

INFOWATCH

InfoWatch Traffic Monitor

Installation Guide

10/29/2026

© JSC “InfoWatch”

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

http://www.infowatch.com

TABLE OF CONTENTS

1 Introduction 4

1.1 Who Should Read this Guide 4

1.2 Set of Documents 4

1.3 Technical Support 4

2 Getting Ready to Install 5

2.1 System Deployment Schemes and Installation Types 5

2.2 Hardware and Software Requirements 16

2.2.1 * Traffic Monitor server can use interceptors which impose additional requirements: 20

2.2.2 Supported DBMS 20

2.3 Operating System and Network Server Configuration Requirements 21

2.3.1 Recommendations on Disk Space Partitioning 23

2.3.2 Configuring Local Repositories 26

2.4 Configuring Remote Database 28

2.4.1 Configuring PostgreSQL 28

2.4.2 Configuring Postgres Pro Enterprise 32

2.4.3 Configuring Jatoba 37

2.4.4 Configuring Tantor 41

3 Installing the System 47

3.1 Installing Data Storage 48

3.1.1 Preparing the Server 50

3.1.2 Installing Platform 54

To install Platform in the central mode: 54

To install Platform in the office mode: 56

Installing Platform with Parameters Speficied in the Command Line 58

3.2 Installing Traffic Monitor Server and Database 60

3.2.1 All-in-One Installation Mode of TM Enterprise and TM Standard 61

3.2.2 Distributed Installation of TM Enterprise 85

3.2.3 Installing the System in Silent Mode Using Parameter File 128

Parameter file (option file) 134

Silent mode installation 135

Full composition of parameter file 137

3.3 Pre-installed Server Parameters 167

4 Updating the System 170

4.1 Before the update 171
4.2 Updating the System 172
4.3 Duplicate-defining script 173
4.4 Updating TM All-in-One Enterprise and Standard 173
4.4.1 Parameter file (option file) 192
4.4.2 Silent mode installation 193
4.4.3 Full composition of parameter file 194
4.5 Updating TM in case of Distributed Installation 206
4.5.1 Parameter file (option file) 226
4.5.2 Silent mode installation 227
4.5.3 Full composition of parameter file 228
4.6 Merging Configuration Files 239
4.6.1 Merging configuration files in Midnight Commander 240
4.6.2 Merging configuration files by means of vimdiff 242
4.7 Updating Data Storage 242
4.7.1 Direct Update of Platform 243
4.7.2 Updating Platform by Resetting the Installation 245
5 Uninstalling the System 247
5.1 Uninstalling Data Storage 247
5.2 Deleting the Database Scheme 247
5.3 Uninstalling Traffic Monitor 249
6 Appendix A. Username and Password Recommendations 252
7 Appendix B. Licenses for Third-Party Technologies 254

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.

In addition to the primary System User Guide and Administration Guide, a Knowledge Base is available at lk.infowatch.ru, which includes troubleshooting materials and answers to questions. If you do not have access to the Knowledge Base, please contact the technical support service of InfoWatch at support@infowatch.com.

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.

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

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

The InfoWatch Traffic Monitor System (hereinafter – TM) is available in several variants. Its features depend on the System, the distribution of components, the DBMS (database management system) in use, and the edition.

Traffic Monitor 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 compared to the Enterprise version (for details, see the article *Differences between Enterprise and Standard Traffic Monitor editions*). 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 Servers with functional roles:**
    - **Database**
    - **Indexer service**
    - **Web console**
    - **Traffic interceptors**

      > **Note:**
      >
      > It is not recommended to install and run applications on servers (especially server applications) or use a computer as a file server.

  - **Device Monitor**, an interception module designed as a server part and controlled via the Management console and Agents deployed to company workstations.
  - **Adapters**, a set of interception modules for integration with third-party systems.
  - **Vision**, a module that visualizes incident investigation. Uses data from InfoWatch Traffic Monitor.
  - **Activity Monitor**, a module for employee actions monitoring.
  - **Prediction**, predictive and behavioral analytics module.
  - **Data Discovery**, a module for searching confidential information on shared network resources, workstations, servers, and in document storages.
  - **Data Analysis Service**, a service for analyzing data from InfoWatch Traffic Monitor or other InfoWatch products.
  - **Data Storage**, an external storage of binary data.

In any Traffic Monitor edition, you can also access the following features without purchasing an additional license:

- **Autolinguist**, a technology for analyzing text data. For details, see *InfoWatch Traffic Monitor. User Guide. Autolinguist* article.

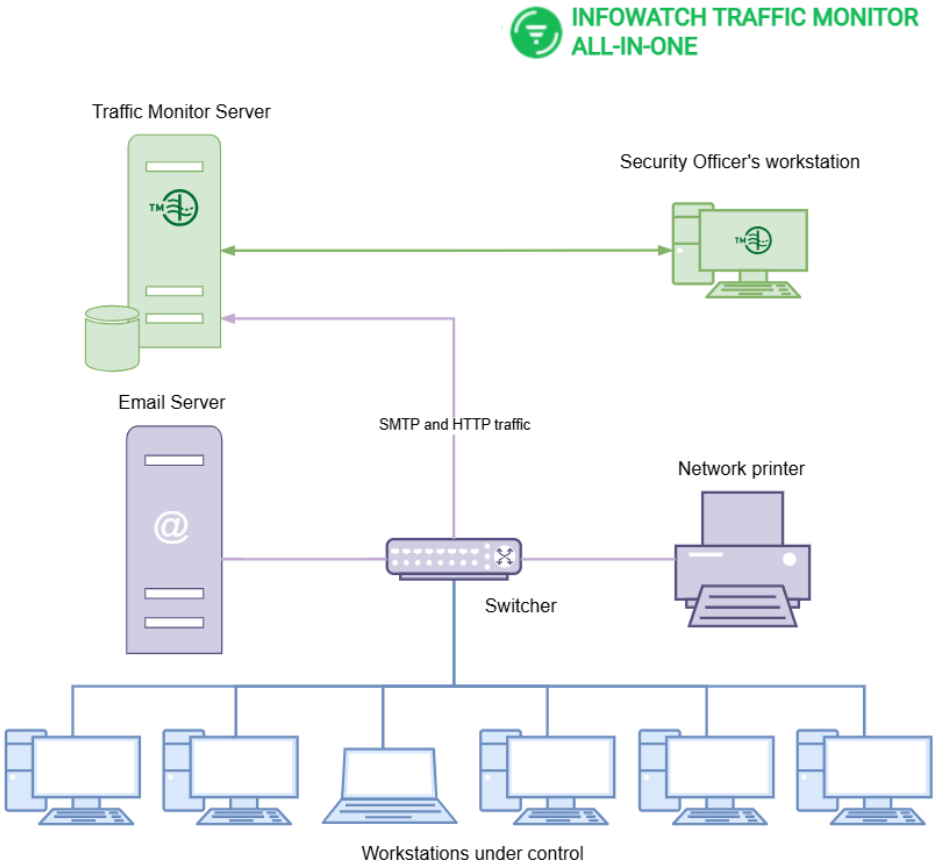
- **Data Explorer**, a software product that allows you to automate the process of forming DLP system policies by allocating thematic clusters of documents in your company information flows.
- Exporting data from Traffic Monitor to InfoWatch Investigation Centre.

> **Note:**
>
> Token for integration between Investigation Centre and Traffic Monitor is available immediately after Traffic Monitor installation. You can find it in the **Administration** -> **Plugins** section of the Traffic Monitor Management console, on the **Tokens** tab of the **InfoWatch Investigation Centre** pre-installed plugin.

Traffic Monitor installation types

You can install Traffic Monitor in one of the modes:

- **All-in-one installation** involves installing all the System components and DBMSs on the same server. This installation type is used if, with respect to the assumed load, the server has resources for both DBMS and TM services. The scheme below illustrates all-in-one deployment:



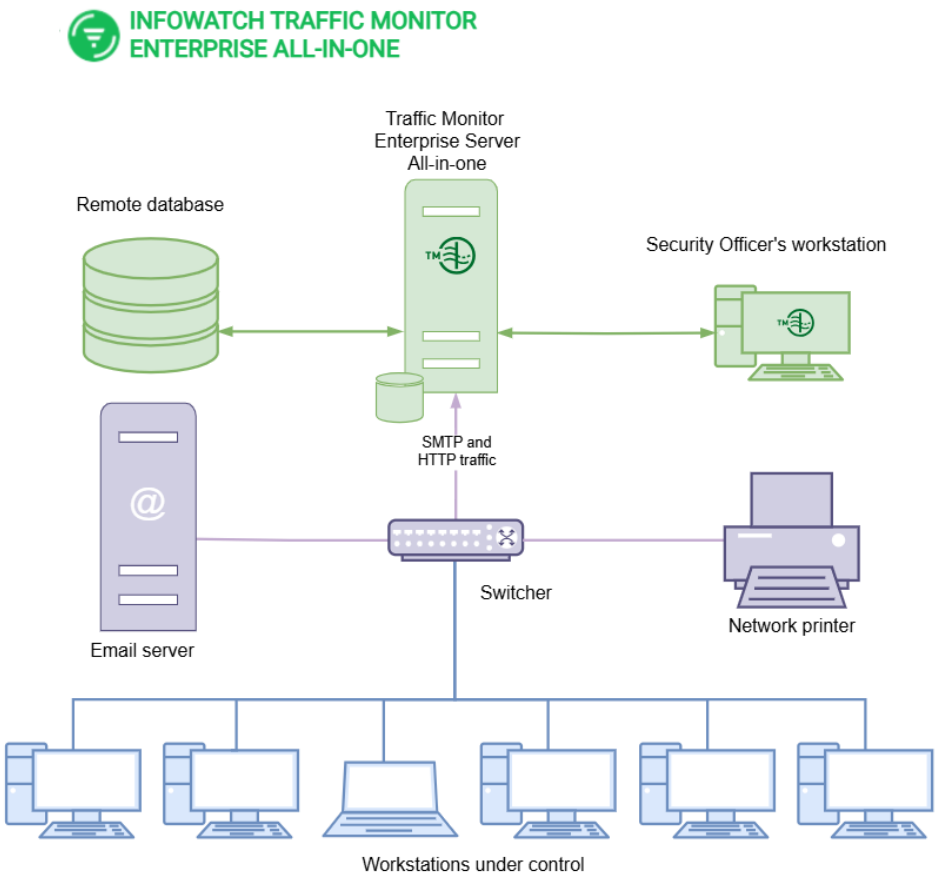
Both Traffic Monitor editions support All-in-one installation:

- When deploying Traffic Monitor **Standard** edition in **All-in-one** mode, you can only install the DBMS provided in the package.
- When deploying Traffic Monitor **Enterprise** edition in **All-in-one** mode, you can:
  - Select a DBMS provided in the package.
  - Connect to an already-deployed DBMS. You can use a DBMS which is deployed:

- On one server with TM.
- On a separate server. In both cases, DBMS is considered `remote`.

