
>
> To finish installation press **OK**.
>
> If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually after the checking described in step 3 of the instruction.

> **Warning!**
>
> Do not run services before the DBMS server is updated. You can wait and start the services after the server update or continue and update it later manually.

After update is complete Nagios monitoring system configuration will be changed to default values. In case you've edited Nagios configuration files before the update, its copies will be created in `/etc/infowatch/nagios/iwmon` as `.saved` files. Before starting the Traffic Monitor services move the configuration from `.saved` files to corresponding new configuration files.

After the update to manage the monitoring system use iwtm-nagios service.

For example, to check Nagios status use the command:

```
systemctl status iwtm-nagios
```

l. To finalise the installation press **Next** or wait till completion of DBMS server update

Updating in silent mode

To reduce a user's role in the System updating process there is a silent mode of installation. In this mode Traffic Monitor can be updated using default parameters.

An options file is realized to be used as a parameter file. In this file you can set required installation parameters. When starting the installation via parameter file, the values specified in this file will be considered the default parameters.

4.2.1 Parameter file (option file)

The file contains the following parameters description:

`<parameter's_name>=<parameter's_value>`

You may leave comments using #.

Parameter file example:

```
# This file is just an example
fix_incorrect_file_owners=1
cleanup_way=clean_fq
start_services_after_upgrade=1
```

The example above contains the parameters as follows:

- change wrong owner of files to correct one;
- before stopping the services wait until all events are processed and the queues are cleared;
- run the services after update.

Warning!

The parameters which are not specified in the file will have the default values. The full list of parameters is specified in the table below.

To use the parameter file go to installer directory and run it using `--optionfile` specifying the file which was previously created.

Example of using parameter file:

```
./iwtm-installer-7.2.0.208-rhel7 --optionfile /some_directory/option-file-example
```

An alternative way to use: give the parameter file the same name the installer has, but use `.options` extension and copy it to installer directory. In this case the running installer will consider the file parameters the default values.

4.2.2 Silent mode installation

To update the System in silent mode use `--mode unattended` option.

Level of interaction with user is set by `--unattendedmodeui` parameter, which has the following values:

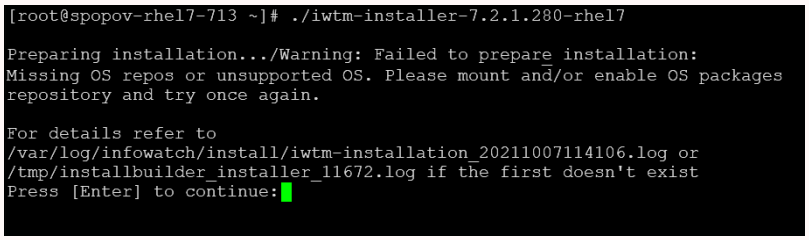
- `none` - no information displayed while updating and no interaction is required;
- `minimal` - status of implementation is displayed while updating, no interaction is required;
- `minimalWithDialogs` - status of implementation is displayed while updating, pop-up windows can be displayed and interaction with user can be required.

Example of installer running command in silent mode with no user assistance and using parameter file:

```
./iwtm-installer-7.2.0.208-rhel7 --optionfile /some_directory/option-file-example --mode unattended --
unattendedmodeui minimal
```

Warning!

If available configured OS repositories are missing the preparation process will stop with the following error message:



To fix this error press **Enter** to exit, connect the standard RHEL repository, EPEL repository and restart the installer.

For more details on the error refer to the log files specified in the error message.

Note:

In case the process is over with no errors, the packages created for installation will be removed by installer. If for any reason the installation process was interrupted, eliminate the cause and restart the installer. The installation will continue from the last step that was successfully completed.

Note:

If Consul service is configured incorrectly, the following warning message will be displayed:

```
\Warning: You should run 'iwtm start' command manually after fixing problems with
Consul.
Press [Enter] to continue:
```

To finish installation press **Enter**.

If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually after the checking described in step 3 of the instruction.

4.2.3 Full composition of parameter file

The table below contains full list of possible parameters used for update and their default values.