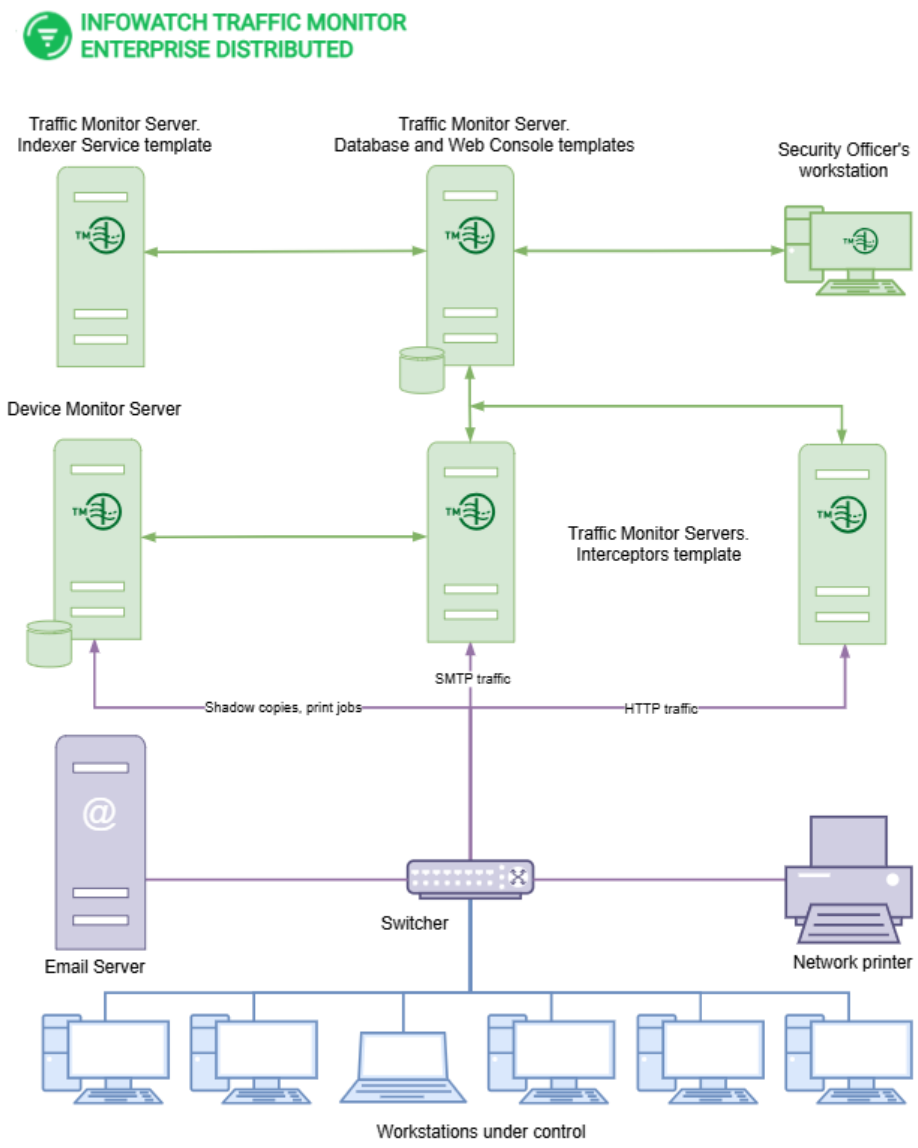
> **Note:**
>
> For details on compatible DBMSs, see *Supported DBMS* section of *Hardware and Software Requirements* article.

The scheme illustrates an example of Traffic Monitor Enterprise deployment in All-in-one mode connected to a remote database:

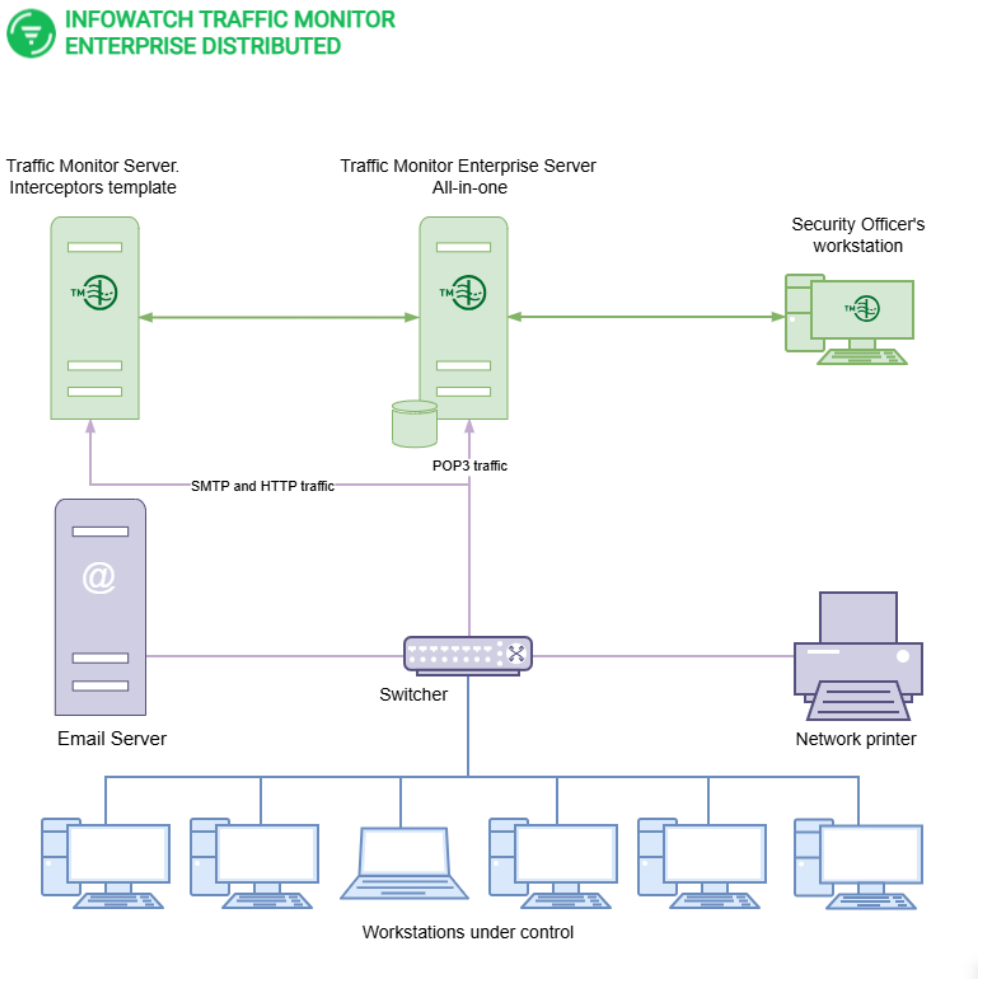


- **Distributed installation** involves installing Traffic Monitor components and DBMS on different computers according to their functional roles. This installation type is available for **Enterprise** edition only. You can use it to enhance the performance of Traffic Monitor services and DBMS by allocating them to different servers load-wise. Functional roles of servers are defined by *templates*.

Here is an example of a multi-server System deployment:



When deploying in the Distributed mode, you can also use an All-in-one TM Enterprise Server as one of the System components. In the example below, the All-in-one Server is extended with the interception server:

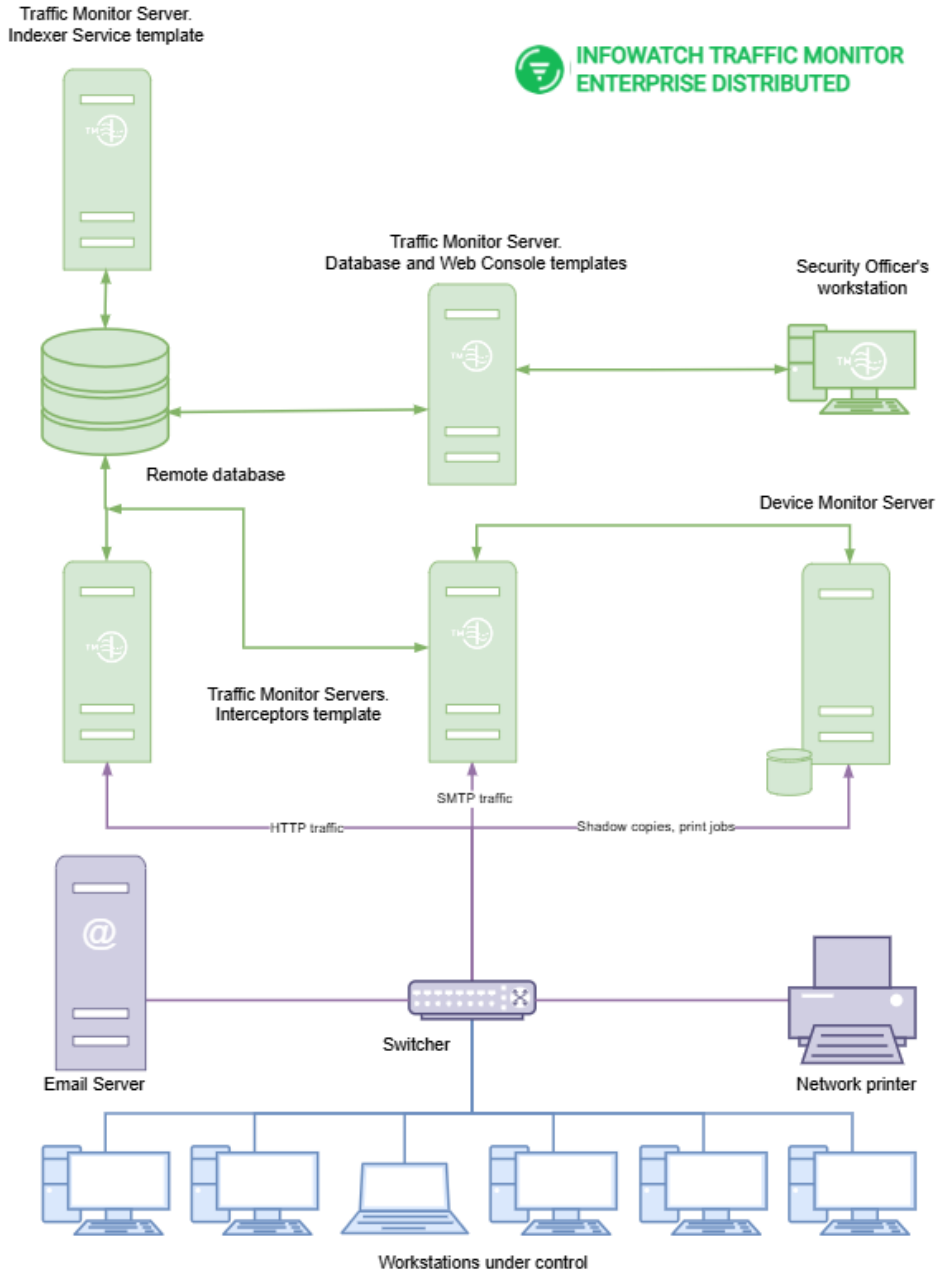


When installing TM in the Distributed mode, you can:

- Select a DBMS provided in the package.
- Connect to an already deployed DBMS. You can use a DBMS which is deployed:
  - On one server with TM.
  - On a separate server. In both cases, DBMS is considered `remote.`

> **Note:**
>
> For details on compatible DBMSs, see *Supported DBMS* section of *Hardware and Software Requirements* article.

The scheme shows a distributed deployment example for TM Enterprise connected to a remote database:



Data Storage

Regardless of installation type, we recommend to *install an external storage of binary data – Data Storage* in addition to a database. It will store contents from interception events, such as attachments, screenshots, audio files, and so on. With it, you can:

- optimize data storing
- increase DBMS productivity
- accelerate the process of updating Traffic Monitor
- significantly reduce the load on DB when working with large amounts of data

You can install Data Storage and Traffic Monitor on the same or different servers. If there are more than 2000 workstations in your company, we recommend to install the storage on a separate server.

Installation templates

Traffic Monitor installation kit contains installation templates. Each template is a set of Traffic Monitor components to be activated after the System is deployed. Sets of components are consistent with the functional roles of the servers. Setting the server roles at the installation stage facilitates the System deployment plan, reduces the installation time, and makes the System easy to operate. Using templates also makes it easier to maintain a large-scale System.

Regardless of the selected template, it is used only to define the set of active Traffic Monitor components, so the server will have all the components installed. If needed, you can change the set of active components on a particular server after the installation.

One server can have several templates installed at the same time. All-in-one installation is equivalent to installing all templates on a single server.

A complex of servers allocated for System deployment composes a cluster.

There are four templates available to install:

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

> **Important!**
>
> One cluster should contain a single copy of the **Database**, **Indexer service**, and **Web console** templates.

In all templates, the following services will be started after the installation:

- `iwtm-consul` ensures service-to-service interaction
- `iwtm-nagios` is a set of sensors to control the System state

"Database" template

The template includes a DBMS and modules to control the server state.
The DBMS provides storage of data analysis results, information about intercepted objects and applied policies. If you are going to connect to an already deployed database, then a DBMS client will be installed on the server with the **Database** template. Using this client, components of other templates will send data to a remote database.

The following processes belong to the **Database** template:

Process name	Brief purpose description
`iw_agent`	Required to manage the configuration of the System
`iw_system_check`	Controls the System state
`iw_space_manager`	Manages tablespaces

> **Warning!**
>
> The process `iw_space_manager` should be in a single instance within one cluster. Otherwise, there will be data inconsistencies in the System.

"Indexer service" template

The template includes components to index text of objects intercepted by the System and stored in the database. Also, the template components are used to index metadata of interception and audit events. With the template modules, you can search by events using queries. To perform fulltext search, the Sphinx engine is used.

The following processes belong to the **Indexer service** template:

Process name	Brief purpose description
`iw_agent`	Required to manage the System's configuration
`iw_indexer`	Indexes events text
`iw_is`	Indexes metadata
`iw_metainfo_fetcher`	Samples data for indexing from the database
`iw_system_check`	Controls the System state

Warning!

A cluster should contain only a single instance of each of the following processes:

- `iw_indexer`
- `iw_is`

Otherwise, there will be data inconsistencies in the System.

"Web console" template

The template includes components of the Traffic Monitor Management console – graphical user interface. Also, this template includes text and graphical object classifiers, as well as license components.

With the Management console, you can monitor summary information, create policies and protected objects, add contacts, view events, export data, and create reports.

The following processes belong to the **Web console** template:

Process name	Brief purpose description
`iw_adlibitum`	Provides integration with LDAP catalogues
`iw_agent`	Required to manage the System's configuration
`iw_blackboard`	Responsible for: • Adding/removing status to persons/workstations from policies • Adding new contacts • Adding new applications to automatic search suggestions • Adding notifications from policies to queue

Process name	Brief purpose description
`iw_bookworm`	Used as System directory
`iw_configerator`	Builds a configuration for Device Monitor Agents regarding data protection policies on agents
`iw_deliver`	Dispatches email messages from quarantine as per Security officer decision, when working in the "inline" mode
`iw_image_autoling`	Automatically classifies graphical objects
`iw_kicker`	This 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
`iw_licensed`	License management
`iw_sample_compiler`	Makes digital fingerprints from downloaded sample documents
`iw_system_check`	Controls the state of the system
`iw_tech_tools`	Auxiliary utilities for content analysis module
`iw_text_autoling`	Automatically classifies text objects
`iw_updater`	Loads configuration from database
`iw_warpd`	Manages data extraction from objects loaded via web interface

Warning!

A cluster should contain only a single instance of each of the following processes:

- `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.

"Traffic interceptors" template

The template includes the modules responsible for collecting and analyzing data, as well as applying policies. Template components ensure in-stream/at-the-gateway interception of traffic sent using the protocols:

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

For the template to receive data from a range of third-party systems, use dedicated adapters. See the document *InfoWatch Traffic Monitor. Administration Guide. Processing Traffic Received from Third-party Systems* for details.

In case the *load average* indicator approximates to the number of kernels, we recommend that you scale out servers with the **Traffic interceptors** role.

The following processes are included to the **Traffic interceptors** template:

Process name	Brief purpose description
`iw_agent`	Required to manage the System's configuration
`iw_analysis`	Is used for content analysis of: • Objects from third-party systems • HTTP and ICQ traffic from the Sniffer module • Objects in Device Monitor events that do not relate to mail protocols
`iw_blackboard`	Responsible for: • Adding/removing status to persons/workstations from policies • Adding new contacts • Adding new applications to automatic search suggestions • Adding notifications from policies to queue
`iw_capstack`	Processes traffic sent via POP3, IMAP, NRPC protocols. Disabled by default
`iw_cas`	Intercepted data content analysis
`iw_icap`	Processes HTTP traffic received from ICAP client
`iw_messed`	Used to process SMTP messages and objects in Device Monitor events that relate to mail protocols
`iw_pas`	Service to process data after analysis

Process name	Brief purpose description
`iw_proxy_icq`	Receives copy of ICQ traffic in copy mode from Sniffer. Disabled by default
`iw_proxy_http`	Receives copy of HTTP traffic in copy mode from Sniffer. Disabled by default
`iw_proxy_smtp`	Receives copy of SMTP traffic in copy mode from Sniffer. Disabled by default
`iw_qmover_client`	Client part of the module that sends objects to a remote database. Disabled by default
`iw_rest2push`	Receives objects from external systems via HTTP/HTTPS and sends events to `iw_xapi_puppy` via the Thrift protocol
`iw_sniffer`	Receives a data copy from switcher's SPAN port. Disabled by default
`iw_smtpd`	Receives SMTP messages
`iw_system_check`	Controls the state of the System
`iw_updater`	Loads configuration from database
`iw_warpd`	Manages data extraction from intercepted objects
`iw_xapi_xapi`	Receives objects from InfoWatch Device Monitor and Data Discovery
`iw_xapi_puppy`	Receives objects from third-party systems
`iw_x2db`	Loads objects to database
`iw_x2x`	Converts objects from interceptors to a standard 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*.

Warning!

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

  > **Note:**
  >
  > The list of DBMS, with which Traffic Monitor can interact, depends on the OS of Traffic Monitor server. See details in *Supported DBMS*.

- **Adapters** – their requirements are listed in the documentation supplied with adapters software.
- **Device Monitor Server and Device Monitor Agents** – the module, containing the agents on Windows, macOS and Linux systems. See the requirements in *InfoWatch Device Monitor. Installation, Configuration and Administration Guide.*
- **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.
- **External storage of binary data - Data Storage** – can be installed on the same server with Traffic Monitor or on different ones. See the requirements *below.*

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.

A significant difference in the load on a certain interception channel can also influence the number and role of Traffic Monitor Servers: for example, the efficient traffic processing from Device Monitor you need to dedicate separate servers for **iw_xapi_xapi** processes.

Software and estimated minimal hardware requirements are listed in the following table. For disk subsystem and RAM size requirements depending on the number of employees and data retention period, as well as considering Device Monitor data collection, see *Recommendations on Disk Space Partitioning* article. 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 7.5, 7.6, 7.7, 7.8, 7.9 with subscription, required for the update; • Red Hat Enterprise Linux 8.10; • Oracle Linux 7.7, 7.8, 7.9; • Oracle Linux 8.10; • AlmaLinux 8.10; • Rocky Linux 8.10.	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® Processor E5-2640 v3 - 2,6 Hz)	24 GB	OS: • Red Hat Enterprise Linux 7.5, 7.6, 7.7, 7.8, 7.9 with subscription, required for the update; • Red Hat Enterprise Linux 8.10; • Oracle Linux 7.7, 7.8, 7.9; • Oracle Linux 8.10; • AlmaLinux 8.10; • Rocky Linux 8.10.	The server should have a network interface with the assigned IP address. Requirements imposed by the interceptors should be fulfilled*

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
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 7.5, 7.6, 7.7, 7.8, 7.9 with subscription, required for the update; • Red Hat Enterprise Linux 8.10; • Oracle Linux 7.7, 7.8, 7.9; • Oracle Linux 8.10; • AlmaLinux 8.10; • Rocky Linux 8.10.	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 7.5, 7.6, 7.7, 7.8, 7.9 with subscription, required for the update; • Red Hat Enterprise Linux 8.10; • Oracle Linux 7.7, 7.8, 7.9; • Oracle Linux 8.10; • AlmaLinux 8.10; • Rocky Linux 8.10.	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
Database 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 from 6xC, 2,6 GHz	16GB and more depending on data volume, insertion and processing speed	OS: • Red Hat Enterprise Linux 7.5, 7.6, 7.7, 7.8, 7.9 with subscription, required for the update; • Red Hat Enterprise Linux 8.10; • Oracle Linux 7.7, 7.8, 7.9; • Oracle Linux 8.10; • AlmaLinux 8.10; • Rocky Linux 8.10.	See *Supported DBMS* for details.
External storage of binary data – Data Storage				
When using Data Storage, the requirements to the Traffic Monitor disk subsystem given above are divided into Traffic Monitor database and Data Storage in the ratio of 15% to 85%. When installing Traffic Monitor and Data Storage on the same server, you do not need the additional space for data storing. **Example:** Traffic Monitor and Data Storage are to be installed on the different servers. The requirements for Traffic Monitor disk subsystem: 400 GB.	CPU from 4xC, 2,1 GHz	From 16GB	OS: • Red Hat Enterprise Linux, versions: • 7.9; • 8.9; • 8.10 (supported for Platform starting from version 2.4.X). • Oracle Linux, versions: • 7.9; • 8.4; • 8.10.	To use Data Storage, you should install Platform version 2.0.0 or higher.

Disk subsystem	**Processor**	**RAM**	**Software**	Additional requirements
Then you need 60 GB for database on the Traffic Monitor server and 340 GB for binary data storing on the Data Storage server.				

Note:

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

2.2.1 * 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.

2.2.2 Supported DBMS

Traffic Monitor Standard installation wizard installs PostgreSQL 15 DBMS together with the product.

When installing **Traffic Monitor Enterprise**, you can:

- Use a DBMS provided in the package. In this case, a database is considered `local`.
- Connect to an already deployed DBMS. In this case, a database is considered `remote`. A DBMS can be deployed:
  - on one server with TM;
  - on a separate server.

Warning!

In case you are planning to use a DBMS in remote mode, configure it before installing Traffic Monitor. See *Configuring Remote Database* for details.