Name	Default value	Valid values	Description	Note
`force_upgrade`	`0`	`0,1`	Forcible switch to updating mode, even if the versions do not match	
`fix_incorrect_file_owners`	`0`	`0,1`	The parameter defines if the wrong owner of files should be changed before the update	If the files to be updated have a wrong owner, the update will be interrupted
`cleanup_way`	`wait_stop`	`quick_stop, wait_stop, clean_fq`	Select the mode to stop services: • `quick_stop` (no events processing); • `wait_stop` (wait until current events processing is complete); • `clean_fq` - (before stopping wait until all events are processed and the	All events processing and file queues clearing mode (`clean_fq`) is available only when interception components are installed on server. In case this mode was selected but there is a lack of interception components on server, the current events processing mode will be used (`wait_stop`)

Name	Default value	Valid values	Description	Note
			queues are cleared)	
`start_services_after_upgrade`	`1`	`0,1`	The parameter defines if the installer should run the services after update	After update is complete Nagios monitoring system configuration will be changed to default values. In case you've edited Nagios configuration files before the update, its copies will be created in `/etc/infowatch/nagios/iwmon` as `.saved` files. Before starting the Traffic Monitor services move the configuration from `.saved` files to corresponding new configuration files. After the update to manage the monitoring system use iwtm-nagios service. For example, to check Nagios status use the command: systemctl status iwtm-nagios

- Update server DBMS (TME DB Server) - see description below.

STEP 2. DBMS Server Update (TME DB Server)
To update server DBMS (TME DB Server), do the following:

- Copy to `/root` directory:

a. The following files which are a part of InfoWatch Traffic Monitor distribution kit

- **`iwtm-installer-x.x.x.xxx-rhel7.run`** (where x.x.x.xxx is the build number)
- **`iwtm-postgresql-13.2-x.xx.x.tar.gz`** - if you use PostgreSQL DBMS;
- **`iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz -`** if you use Oracle DBMS.

b. ISO- image of OS Red Hat Enterprise Linux 7.x distribution kit.

> **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.

As per our example:

- **`iwtm-installer-7.2.0.208-rhel7`**;
- **`iwtm-postgresql-13.2-7.2.0.tar.gz`** - if you use PostgreSQL DBMS;
- **`iwtm-oracle-19.0.0.0.0-7.2.0.tar.gz`** - if you use Oracle DBMS;
- **`rhel-server-7.6-x86_64-dvd.iso`**.

- To make the file **`iwtm-installer-x.x.x.xxx-rhel7`** executable, enter the command:
  `chmod u+x /root/iwtm-installer-x.x.x.xxx-rhel7`
  Our example command:
  `chmod u+x /root/iwtm-installer-7.2.0.208-rhel7`
- To stop TM services enter the command:
  `service iwtm stop && chkconfig iwtm off`
- To stop the service enter the command:
  `service iwtm-consul stop && chkconfig iwtm-consul off`
- Depending on DBMS being used, enter the command to stop DB:
  - For **Oracle DBMS**:
    - `service oracle stop && chkconfig oracle off`
  - For **PostgreSQL DBMS**:
    - `service postgresql-9.6 stop && chkconfig postgresql-9.6 off`
- Perform the actions 9-16, 18-24 of Step 1 of this instruction.

> **Note:**
>
> Before starting the installer you are recommended to run DB service in case it was stopped before. Depending on DBMS used input the command to run:
>
> - `service oracle start` (**Oracle DBMS**)
> - `service postgresql-9.6 start` (**PostgreSQL DBMS**)

- Perform the action 25 of Step 1 of this instruction.

> **Warning!**
>
> Do not run the services before the clusters of Consul service were not checked as well as internal services functionalities.

- 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").
- Enter the command to call the file manager again:
  `mc`
- Create a backup file for `/opt/iw/tm5/etc/scripts/`**`iwssid.lua`**.
- In this directory rename the file **`iwssid.lua.rpmnew`** to **`iwssid.lua`**.
- In case **`iwssid.lua`** file was edited before the upgrade, you should relocate the interception configuration from its backup copy to `/opt/iw/tm5/etc/`**`luaengined.conf`** file and the rest customization elements should be relocated to the updated **`iwssid.lua`** file. Otherwise, both files are to be left with no changes.

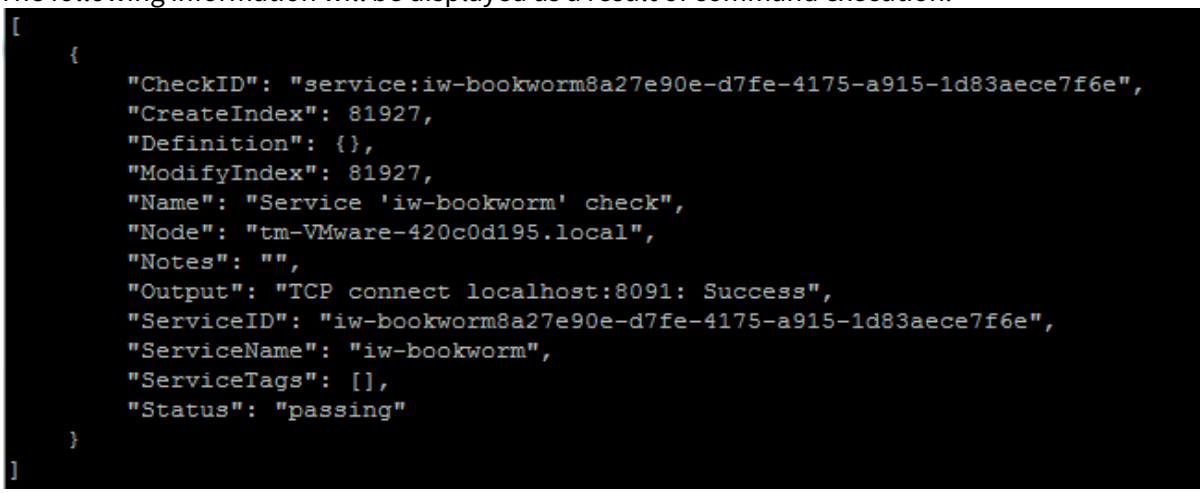
> **Note:**
>
> All settings for Inline System are relocated to the configuration file `luaengined.conf`.

- To exit the file manager:
  `exit`
- 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:
   `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 the 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 the description below.

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

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 the 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 the 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.

Warning!

In case a service has not started successfully, check if there are errors in appropriate log file occured during the update. And contact InfoWatch technical service at support@infowatch.com.

Also, you can check the support section on our site:

www.infowatch.ru/services/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, we recommend checking log files even if the services have been 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 the update of DBMS server (TME DB Server):

1. If the installer operation was not completed before, select the services running and finalise the update.
   In case the installer completed operation with no services started, run them manually or reboot the server to restart all the services.
   Use the following command:
   `reboot`

   Note:

In case all Traffic Monitor components are operating on few servers, they should be stopped in the following order:

i. Database

ii. Web console

iii. Indexer

iv. Interceptors

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`
5. Run all TM servers, the description can be found below.

STEP 6. COMPLETING TM SERVERS UPDATE (TME Node Server)

To complete TM servers update (TME Node Server), the following action are to be taken as per each of the servers:

1. 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").
Traffic Monitor configuration files located in the `/opt/iw/tm5/etc` directory will be merged automatically when starting the installer.

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

2. Again, enter the command to call the file manager:
`mc`
3. Create a backup file for `/opt/iw/tm5/etc/scripts/`**`iwssid.lua`** .
4. In this directory rename the file **`iwssid.lua.rpmnew`** to **`iwssid.lua`** .
5. In case **`iwssid.lua`** file was edited before the upgrade, you should relocate the interception configuration from its backup copy to `/opt/iw/tm5/etc/`**`luaengined.conf`** file and the rest

customization elements should be relocated to the updated **`iwssid.lua`** file. Otherwise, both files are to be left with no changes.

> **Note:**
>
> All settings for Inline System are relocated to the configuration file `luaengined.conf`.

6. To exit the file manager:
   `exit`
7. If the installer operatin was not completed before, select the services running and finalise the update.
   In case the installer completed operation with no services started, run them manually or reboot the server to restart all the services.
   Use the following command:
   `reboot`

> **Warning!**
>
> After Traffic Monitor was started, it 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, the System may record error messages in log files:
>
> - **/opt/iw/tm5/log/cas_config_compiler.log**
>
> **Error record of a type**
>
> ```
> 1 2019-10-07 17:00:57.351489 (3936:0x00007f4008de8880) [ERRORâ€,â€
> ,] : <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**
>
> **Error record of a type**
>
> ```
> 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) [ERRORâ€,â€
> ,] : <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) [ERRORâ€,â€
,] : <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.