The table represents DBMS with which Traffic Monitor Enterprise can interact, depending on the server OS:

Operating System of Traffic Monitor Server	DBMS	
	`local` mode, DBMS included in a distribution kit	`remote` mode
Red Hat Enterprise Linux 7.x	• Oracle 19c • PostgresSQL 15	• Oracle Enterprise 19c • PostgreSQL 15 • Postgres Pro Enterprise 15 • Jatoba 5 • Tantor 15
Red Hat Enterprise Linux 8.10	PostgresSQL 15	• PostgreSQL 15 • Postgres Pro Enterprise 15 • Jatoba 5 • Tantor 15
AlmaLinux 8.10		
Rocky Linux 8.10		
Oracle Linux 8.10		
Oracle Linux 7.x	• Oracle 19c • PostgresSQL 15	• Oracle Enterprise 19c • PostgreSQL 15 • Jatoba 5 • Tantor 15

2.3 Operating System and Network Server Configuration Requirements

For successful installation of the System, the server should meet the following requirements:

Operating system

The server should have Red Hat Enterprise Linux OS 7.x (latest version).

Note:

You can also install the System on one of the other supported OS:

- RED OS;
- Oracle Linux OS;
- Red Hat Enterprise Linux 8;
- AlmaLinux;
- Rocky Linux;
- Alt Server.

You can find information on versions of supported OS in the *Hardware and Software Requirements* article.

For all OS listed above, you can use the following instructions on System installation and operation.

Warning!

When loading Oracle Linux OS, please select Red Hat Compatible Kernel (RHCK), for example, Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`.

After loading Oracle Linux OS:

- Remove the UEK kernel by running the command:

```
yum remove kernel-uek*
```

- Disable the `uek-ol7.repo` repository:

```
sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/uek-ol7.repo
```

Repositories

OS repositories should be configured to install the following packages:

- `redhat-lsb-core`;
- `lshw`;
- `ntp`;
- `ntpdate`;
- `tuned`;
- `postfix`;
- `perl-Dist-CheckConflicts`;
- `perl-List-MoreUtils`;
- `urw-base35-fonts-legacy`;
- `python3-psycopg2`;
- `libzstd`;
- `redis`.

See how to configure a local repository on the *Red Hat Enterprise Linux* official website.

Note:

If you are installing or updating Traffic Monitor on a 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.

See instructions on preparing a server for System installation or update on Oracle Linux 7 OS in *Configuring Local Repositories*.

The following common repositories should be available depending on the operating system:

- For OS Red Hat Enterprise Linux 7:
  - `os`;

    - `updates`;
    - `optional`;
- For OS Oracle Linux 7:
    - `ol7_latest`;
    - `ol7_optional_latest`;
    - ol7_developer_EPEL.
- For OS Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 and Rocky Linux 8:
    - `BaseOS`;
    - `AppStream`;
    - `EPEL`.

Disk space

Disk space partitioning should be configured according to *Recommendations on Disk Space Partitioning* article.

Mount point

Mount points options should not contain `nosuid` and `noxattr` command options (you can check this when opening the file `/etc/fstab`).

Network configuration

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.

Antivirus

Antivirus on the server should be configured to operate together with the System (see the knowledge base article *Antivirus configuration for Traffic Monitor server*).

2.3.1 Recommendations on Disk Space Partitioning

The article contains recommendations on disk space partitioning for Traffic Monitor deployment in All-in-One mode with Device Monitor server. For deployment modes, see *System Deployment Schemes and Installation Types*.

The calculations correspond to the expected network load:

- 100 employees;
- 300 employees;

- 500 employees.

For expected load of 1000 employees and more, distributed installation is recommended. In case of distributed installation, 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.

> **Note:**
>
> On how to configure *partitions* and *swap space*, see the Red Hat Enterprise Linux official website.

Recommendations on disk space partitioning to process data for 100 employees:

		Data retention period, months		
		3	6	12
Total disk size, GB		1228.8	1945.6	3584
Disk sections, GB	`swap`	8	8	8
	`/boot`	1	1	1
	`/`	150	180	220
	`/opt`	150	150	150
	`/u01`	50	70	100
	`/u02`	868	1536	3174.4
RAM, GB		22	28	40

Recommendations on disk space partitioning to process data for 300 employees:

		Data retention period, months			
		3	6	12	24
Total disk size, TB		2764.8	5017.6	9830.4	*Distributed installation is recommended*
Disk sections, GB	`swap`	16	16	32	

		Data retention period, months			
		3	6	12	24
	`/boot`	1	1	1	
	`/`	180	200	200	
	`/opt`	220	220	220	
	`/u01`	100	150	200	
	`/u02`	2048	3993.6	8192	
	`/var/lib/sphinx`	200	400	800	
RAM, GB		40	56	96	

Recommendations on disk space partitioning to process data for 500 employees:

		Data retention period, months		
		3	6	12
Total disk size, GB		4300.8	8192	*Distributed installation is recommended*
Disk sections, GB	`swap`	16	32	
	`/boot`	1	1	
	`/`	200	200	
	`/opt`	220	220	
	`/u01`	200	200	
	`/u02`	3379.2	6860.8	
	`/var/lib/sphinx`	300	600	
RAM, GB		24	96	

2.3.2 Configuring Local Repositories

If you are installing or updating Traffic Monitor on Oracle Linux 7 OS with no internet access:

1. Make sure that, in operating system, the current kernel is Red Hat Compatible Kernel (RHCK), for example, Oracle Linux Server Kernel `3.10.0-xxxx.el7.x86_64`, and the UEK kernel is removed. For details, see *Operating System and Network Server Configuration Requirements*.
2. If the OS kernel contains updates, provide the installation of the `kernel-headers` and `kernel-devel` packages that correspond to the loaded kernel version.

   Note:

   You can display the kernel version by running the command:

   ```
   uname -r
   ```

   To display installed `kernel` packages, run the command:

   ```
   yum list installed|grep kernel
   ```

   If, when installing Traffic Monitor, the installer does not find needed packages, the installation fails with an error.

   Example of the error text:

   ```
   Preparing installation...|Warning: Failed to prepare installation.
   Cannot find kernel-headers-3.10.0-1160.119.1.0.5.el7.x86_64 package.
   Missing OS repos or unsupported OS. Please mount and/or enable OS packages
   repository and try once again.
   ```

3. Disable external repositories by running the following command:

   ```
   find /etc/yum.repos.d/ -iname "*.repo" -exec sed -i -e "s/enabled=.*/enabled=0/g" {} \;
   ```

4. Connect the disk with the OS Oracle Linux distributive to the server.
5. Mount the disk with the OS Oracle Linux distributive, using the following command:

   ```
   mkdir -p /media/cdrom/ && mount /dev/cdrom /media/cdrom/
   ```

6. Create the `/etc/yum.repos.d/cdrom.repo` file specifying the mounted disk as a repository. For this, run the following command:

   ```
   cat << EOF > /etc/yum.repos.d/cdrom.repo
   [cdrom]
   ```

```
name=cdrom
baseurl=file:///media/cdrom/
enabled=1
gpgcheck=0
EOF
```

7. Remove temporary files and make sure that repository list contains the repository from the disk:

```
yum clean all && yum repolist
```

8. Install `Perl`:

```
yum install perl
```

9. Install the following packages:
   - `perl-List-MoreUtils-0.33-9.el7.x86_64.rpm` (you can download the package from *the official Oracle Linux 7 Latest repository*)
   - `perl-Dist-CheckConflicts-0.06-2.el7.noarch.rpm` (you can download the package from *the official Oracle Linux 7 Optional Latest repository*)
   - `urw-base35-fonts-legacy-20170801-10.el7.noarch.rpm` (you can download the package from *the official Oracle Linux 7 Optional Latest repository*)
   - `python3-psycopg2-2.7.7-2.el7.x86_64.rpm` (you can download the package from *the official Oracle Linux 7 EPEL repository*)
   - `libzstd-1.5.5-1.el7.x86_64.rpm` (you can download the package from *the official Oracle Linux 7 EPEL repository*)

   For this:
   a. Download the listed packages from the official Oracle Linux repositories.
   b. Copy them to the server where Traffic Monitor is to be installed.
   c. Go to the directory where you copied the packages.
   d. Run the following command for each package:

```
yum localinstall <package_name>
```

> **Note:**
>
> Optionally you can install tools for work in operating system by running the command:
>
> ```
> yum install mc vim screen telnet bind-utils mlocate net-tools iptraf sysstat
> iotop rsync
> ```

10. Make sure you have correctly configured network settings (see *Operating System and Network Server Configuration Requirements*) and the `/etc/hosts` file contains the hostname resolving setting. If it does not, run the command:

```
sh -c "echo '<IP_address> `hostname -f` `hostname -s`' >> /etc/hosts"
```

2.4 Configuring Remote Database

If you plan using an already deployed database:

1. Make sure the version of your database is supported by Traffic Monitor. For details, see *Supported DBMS* section of *Hardware and Software Requirements* article.

   > **Note:**
   >
   > If required, update the DBMS to supported version. To do this, use the official instructions.

2. Perform preliminary setup:
   - Configuring PostgreSQL
   - Configuring Postgres Pro Enterprise
   - Configuring Jatoba
   - Configuring Tantor

2.4.1 Configuring PostgreSQL

To prepare a remote database for installation of Traffic Monitor components, follow these steps on the database server:

1. Install additional packages running the commands:

   ```
   yum -y install pgagent_15* postgresql15-contrib
   ```

2. Stop `postgresql` and `pgagent` services operation using the commands:

   ```
   systemctl stop postgresql-15
   systemctl stop pgagent_15
   ```

3. Create a file `/etc/systemd/system/postgresql-15.service.d/override.conf` or add the following content to it:

   ```
   [Service]
   Environment=PGDATA=/u01/postgres
   ```

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"
sudo -u postgres /usr/pgsql-15/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. To `/u01/postgres/iwtm-postgres.conf` file, add 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'
track_io_timing = on
track_activity_query_size = 32768

constraint_exclusion = off                    # on, off, or partition
```

Important!

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. In `/u01/postgres/postgresql.conf` file, add a link to `iwtm-postgres.conf` file. Use 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. Start `postgresql` service and check its status using the commands:

```
systemctl enable postgresql-15
systemctl start postgresql-15
systemctl status postgresql-15
```

12. Change the database administrator's default password:

```
su - postgres psql -p 5433 alter user postgres password 'xxXX1234';
```

13. Create all required extensions 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 pgagent;
```

14. To exit, enter the commands:

```
\q
exit
```

15. To configure `pgagent` user in OS, run the commands:

```
mkdir /home/pgagent
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`, so that the content looks as follows:

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

> **Important!**
>
> Empty line at the end of `pgagent` file is compulsory.

17. Change the privileges, owner and group as per `/etc/sudoers.d/pgagent`. Run the commands:

```
chmod 440 /etc/sudoers.d/pgagent
chown root:root /etc/sudoers.d/pgagent
```

18. In `/etc/pgagent/pgagent_15.conf` configuration file, change the value of `DBPORT` parameter from `5432` to `5433`:

```
sed -i --follow-symlinks "s/DBPORT=5432/DBPORT=5433/" /etc/pgagent/pgagent_15.conf
```

19. Run `pgagent` and check its status using the commands:

```
systemctl enable pgagent_15
systemctl start pgagent_15
systemctl status pgagent_15
```

Once you have configured the database, make sure there are no critical errors in `/var/log/pgagent_15.log` and database logs.

2.4.2 Configuring Postgres Pro Enterprise

To prepare a remote database for installation of Traffic Monitor components, follow these steps on the database server:

1. Install an additional package using the command:

```
yum -y install postgrespro-ent-15-contrib
```

2. Stop `postgrespro` service operation. Use the command:

```
systemctl stop postgrespro-ent-15.service
```

3. Edit `/etc/systemd/system/postgrespro-ent-15.service.d/override.conf` file. In case it does not exist, create a new one. Add the following lines to it:

```
[Service]
Environment=PGDATA=/u01/postgres
```

4. In order to apply changes in 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
sudo -u postgres initdb --encoding=UTF8 --locale=en_US.UTF-8 -D /u01/postgres
mkdir -p /u01/postgres/tmp
```

6. Create `/u01/postgres/iwtm-postgres.conf` file. You can use the command:

```
touch /u01/postgres/iwtm-postgres.conf
```

7. Добавьте в файл `/u01/postgres/iwtm-postgres.conf` следующее содержимое:

```
# -----------------------------
# Postgres Pro 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 = 128kB

huge_pages = try                        # on, off, or try

max_locks_per_transaction = 512
temp_buffers = 32MB
work_mem = 16MB
effective_cache_size = 4096MB

min_wal_size = 6144MB
max_wal_size = 6144MB
lc_messages = 'en_US.UTF-8'             # locale for system error message
log_directory = 'pg_log'
log_filename = 'postgresql.log'         # log file name pattern
log_rotation_age = 0                    # Automatic rotation of logfiles will happen
after that time. 0 disables.
log_rotation_size = 0                   # Automatic rotation of logfiles will happen
after that much log output. 0 disables.
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

autovacuum_max_workers = 5
autovacuum_naptime = 20
maintenance_work_mem = 1GB
autovacuum_freeze_max_age = 10000000000

shared_preload_libraries = 'pg_stat_statements'
track_io_timing = on
track_activity_query_size = 32768

constraint_exclusion = off                 # on, off, or partition
standard_conforming_strings = on
```

Важно!

The configuration file's content above contains example values 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. To `/u01/postgres/postgresql.conf` configuration file, add the link to the `iwtm-postgres.conf` file.
Run the command:

```
echo "include = 'iwtm-postgres.conf'" >> /u01/postgres/postgresql.conf
```

10. Edit the access file `/u01/postgres/pg_hba.conf`:
    a. After the lines:

```
# IPv6 local connections:
host    all             all             ::1/128                 md5
```

add the line:

```
host    postgres        all             0.0.0.0/0               md5
```

> **Note:**
>
> The provided values are suitable for Traffic Monitor installation with default parameters. In case you are going to use different values during Traffic Monitor installation, specify them here.

b. Replace the lines using the commands:

```
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*127.0.0.1/32[[:space:]]*md5|
host    all             all             127.0.0.1/32            trust|" /u01/
postgres/pg_hba.conf
sed -i "s|local[[:space:]]*all[[:space:]]*all[[:space:]]*peer|local   all
all                                     trust|" /u01/postgres/pg_hba.conf
```

11. Start `postgrespro` service:

```
systemctl start postgrespro-ent-15.service
```

12. Follow the link to load `pgagent_15-4.2.2-3.rhel7.x86_64.rpm` package.
13. Install the package using the command:

```
yum install pgagent_15-4.2.2-3.rhel7.x86_64.rpm
```

14. Change the default password for database administrator:

```
su - postgres
psql -p 5433
alter user postgres password 'xxXX1234';
```

15. Create all required extensions 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 pgagent;
```

16. To exit, enter the commands:

```
\q
exit
```

17. To configure `pgagent` user in 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
```

18. Create `/etc/sudoers.d/iw-pgagent` file with the following content:

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

19. Change the privileges, owner and group as per `/etc/sudoers.d/iw-pgagent` :

```
chmod 440 /etc/sudoers.d/iw-pgagent
chown root:root /etc/sudoers.d/iw-pgagent
```

20. Edit the configuration file `/etc/pgagent/pgagent_15.conf` using the commands:

```
sed -i --follow-symlinks "s/DBPORT=5432/DBPORT=5433/" /etc/pgagent/pgagent_15.conf
echo "LD_LIBRARY_PATH=/opt/pgpro/ent-15/lib" >> /etc/pgagent/pgagent_15.conf
```

21. Enable the service `pgagent` , run it and check its status using the commands:

```
systemctl enable pgagent_15
systemctl start pgagent_15
systemctl status pgagent_15
```

22. Create `/u02` directory:

```
mkdir /u02
```

23. Mount the disk storage into `/u02` directory.
24. Create directories for tablespaces, change the owner and group to `postgres` :

```
mkdir /u02/pgdata
mkdir /u02/pgdata1
mkdir /u02/arch
chown -R postgres:postgres /u02
```

Once you have configured the database, make sure that there are no critical errors in `/var/log/pgagent_15.log` and the database logs.

2.4.3 Configuring Jatoba

To prepare a remote database for installation of Traffic Monitor components, follow these steps on the database server:

1. Install an additional package using the command:

```
yum -y install jatoba5-contrib
```

2. Create a new file `/etc/systemd/system/jatoba-5.service.d/override.conf` or add the following content to the existing file:

```
[Service]
Environment=PGDATA=/u01/postgres
```

3. Apply service configuration changes by running the command:

```
systemctl daemon-reload
```

4. Create directories for files and archives, change directory owner and group to `postgres`. Use the commands:

```
mkdir -p /u01/postgres
chown postgres:postgres /u01/postgres
mkdir -p /u02/pgdata
mkdir -p /u02/pgdata1
mkdir -p /u02/arch
chown -R postgres:postgres /u02
```

5. Initialize the database. For this:
   a. Go to `/usr/jatoba-5/bin/`:

```
cd /usr/jatoba-5/bin/
```

   b. Use the initialization command:

```
PGSETUP_INITDB_OPTIONS=" --encoding=UTF8" ./jatoba-setup initdb jatoba-5 --
encoding=UTF8 --locale=en_US.UTF-8 -D /u01/postgres
```

6. Create a temporary directory and change its owner and group to `postgres`. Use the commands:

```
mkdir -p /u01/postgres/tmp
chown postgres:postgres /u01/postgres/tmp
```

> **Important!**
>
> You can create the temporary directory only *after* the database initialization.

7. In `/u01/postgres/` directory, create `iwtm-postgres.conf` configuration file:

```
touch /u01/postgres/iwtm-postgres.conf
```

8. To `iwtm-postgres.conf` file, add 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                     # min 128KiB

huge_pages = try                        # on, off, or try

max_locks_per_transaction = 256
temp_buffers = MB
work_mem = MB
effective_cache_size = MB

min_wal_size = MB
max_wal_size = MB
lc_messages = 'en_US.UTF-8'             # Locale for system error message
log_directory = 'pg_log'
log_filename = 'postgresql.log'         # Log file name pattern
log_rotation_age = 0                    # Automatic rotation of logfiles will happen
after that time. 0 disables.
log_rotation_size = 0                   # Automatic rotation of logfiles will happen
after that much log output. 0 disables.
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

autovacuum_max_workers = 5
autovacuum_naptime = 20
max_parallel_maintenance_workers = 8
maintenance_work_mem = MB
```

```
autovacuum_freeze_max_age = 1000000000

shared_preload_libraries = 'pg_stat_statements'
track_io_timing = on
track_activity_query_size = 32768

constraint_exclusion = off                # on, off, or partition
standard_conforming_strings = on
```

Important!

In the sample configuration file above, fields for the following parameters are empty:

- `shared_buffers`
- `work_mem`
- `maintenance_work_mem`
- `effective_cache_size`
- `temp_buffers`
- `min_wal_size`
- `max_wal_size`

Configure the parameters in accordance with *official PostgreSQL instructions*.

9. Change the configuration file and group owner to `postgres`:

```
chown postgres:postgres /u01/postgres/iwtm-postgres.conf
```

10. To `/u01/postgres/`**`postgresql.conf`** configuration file, add a link to **`iwtm-postgres.conf`**. Use the command:

```
echo "include = 'iwtm-postgres.conf'" >> /u01/postgres/postgresql.conf
```

11. Configure **`pg_hba.conf`** access file 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
```

12. Activate the DBMS as described in Jatoba DBMS Installation Guide.
13. Run `jatoba-5` service and check its status. Use the commands:

```
systemctl enable jatoba-5
```

```
systemctl start jatoba-5
systemctl status jatoba-5
```

14. Install pgAgent from OS repository. Use the command:

```
yum install pgagent_15
```

15. Move the files for installation of extensions from **`postgresql-15`** directory to **`jatoba-5`**. For this:
    a. Go to `/usr/pgsql-15/`**`share`**`/` :

```
cd /usr/pgsql-15/share
```

    b. Use the commands to change directories:

```
cp -R pgagent_15-x.x.x /usr/jatoba-5/share/
cp extension/* /usr/jatoba-5/share/extension/
```

> **Important!**
>
> In the first command, replace `pgagent_15-x.x.x` with the exact name of the catalogue from `/usr/jatoba-5/share/` directory. For example, `pgagent_15-4.0.0`.

16. Change the default password for the database administrator. Use the commands:

```
su - postgres
psql -p 5433
alter user postgres password 'xxXX1234';
```

17. Create extensions by running the requests:

```
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 pgagent;
```

18. To exit, enter the commands:

```
\q
exit
```

19. To configure pgAgent user in the OS, run the commands:

```
mkdir /home/pgagent
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
```

20. Create or edit `/etc/sudoers.d/pgagent` file, so that the content looks as follows:

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

21. For `/etc/sudoers.d/pgagent` file, change owner and group by running:

```
chmod 440 /etc/sudoers.d/pgagent
chown root:root /etc/sudoers.d/pgagent
```

22. In `/etc/pgagent/pgagent_15.conf` configuration file, change the value of `DBPORT` parameter from `5432` to `5433`:

```
sed -i --follow-symlinks "s/DBPORT=5432/DBPORT=5433/" /etc/pgagent/pgagent_15.conf
```

23. Run `pgagent_15` service and check its status. Use the commands:

```
systemctl enable pgagent_15
systemctl start pgagent_15
systemctl status pgagent_15
```

Once you have configured the database, make sure there are no critical errors in `/var/log/pgagent_15.log` and database logs.

2.4.4 Configuring Tantor

To prepare a remote database for installation of Traffic Monitor components, follow these steps on the database server:

1. Stop `tantor-be-server-15` service with the command below:

```
systemctl stop tantor-be-server-15.service
```

2. To `/var/lib/postgresql/tantor-be-15/data/` directory, copy the existing **`iwtm-postgres.conf`** configuration file or create a new one with the following contents:

```
# ----------------------------
# Tantor 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 = 128kB

huge_pages = try                        # on, off, or try

max_locks_per_transaction = 512
temp_buffers = 32MB
work_mem = 16MB
effective_cache_size = 4096MB

min_wal_size = 6144MB
max_wal_size = 6144MB
lc_messages = 'en_US.UTF-8'             # locale for system error message
log_directory = 'pg_log'
log_filename = 'postgresql.log'         # log file name pattern
log_rotation_age = 0                    # Automatic rotation of logfiles will happen
after that time. 0 disables.
log_rotation_size = 0                   # Automatic rotation of logfiles will happen
after that much log output. 0 disables.
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 = '/var/lib/postgresql/tantor-be-15/data/pg_stat_tmp'

autovacuum_max_workers = 5
autovacuum_naptime = 20
maintenance_work_mem = 1GB
autovacuum_freeze_max_age = 1000000000

#shared_preload_libraries =  'pg_stat_statements'
track_io_timing = on
track_activity_query_size = 32768
```

```
constraint_exclusion = off                # on, off, or partition
standard_conforming_strings = on
```

Important!