8. Enter the command to clear cash on TM server (TME Node Server), that has web-gui package functioning:
   `redis-cli flushall`
9. `Enter the command to delete packages from Red Hat Enterprise Linux 6:`
   `yum remove *.el6*`

Warning!

Before the deletion the list of packages to be removed and a query for removal will be displayed. 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**.

10. Enter the command to clear cash of package manager:
    `yum clean all`
11. Enter the command to check the start of processes:
    `iwtm status`

A list of processes and their statuses will be displayed.

Note:

If the Crawler subsystem is a part of the System, it is required to stop the services of this subsystem (on the 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**.

Updating Traffic Monitor distributed installation type server is complete. The version of the System 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 the instructions in this section.

Note:

After the DBMS was successfully update you can remove files which belongs to previous versions.

This can be done **only after** the System is completely updated and check is performed.

Before removing the files, please make sure that:

- the services arranged for this System are running and working;
- the Management concole contains no errors at System state section;
- old events are placed to DB. You can check this on Events section, using a query with corresponding date of interception;
- new events are sent to DB.

To remove the files run the following commands:

- if you use PostgreSQL DBMS:
  ```
  yum erase postgresql96*
  /u01/postgres/tmp/delete_old_cluster.sh
  ```
- if you use Oracle DBMS:
  ```
  su - "oracle" -c "rm -rf ${ORACLE_HOME}.backup"
  ```

Warning!

If you have configured automatic synchronizations with LDAP servers, to guarantee the download of essences after update is completed, you should run the synchronising manually (for more details please see "*Infowatch Traffic Monitor. User guide",*

"Running Synchronization with Server Manually" article).

Note:

To display data correctly via Management console you should delete the cache in the browser you use. This can be done using the browser standard tools.

4.3 Updating Crawler Subsystem

Important!

To enable compatibility, update the Crawler subsystem to the corresponding version of Traffic Monitor.

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 compatibility in the InfoWatchKnowledge Base article "Compatibility among the versions of TM, DM and Agents".

The 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 7.2:
   >
   > 1. 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.
   > 2. 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 an existing database.
   > 3. If you want to update Device Monitor starting from version 4.0, use the standard procedure.
   > 4. 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 connect to the new Server:
   >
   > - When deleting - save encryption key stored in the DM Server installation folder, `SSLServerKey.pfx` file.
   >
   > - When installing - specify the path to the saved encryption key used on the old Server.

2. Updating InfoWatch Device Monitor Agent.

   > **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

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 the 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

The 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 a built-in DB.

Update Database Under Microsoft SQL Server DBMS

On the **Authentication Method** panel, select the 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 the section "Database deployment under Microsoft SQL Server DBMS".

Update Database Under Oracle DBMS

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

On the **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 the **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.

Important!

If after updating the Device Monitor Server, the `InfoWatch.DeviceMonitor.Server.exe.config` configuration file does not contain parameters for integration with InfoWatch Activity Monitor, take steps described in the KB article.

Note:

After updating the server to version 7.2, the **Status** field of Agent can have one of the following values:

- **Not specified** - if Agent had no connection to the server;
- **Specified** - if Agent established at least one connection to the server.

The actual status of the **Agent Activity** field is set according to the values specified in settings.

When updating to a new version, workstations that already are in the security scheme, are not renamed. A new checking and registration procedure will apply only to computers that will address the server after the update. This procedure checks only the identifier: if it matches, the workstation is renamed, and its old name is only displayed in the DM Management console until the user deletes it

The procedure that was used before checked also the name, which was the reason why the DM Management console could have two records for the same workstation, with its new and old name.

4.4.2 Updating InfoWatch Device Monitor Agent

The system supports Agent versions 6.10, 7.0, 7.1. Therefore, updated system components can work with older Agent versions. However, you can update it to a later version.

Agent's update is similar to its installation:

- local update using Setup Wizard;
- remote update using software distribution tools;
- automatic update (for details, see "*InfoWatch Traffic Monitor. User Guide*", "*Agent Automatic Update*" section);
- 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.

When updating Device Monitor Agent to new version, 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, note that:

If the **Corporate network control** component was installed before, it will be removed during the update. If necessary, you can install the component manually from the command line.