In the sample configuration file above, the values for the following parameters are exemplary:

- `shared_buffers`
- `work_mem`
- `maintenance_work_mem`
- `effective_cache_size`
- `temp_buffers`
- `min_wal_size`
- `max_wal_size`

Configure the parameters for your system as described in the *official PostgreSQL instruction*.

3. Assign rights for **`iwtm-postgres.conf`** file to `postgres` user.

```
chown postgres:postgres /var/lib/postgresql/tantor-be-15/data/iwtm-postgres.conf
```

4. To `/var/lib/postgresql/tantor-be-15/data/`**`postgresql.conf`** configuration file, add a link to **`iwtm-postgres.conf`**.
Use the command:

```
echo "include = 'iwtm-postgres.conf'" >> /var/lib/postgresql/tantor-be-15/data/
postgresql.conf
```

5. Edit `/var/lib/postgresql/tantor-be-15/data/`**`pg_hba.conf`** access file:
   a. After these lines:

```
# IPv6 local connections: host    all
all             ::1/128                 md5
```

   add the line:

```
host    postgres        all             0.0.0.0/0               md5
```

Note:

Use the values specified in the line above if you want to install Traffic Monitor with default parameters. Otherwise, specify different parameters here.

   b. Change lines using the commands:

```
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*127.0.0.1/32[[:space:]]*md5|
host    all             all             127.0.0.1/32            trust|" /var/lib/
postgresql/tantor-be-15/data/pg_hba.conf
sed -i "s|local[[:space:]]*all[[:space:]]*all[[:space:]]*peer|local   all
  all                                     trust|" /var/lib/postgresql/tantor-be-15/
data/pg_hba.conf
```

6. Create `/var/lib/pgpro/ent-15/data/tmp` directory and assign owner and group to it. Use the commands:

```
mkdir –p /var/lib/postgresql/tantor-be-15/data/tmp
chown postgres:postgres /var/lib/postgresql/tantor-be-15/data/tmp
```

7. Install pgAgent:
   a. Start Tantor service:

```
systemctl start tantor-be-server-15.service
```

   b. Download `pgagent_15-4.2.2-3.rhel7.x86_64.rpm` package from *Yum repository*.
   c. Install the package:

```
yum install pgagent_15-4.2.2-3.rhel7.x86_64.rpm
```

8. Copy the extension files:

```
cp /usr/pgsql-15/share/extension/pgagent* /opt/tantor/db/15/share/postgresql/extension/
```

9. Switch user to `postgres`:

```
su - postgres
```

10. Connect to the database:

```
psql -p 5433
```

11. Change default password for database administrator:

```
alter user postgres with password 'xxXX1234';
```

12. Create required extensions by running the requests:

```
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 pgagent;
```

13. To exit, enter the commands:

```
\q
exit
```

14. To configure pgAgent user in the OS, run the commands:

```
mkdir /home/pgagent/
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
```

15. Create `/etc/sudoers.d/iw-pgagent` file with the following content:

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

    You can do this with the commands:

```
touch /etc/sudoers.d/iw-pgagent
echo "# allow pgagent to execute any command" > /etc/sudoers.d/iw-pgagent
echo "pgagent ALL = (postgres) NOPASSWD: ALL" >> /etc/sudoers.d/iw-pgagent
echo 'Defaults:pgagent !requiretty' >> /etc/sudoers.d/iw-pgagent
```

16. Change permissions, owner and group for `/etc/sudoers.d/iw-pgagent` file by running:

```
chmod 440 /etc/sudoers.d/iw-pgagent
chown root:root /etc/sudoers.d/iw-pgagent
```

17. Edit `/etc/pgagent/pgagent_15.conf` configuration file with the commands:

```
sed -i --follow-symlinks "s/DBPORT=5432/DBPORT=5433/" /etc/pgagent/pgagent_15.conf
echo "LD_LIBRARY_PATH=/opt/tantor/db/15/lib/" >> /etc/pgagent/pgagent_15.conf
```

18. Enable pgAgent service, start it and check its status. Use the commands:

```
systemctl enable pgagent_15
systemctl start pgagent_15
systemctl status pgagent_15
```

19. Create `/u02` directory:

```
mkdir /u02
```

20. Create directories for tablespaces and change owner and group to `postgres`:

```
mkdir /u02/pgdata
mkdir /u02/pgdata1
mkdir /u02/arch
chown -R postgres:postgres /u02
```

Once you have configured the database, make sure there are no critical errors in `/var/log/**pgagent_15.log**` and database logs.

3 Installing the System

This section contains instructions for each type of System installation.

You can find the instruction for installation of the external storage of binary data – Data Storage in the *Installing Data Storage* article.

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.

Note:

Traffic Monitor installation is not supported when connecting to server via HP Integrated Lights Out (ILO).

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 parameters 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.

Note:

InfoWatch Device Monitor installation is described in *InfoWatch Device Monitor. Installation, Configuration and Administration Guide*.

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 or a PostgreSQL-based 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, uninstall 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 Data Storage

External storage of binary data - Data Storage - is a part of Platform. To use Data Storage, install Platform.

If Traffic Monitor is not already installed:

1. Install Platform. You can do it in one of the following ways:
    - Install Platform without products. This type of installation is described in the following articles:

a. Preparing the Server
b. Installing Platform

- Install a Platform product. In this case Platform will be installed automatically.
  You can find installation description in this product documentation. Also there you can find information about possibility of installing Traffic Monitor and the Platform product on the same server.

2. Install Traffic Monitor. During the installation, specify parameters of connection to Data Storage. One of these parameters is the Data Storage authorization token.

> **Warning!**
>
> To improve security, it is not recommended to use the default value of the token.

You can check the actual value of the token:

- On the Data Storage server, via the command line. For this:
  a. Go to the directory where the Platform distribution kit was extracted.
  b. Run the command:
  `./setup.py tokens list`
  As a result, you will see a list of tokens for connecting to the Platform. The actual Data Storage authorization token will be displayed opposite the *DataStorageUser* identity.
  c. If the token has the default value: `1exwo92iwpczl1hy6jxy`, refresh it by running the command:
  `./setup.py tokens refresh DataStorageUser`
- In the Platform product management console, in the **Token for Data Storage User** field of the **Global settings** section.
  It is available if the Platform product with web interface is installed on the server with Data Storage and the web interface contains such a setting.
  In this case, you can refresh the token by pressing the  button.

3. If Platform is installed on the server where Traffic Monitor was already installed, make sure that IP address of the Traffic Monitor server is specified in the `/opt/iw/tm5/etc/consul/consul.json` configuration file, in the " `bind_addr` " field.

If Traffic Monitor was installed before Data Storage:

1. Install Platform. See step 1 above.
2. Configure the connection between Traffic Monitor and Data Storage. For the details, see *InfoWatch Traffic Monitor. Administration Guide. Configuring Connection with Data Storage*.

> **Note:**
>
> You can configure the connection between Traffic Monitor and Data Storage in case of All-in-one installation type or server installation with the help of Database template.

3. If Platform is installed on the same server with Traffic Monitor, make sure that IP address of the Traffic Monitor server is specified in the `/opt/iw/tm5/etc/consul/consul.json` configuration file, in the " `bind_addr` " field.

3.1.1 Preparing the Server

Before installing Platform, you need to prepare the server:

1. **On a server running MOS OS:**

   Make sure that the official OS repositories are available:

   - `software`
   - `update`
   - `oss`
2. The installation program is written in Python version 2.7. So to install the Platform, you need to install the Python 2.7 interpreter first. The distribution kit does not include the interpreter package.
3. **In the Red Hat Enterprise Linux and RED OS environments, configure SELinux.**

   For the correct operation of `containerd`, **update** the SELinux policies or **disable** the access control system:

   - **To update the SELinux policies**, download and install the package `container-selinux`. You can do it with the command:

     ```
     yum install container-selinux
     ```

     > **Note:**
     >
     > The package is not included in the product's distribution kit.
     >
     > The package may be missing in the repositories. In this case, download and install it manually.

   - **To disable SELinux**:
     a. Run the following commands on behalf of the `root` superuser:

        ```
        setenforce 0
        sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config
        ```

     b. Reboot the server with the command:

        ```
        reboot
        ```

     c. Check the status of the SELinux system with the command:

        ```
        sestatus
        ```
4. Configure the POD network rules or disable the firewall (see *Firewalld and Kubernetes interaction conflicts* and *Firewall complete shutdown*). Otherwise, you will not be able to install the Platform.
5. If you are using an antivirus, configure it to work with the Platform (see *Antivirus configuration for Platform products*).

6. The Platform uses the Kubernetes component. For the correct installation of the Platform and operation of the Kubernetes, the `conntrack` package should be installed on the server. Make sure that the package is installed. For this, in the command line, enter:

```
conntrack
```

You will see information about working with the `conntrack` module and the module version.

```
Command line interface for the connection tracking system. Version 1.4.4
Usage: conntrack [commands] [options]

Commands:
  -L [table] [options]          List conntrack or expectation table
  -G [table] parameters         Get conntrack or expectation
  -D [table] parameters         Delete conntrack or expectation
  -I [table] parameters         Create a conntrack or expectation
  -U [table] parameters         Update a conntrack
  -E [table] [options]          Show events
  -F [table]                    Flush table
  -C [table]                    Show counter
  -S                            Show statistics

Tables: conntrack, expect, dying, unconfirmed

Conntrack parameters and options:
  -n, --src-nat ip                      source NAT ip
  -g, --dst-nat ip                      destination NAT ip
  -j, --any-nat ip                      source or destination NAT ip
  -m, --mark mark                       Set mark
  -c, --secmark secmark                 Set selinux secmark
  -e, --event-mask eventmask            Event mask, eg. NEW,DESTROY
  -z, --zero                            Zero counters while listing
  -o, --output type[,...]               Output format, eg. xml
  -l, --label label[,...]               conntrack labels

Expectation parameters and options:
  --tuple-src ip        Source address in expect tuple
  --tuple-dst ip        Destination address in expect tuple

Updating parameters and options:
  --label-add label     Add label
  --label-del label     Delete label

Common parameters and options:
  -s, --src, --orig-src ip              Source address from original direction
  -d, --dst, --orig-dst ip              Destination address from original direct
ion
  -r, --reply-src ip            Source addres from reply direction
  -q, --reply-dst ip            Destination address from reply direction
  -p, --protonum proto          Layer 4 Protocol, eg. 'tcp'
  -f, --family proto            Layer 3 Protocol, eg. 'ipv6'
  -t, --timeout timeout         Set timeout
  -u, --status status           Set status, eg. ASSURED
  -w, --zone value              Set conntrack zone
  --orig-zone value             Set zone for original direction
  --reply-zone value            Set zone for reply direction
  -b, --buffer-size             Netlink socket buffer size
  --mask-src ip                 Source mask address
  --mask-dst ip                 Destination mask address
```

If the module is not installed, install it using the following command:

- **Red Hat Enterprise Linux**, **Oracle Linux**, **RED OS:**

  ```
  yum install conntrack
  ```

- **Alt Server:**

  ```
  apt-get install conntrack-tools
  ```

- **MOS OS:**

```
zypper install conntrack-tools
```

If the package is not available in the repository, then download it, go to the directory with the package, and install it manually using the command:

- **Red Hat Enterprise Linux, Oracle Linux, RED OS:**

```
rpm -Uhv ./<package_name>
```

- **Alt Server:**

```
rpm -Uhv ./<package_name>
```

- **MOS OS:**

```
zypper install <package_name>
```

7. **On a server running MOS OS:**

   Install the packages `socat`, `ethtool`, `app_armor`, and `sysctl` with dependencies:

```
zypper install socat
zypper install ethtool
zypper install patterns-base-apparmor
zypper install procps
zypper install libprocps7
```

8. **On a server running Alt Server:**

   Install the packages:

   - `python-modules-json`
   - `python-modules-distutils`
   - `python-modules-sqlite3`

9. **If you are installing the Platform on the server where Traffic Monitor with a local database is already installed, then disable Huge Pages. For this:**

   a. Stop the System by running the command:

```
iwtm stop
```

   b. Stop the DBMS.

   - If you are using PostgreSQL on a computer running Red Hat Enterprise Linux, RED OS, or Oracle, run the following commands:

```
systemctl stop pgagent-15
systemctl stop postgresql-15
```

   - If you are using PostgreSQL on a computer running Alt Server, run the following commands:

```
systemctl stop pgagent
systemctl stop postgresql
```

- If you are using Oracle DBMS:
  i. Open Oracle SQL*Plus and connect as the **sysdba** user:

```
sqlplus / as sysdba
```

  ii. Run the command:

```
dbshut $ORACLE_HOME
```

c. Set the *Huge Pages* parameter to zero:
- `In the file /etc/sysctl.conf`, insert the line:

```
vm.nr_hugepages=0
```

- Save and apply the changes by running the command:

```
sysctl -p
```

> **Note:**
>
> To view the current value of *Huge Pages,* run the command:
>
> ```
> sysctl -a | grep 'huge*page'
> ```

d. Start the DBMS:
- If you are using PostgreSQL on computers running Red Hat Enterprise Linux, RED OS, or Oracle, run the following commands:

```
systemctl start pgagent-15
systemctl start postgresql-15
```

- If you are using PostgreSQL on computers running Alt Server, run the following commands:

```
systemctl start pgagent
systemctl start postgresql
```

- If you are using Oracle DBMS:
  i. Open Oracle SQL*Plus and connect as the **sysdba** user:

```
sqlplus / as sysdba
```

ii. Run the command:

```
dbstart $ORACLE_HOME
```

e. Start the System:

```
iwtm start
```

3.1.2 Installing Platform

Important!

Before the installation, be sure to prepare the server (see *Preparing the Server*).

Platform is installed manually via the command line.

To install the Service, use the `iw_platform.tar.xz` archive from the Traffic Monitor distribution kit. The archive contains a full set of binary modules of container images that are necessary for deploying Platform without access to the Internet. The archive also includes the installation program.

Platform have two installation modes:

- **`central` (central node)**
- **`office` (office node)**

The central and office nodes of the Platform are combined into a cluster.

Installation in the central mode

To install Platform in the `central` mode:

1. Follow the steps to prepare the server for installing Platform (see *Preparing the Server*).

Note:

During installation the installer will check the availability of:

- at least 100 GB on the hard drive for each directory that you will specify in steps 9-12. If the directories for data storing are located on different disks then the installer will check the availability of 100 GB of free space on each of them;
- at least 20 GB on the disk for directories with images;
- at least 8 GB of RAM;
- at least 2 processor cores;

- support for SSE 4.2 instructions;
- the installed **`conntrack`** package.

2. Create a new directory on the disk (e.g. Platform):
`mkdir Platform`
3. Copy the **`iw_platform.tar.xz`** archive to this directory.
4. Open the directory where you have pasted the archive.
5. Unpack the archive with Platform distribution kit to this directory:
`tar -xvf iw_platform.tar.xz`
6. Run the Platform installation program:
`./setup.py install`
If necessary, specify additional parameters:
   - For archiving daily tablespaces, specify the path to the slow disk of the Data Storage server. When archiving, the System will move binary data there. For this, run the Platform installation program with the `--dsslowdatapath` parameter:
`./setup.py install --dsslowdatapath=/root/slowdisk`
where `/root/slowdisk` is the path to the slow disk.
For details on archiving tablespaces, see *InfoWatch Traffic Monitor. Administration Guide. Archiving Daily Tablespaces*;
   - To enable Data Storage backuping, run the Platform installation program with the `--dsbackupspath` parameter:
`./setup.py install --dsbackupspath=/opt/dsbackups`
where `/opt/dsbackups` is the path to the storage of backups.
For details on backuping Data Storage, see *InfoWatch Traffic Monitor. Administration Guide. Creating Data Storage Backup*.
7. Enter the IP address of the network interface to communicate with the cluster and press **Enter**.
The IP address should be in IPv4 format: "`xxx.xxx.xxx.xxx`".

> **Note:**
>
> If you specify `0.0.0.0` as the IP address, then all available network interfaces will be used.
>
> Hereinafter, to use the default values, press **Enter** without entering values.

8. Allocate RAM to host Clickhouse data (by default, `80%`) and press **Enter**.
9. Specify the path to place Clickhouse data (by default, `/opt/chdata`) and press **Enter**.
10. Specify the path to place PostgreSQL data (by default, `/opt/pgdata`) and press **Enter**.
11. Specify the path to place NATS data (by default, `/opt/natsdata`) and press **Enter**.
12. Specify the path to place binary data (by default, `/opt/dsdata`) and press **Enter**.
13. Specify the path to temporarily place Traffic Monitor events before uploading them into the Platform (by default, `/opt/factsldrtmdata`) and press **Enter**.
14. Specify the port for connecting to the Platform web interface and press **Enter**.

> **Important!**
>
> When installing on the same server with Traffic Monitor, specify port different than 443 because port 443 is used by default for connecting to the Traffic Monitor web interface.

15. Wait for the installation of Platform to complete.

16. Read the Platform installation report. The **web ui** column contains the address and port to connect to the Platform web interface:

```
###Result###
Install product: Infowatch Platform(platform)
Install manifest section: central
Install node label: central
installed 41 components
updated   0 components
add ref   0 components
web ui:
https://10.60.25.54:444
```

17. To display information about Platform, use the command:
`./setup.py showproducts`
18. Make sure that all services are running. For this, use the command:
`kubectl get pods -n infowatch`
The list of services will be displayed. Each service should have the `Running` status.

Installation in the office mode

To install Platform in the `office` mode:

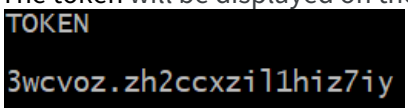
1. Follow the steps to prepare the server for installing Platform (see *Preparing the Server*).

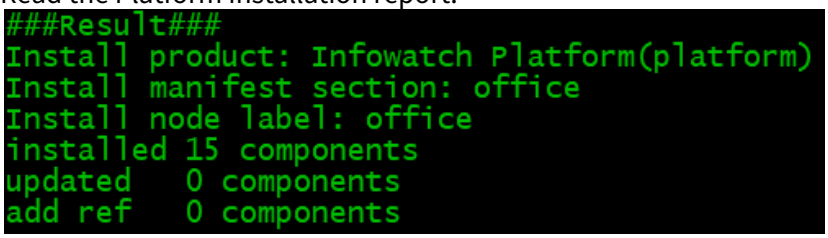
> **Note:**
>
> During installation the installer will check the availability of:
>
> - at least 100 GB on the hard drive for each directory that you will specify in steps 11-14. If the directories for data storing are located on different disks then the installer will check the availability of 100 GB of free space on each of them;
> - at least 20 GB on the disk for directories with images;
> - at least 8 GB of RAM;
> - at least 2 processor cores;
> - support for SSE 4.2 instructions;
> - the installed **conntrack** package.

2. Create a new directory on the disk (e.g. Platform):
`mkdir Platform`
3. Copy the **iw_platform.tar.xz** archive to this directory.
4. Open the directory where you have pasted the archive.
5. Unpack the archive with Platform distribution kit to this directory:
`tar -xvf iw_platform.tar.xz`
6. Run the Platform installation program:
`./setup.py install --nodemode=office`
If necessary, specify additional parameters:
   - For archiving daily tablespaces, specify the path to the slow disk of the Data Storage server. When archiving, the System will move binary data there. For this, run the Platform installation program with the `--dsslowdatapath` parameter:
   `./setup.py install --nodemode=office --dsslowdatapath=/root/slowdisk`
   where `/root/slowdisk` is the path to the slow disk.

For details on archiving tablespaces, see *InfoWatch Traffic Monitor. Administration Guide. Archiving Daily Tablespaces*;

- To enable Data Storage backuping, run the Platform installation program with the `--dsbackupspath` parameter:
  `./setup.py install --nodemode=office --dsbackupspath=/opt/dsbackups`
  where `/opt/dsbackups` is the path to the storage of backups.
  For details on backuping Data Storage, see *InfoWatch Traffic Monitor. Administration Guide. Creating Data Storage Backup*.

7. Enter the address of the central node. You can specify it as an IP address or domain name (e.g., `192.0.2.0` or `host.example.com`).
8. Specify a token to connect to the central node.
   To get the token:
   a. Connect to the central node server.
   b. On the server command line, run the following command to get the token:
      `kubeadm token list`
      The token will be displayed on the screen:
      

      Here the token is as follows: `3wcvoz.zh2ccxzil1hiz7iy`
9. Specify the node label (the default value is `office`) and press **Enter**.
   The label may consist of letters of the Latin alphabet and/or numbers. Label length must not exceed 32 characters.
10. Allocate RAM to host Clickhouse data (by default, `80%`) and press **Enter**.
11. Specify the path to place Clickhouse data (by default, `/opt/chdata`) and press **Enter**.
12. Specify the path to place PostgreSQL data (by default, `/opt/pgdata`) and press **Enter**.
13. Specify the path to place NATS data (by default, `/opt/natsdata`) and press **Enter**.
14. Specify the path to place binary data (by default, `/opt/dsdata`) and press **Enter**.
15. Specify the path to temporarily place Traffic Monitor events before uploading them into the Platform (by default, `/opt/factsldrtmdata`) and press **Enter**.
16. Wait for the installation of the Platform to complete.
17. Read the Platform installation report.
    

18. To display information about Platform, use the command:
    `./setup.py showproducts`
19. Make sure that all services are running. For this, use the command:
    `kubectl get pods -n infowatch`
    The list of services will be displayed. Each service should have the `Running` status.

After installing Platform, follow the further instructions in the *Installing Data Storage* article.

See also in this section:

- Installing Platform with Parameters Speficied in the Command Line.

Installing Platform with Parameters Speficied in the Command Line

With Platform installer, you can install it with minimum operations performed by the user. For this, specify all the required parameters in the command line.

Before running the Platform installer:

1. Make sure your server meets the hardware and software requirements (see *Hardware and Software Requirements*).
2. Complete the steps to prepare your server for Platform installation (see *Preparing the Server*).
3. Create a new directory on the disk (such as `Platform`):

   ```
   mkdir Platform
   ```

4. Copy the **`iw_platform.tar.xz`** archive to this directory.
5. Go to the directory with the copied archive.
6. Unpack the archive to this directory:

   ```
   tar -xvf iw_platform.tar.xz
   ```

Check the list of keys from the table below. You can use them to specify product installation parameters for the installer.