Warning!

Workstation reboot after update to the version 7.2 is required, so the applications started before update can use the new interception mechanism.

4.5 Merging Configuration Files

During the update of Traffic Monitor server configuration 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.

Important!

During the update, do not change the `web.conf`, `database.conf`, `consul.json` files.

You can use any method of file merging type described below.

4.5.1 Automatic merge of Traffic Monitor configuration files

Important!

Automatic merging applies **only** to Traffic Monitor configuration files with the `.conf` extension that are located in the `/opt/iw/tm5/etc` directory.
Before merging, backup copies for source configuration files are created in the `/opt/iw/tm5/etc_conf_backup_<date_time>` directory. An example of the directory name: `/opt/iw/tm5/etc_conf_backup_11.12.2020_09:26:33`.
After merging, files with the `.rpmnew` extension, which relate to merged configuration files, will be deleted.
All steps will be logged in the `/var/log/infowatch/iwtm-install-<version>-<date> <time>.log` file. An example of the log file name: `/var/log/iwtm-install-7.1.0.231-2020-11-19_09-56-25.log`.
You can also find information on the merge process in the `/var/log/infowatch/config_merge/`

directory.
If during operations with a configuration file, some errors occur, the process is not stopped and other files are merged. Records concerning the errors will be added to the log file.

To start the process, you will need the **`iwtm-config-merge-tools-x.x.x.xxx-release.x86_64.rpm`** package, which is a part of the Traffic Monitor distribution kit.

In our example: `iwtm-config-merge-tools-7.1.0.250-release.x86_64.rpm`

Note:

If the `iwtm-config-merge-tools-x.x.x.xxx-release.x86_64.rpm` package is missing, you can find it in packages of the installer: `iwtm-installer-x.x.x.xxx-rhel7.run`.

For this:

1. Go to the directory with the Traffic Monitor distribution kits. In our example: `cd /root`
2. Extract the contents of the installer with the command: `bash ./iwtm-installer-x.x.x.xxx-rhel7.run --target <директория>`
   In our example, the command is as follows: `bash ./iwtm-installer-7.1.0.250-rhel7.run --target /root`
3. To find the required package, use the command: `find / -name "iwtm-config-merge-tools*" -print`

To start automatic merging of Traffic Monitor configuration files:

1. Find out which version of Traffic Monitor is installed. For this, enter the command: `cat /opt/iw/tm5/version`
2. Go to the directory, to which the `iwtm-config-merge-tools-x.x.x.xxx-release.x86_64.rpm` package was copied.
   In our example, the command is as follows: `cd /root`
3. To install the package, run the command: `rpm -i iwtm-config-merge-tools-x.x.x.xxx-release.x86_64.rpm`
   In our example, the command is as follows: `rpm -i iwtm-config-merge-tools-7.1.0.250-release.x86_64.rpm`
4. To run the script, use the command: `/opt/iw/tm5/bin/config/config_merge/scripts/run_merge.sh -cv <current_version> -nv <new_version> -b <directory_for_backup>`
   In our example, the command is as follows: `/opt/iw/tm5/bin/config/config_merge/scripts/run_merge.sh -cv 6.10.10.123 -nv 7.1.0 -b`

   Note:

   If you do not specify a directory for the backup, the `/opt/iw/tm5/` directory is used by default.

Wait until file processing is complete.

Note:

If you receive error messages, fix the errors and the script again or merge configuration files manually.

4.5.2 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"
}
```

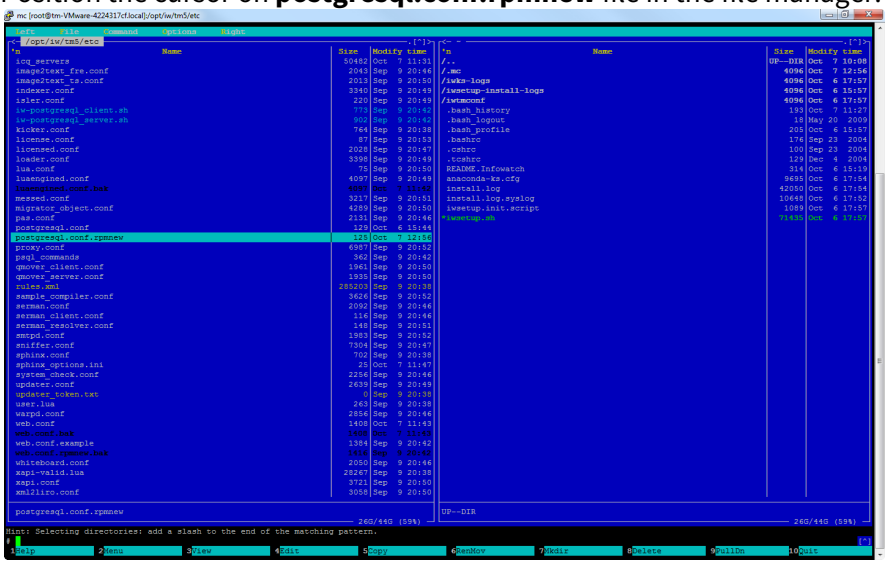
The **postgresql.conf.rpmnew** file looks like:

```
{
    "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"
}
```

4.5.3 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 to follow the instructions.

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

The 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

5 Uninstalling the System

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

- See details on DB schema removal (Oracle as well as PostrgreSQL) in "Deleting the Database Scheme".
- See details on Device Monitor removal (Server and Clients) in "Uninstalling Device Monitor".
- The Crawler subsystem (server as well as scanner) can be removed by standard OS Windows tools: **Start -> Control panel -> Programs and components**, a **Delete** command.
- 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.
>
> The process of database deletion launches on the server with database installation template, including cases when remote database is used.

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`

4. **Removing old versions of configuration**
   a. Go to directory
   `/opt/iw/tm5/etc/configerator`
   b. Remove all content of the directory.

> **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 and Distribution service:

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 or Distribution service:

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.

Warning!

When Distribution service is removed the distribution point and directory containing ditribution kits are to be removed as well.

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.

If you encounter any difficulties removing Agent, please contact our technical support at support@infowatch.com.

You can also visit the technical support section on our website: http://www.infowatch.com/support.

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.

To remove InfoWatch Device Monitor Agent which was installed to OS Astra Linux, please run the following command:

dpkg --purge iwdm

5.4 Uninstalling Traffic Monitor

Warning!

If the database is located on the same server, where the unintstallation process is to be started, first, remove DBMS.

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

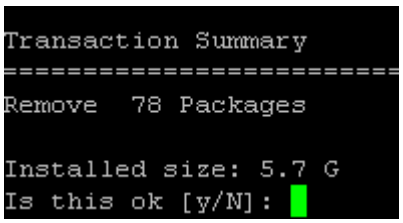
If you require to restore events when reinstalling Traffic Monitor, you are recommended to create a database reserve copy before processing the uninstallation (for more details see "*InfoWatch Traffic Monitor. Administration Guide".* Database Administration - **PostgreSQ**L > Database Backup "Creating 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. Stop Traffic Monitor processes by entering the command:
   `iwtm stop`
3. To remove Traffic Monitor packages, enter the commad:
   `yum remove `rpm -qa | grep iwtm``
   Preparing for removal will start.
4. Preparation finished, the list of packages to be removed will be displayed in a confirmation window:

   To continue, enter "**Y**" and press **Enter**.
   Traffic Monitor packages removal will start.
   Wait until the end of uninstalling process.

All Traffic Monitor services will be removed. After removal, the following entities will stay on the computer:

- configutation files, that were changed (changed files will get the suffix **.rpmsave**, for example, **web.conf.rpmsave**; unchanged files will be removed);
- objects queue (for details on how to remove files from the directory containing OS temporary files and Traffic Monitor file queues directory, see «*InfoWatch Traffic Monitor. Administration Guide", article "Deleting Temporary Files"*);
- configuration elements;
- license file;
- user account – InfoWatch Traffic Monitor owner and the group, this user was in;
- logs;
- distributives.

To remove all other files, you can remove the directory / `opt/iw` and all of its content by using OS tools.

Warning:

Before removal, make sure that directories do not contain some important information.

To remove a directory, you can use the command:

```
rm -Rvf /opt/iw
```

Note:

In case of distributed installation of Traffic Monitor, the actions described above should be performed on each server.

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.

Requirements for DB user's passwords

- The user password should not contain the symbols «"» and «'».

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