Key	Description
`--nodemode`	The mode of installation: `central` or `office`. To install the Platform in the office mode, specify the `office` value for this parameter. For the installation in the central mode, you do not need to specify this parameter
`--advertise`	IP address of the network interface to communicate with the cluster. The default value: `0.0.0.0` Do not specify in case of installation in the office mode
`--chmemsize`	Amount of RAM used for ClickHouse data **Available values:** • `1` - `100%` or a numeric value If you do not specify `%`, then the specified value will be treated as the volume in GB
`--disable-check-free-disk`	Disabling the check of availability of free space on the disk: • 20 GB for storing images; • 100 GB for storing data in the directories specified above **Note**: If the directories for storing data are located on different disks then the installer will check the availability of 100 GB of free space on each of them

Key	Description
`--disable-check-total-ram`	Disabling the check of availability of 8 GB of RAM on the computer
`--chdbpath`	Path for placing Clickhouse data
`--pgdbpath`	Path for placing PostgreSQL data
`--natspath`	Path for placing NATS data
`--dsdatapath`	Path for placing binary data
`--factsldrtmdatapath`	Path for temporary placing Traffic Monitor events before loading them into the Platform
`--advertise`	IP address of the network interface on which the `kubelet` service is running. Specify the value when installing the Platform central node.
`--guiport`	The port for connecting to the web interface. The default value: `443.` Do not specify in case of installation in the office mode. **Important!** When installing on the same server with Traffic Monitor, specify port different than 443 because port 443 used by default for connecting to the Traffic Monitor web interface
`--cluster`	Address of the Platform central node in the cluster. Specify the value when installing the Platform office node.

`--clustertoken`	The token to connect to the Platform central node.
	To get the token, in the Platform central node terminal, run the command:
	`kubeadm token list`
	You can create a token using the command:
	`kubeadm token create`
	Specify the value when installing the Platform office node.

`--nodelabel`	Label of the Platform node (unique within the cluster). The default value for the office node is `office`. If the cluster has more than one office node, specify unique labels.

Key	Description
`--dsslowdatapath`	Path to the slow disk of the Data Storage server. When archiving daily tablespaces, the System will move binary data there. Example: `--dsslowdatapath=/root/slowdisk` For details on archiving tablespaces, see *InfoWatch Traffic Monitor. Administration Guide. Archiving Daily Tablespaces*.
`--dsbackupspath`	Path to the storage of backups. Specify it to enable Data Storage backuping. Example: `--dsbackupspath=/opt/dsbackups` For details on backuping Data Storage, see *InfoWatch Traffic Monitor. Administration Guide. Creating Data Storage Backup*.

To install Platform:

1. Run the Platform installation program and specify the parameters.
   Example of a command for installing the Platform central node:

   ```
   ./setup.py install \
   --advertise=0.0.0.0 \
   --chmemsize=60% \
   --chdbpath=/opt/chdata \
   --pgdbpath=/opt/pgdata \
   --natspath=/opt/natsdata \
   --dsdatapath=/opt/dsdata \
   --factsldrtmdatapath=/opt/factsldrtmdata \
   --guiport=444 \
   --dsslowdatapath=/root/slowdisk
   ```

   If you have not specified values for any required parameters, the installer will start the interactive mode and ask you to specify them. See *Installing Platform* for details.
2. Wait for installation to complete.
3. To display the information about the Platform, run the command:

   ```
   ./setup.py showproducts
   ```

4. Make sure that all services are running. To do this, use the command:

   ```
   kubectl get pods -n infowatch
   ```

   The command displays the list of services. Each service should have the status `Running`.

3.2 Installing Traffic Monitor Server and Database

You can find information on installing Traffic Monitor on OS Red Hat Enterprise Linux, Oracle Linux, AlmaLinux and Rocky Linux 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

3.2.1 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 similar to all templates installation on the same computer. The packages unpack will start before the installation process after all the parameters 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 (deployed locally or on a separate server), you should *prepare* it first.
   >
   > Before installing, in order to clear memory, it is recommended to reboot the server on which database will be deployed.

2. Connect external or local OS repositories.
   For example, you can find instructions on how to configure local Red Hat Enterprise Linux repository at the *official web page*.
   Find instructions on preparing the server for offline System installation on Oracle Linux 7 in *Configuring Local Repositories*.
3. **If you install Traffic Monitor on Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS:**

   > **Warning!**

Make sure that, in Oracle Linux 8.10 operating system, the current kernel is Red Hat Compatible Kernel (RHCK), for example, Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`, and the UEK kernel is removed. For details, see *Operating System and Network Server Configuration Requirements*.

a. Install the `redhat-lsb-core` package by running the following command:

```
dnf install redhat-lsb-core
```

b. Create a backup copy of the OS release file and replace the content of the original file. For this, run the commands depending on OS:
   - in Oracle Linux 8:

```
cp /etc/oracle-release /etc/release.bak

echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/oracle-release
```

   - in AlmaLinux 8 or Rocky Linux 8:

```
cp /etc/redhat-release /etc/release.bak
echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/redhat-release
```

c. Run the command:

```
lsb_release -a
```

As a result, the following information should be displayed:

```
Distributor ID: RedHatEnterprise
Description:    Red Hat Enterprise Linux release 8.10 (Ootpa)
Release:        8.10
Codename:       Ootpa
```

> **Note:**
>
> After installing Traffic Monitor, recover the original OS release file. For details, see *below*.

4. 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`
5. Copy the files from InfoWatch Traffic Monitor distributive – installer and archive with DBMS components – into the created directory:

OS	Distribution files
Red Hat Enterprise Linux 7	**Installer**: `iwtm-installer-x.x.x.xxx-rhel7`

OS	Distribution files

Oracle Linux 7 [4]	**Archive with DBMS components** [1] [2]:
	PostgreSQL:
	`iwtm-postgresql-15.14-x.x.x.xxx-rhel7.tar.gz`
	Oracle [3]:
	`iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz`

RED OS	**Installer**:
	`iwtm-installer-x.x.x.xxx-redos-7.3`
	Archive with DBMS components [1] [2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-redos-7.3.tar.gz`

Red Hat Enterprise Linux 8
Oracle Linux 8
AlmaLinux 8
Rocky Linux 8
	Installer:
	`iwtm-installer-x.x.x.xxx-rhel8`
	Archive with DBMS components [1] [2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-rhel8.tar.gz`

Alt Server	**Installer**:
	`iwtm-installer-x.x.x.xxx-altlinux-10`
	Archive with DBMS components [1] [2]:
	`iwtm-postgresql-15.10-x.x.x.xxx-altlinux-10.tar.gz.md5`

Important!

[1] Archive with DBMS components is required *both* when installing DBMS distributed with the product (`local` mode) *and* when using an already deployed DBMS in *remote* mode. See *System Deployment Schemes and Installation Types* for details.

[2] In case you are planning to use an already deployed PostgreSQL-based DBMS, use an archive from PostgreSQL column. For the list of supported PostgreSQL-based DBMS, see *Hardware and Software Requirements*.

[3] If you use Oracle DBMS and network file system (NFS), before launching the installer:

- **When using Oracle Real Application Clusters (RAC):**

  Set the options for mounting in accordance to *the article on the official site*.

- **When not using RAC:**

  Open settings of the mount point (by default, `/etc/fstab`) and make sure that the `noac` option is not used and the `actimeo` parameter has the `0` value.

For details, see *the article on the official site*.

[4] For Traffic Monitor installed on a server running Oracle Linux 7, Postgres Pro Enterprise DBMS is not supported.

Installation using distributive files for Red Hat Enterprise Linux 7 will be described further. In our example, we need to copy an installer file and an archive with DBMS components:

- Installer:
  `iwtm-installer-7.15.0.97-rhel7`
  where `7.15.0.97` is the build number, `rhel7` is the OS designation;
- Archive with DBMS components:
  - In case of PostgreSQL (or one of supported PostgreSQL-based DBMS):
    `iwtm-postgresql-15.14-7.15.0.97-rhel7.tar.gz`
    where `postgresql-15.14` is the DBMS designation, `7.15.0.97` is the build number, `rhel7` is the OS designation;
  - In case of Oracle DBMS:
    `iwtm-oracle-19.0.0.0.0-7.15.0.97.tar.gz`
    where `oracle-19.0.0.0.0` is the DBMS designation, `7.15.0.97` is the build number.

This instruction is relevant for other supported OS: Oracle Linux, RED OS, AlmaLinux, Rocky Linux and Alt Server.

6. Enter the command to shift to Traffic Monitor distributive directory.
   As per our example:
   `cd /distr`
7. 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-7.15.0.97-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-7.15.0.97-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:

```
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 OS 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 welcoming window will be displayed:



2. You must accept the terms of the License Agreement before continuing with the installation. Select one of the following options. For this, type the figure specified next to it and press **Enter**:
   - `Show the License Agreement` - to view the License Agreement;
     If this option is selected:
     a. Select language to display the License Agreement:
        - `English`
        - `Russian`
     b. Read the License Agreement. To go to the next page, press **Enter**.
     c. Accept the License Agreement. For this, type **y** and press **Enter**.
   - `I accept the License Agreement` – to accept the License Agreement without preview;
   - `I do not accept the License Agreement` – to not accept the License Agreement and abort the installation process.

     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] Show the License Agreement` will be selected.

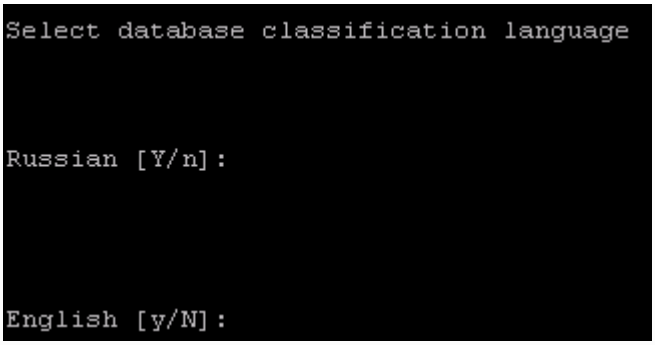
3. Select Traffic Monitor edition type:
   - `Traffic Monitor Enterprise (TME)` to install Enterprise edition;
   - `Traffic Monitor Standard (TMS)` to install Standard edition.

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

4. If `Traffic Monitor Enterprise (TME)` edition was selected, in the window of installation type select `All-in-one`.
5. Then select the main language of user interface management console, as well as date and time displaying format and preset configuration language:
   - `Russian`;
   - `English`.
6. Select the classification base language. A classification base includes preset policies, elements of technology configuration and protected objects.
   The following languages are available to select:
   - `Russian`;
   - `English`.

   You can select both languages. If you do not require to install a classification base, do not select any language.
   Options will be displayed one by one. Type **Y** to select an option or **N** to refuse it. Press **Enter** to confirm the selection.

> **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**



7. 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.

   > **Note:**
   >
   > `Install database server locally` is supported only for DBMS included in the distribution kit.

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

   > **Important!**
   >
   > Select `PostgreSQL`:
   >
   > - If you install Traffic Monitor on Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS
   >
   > and/or
   >
   > - If you use Postgres Pro Enterprise, Jatoba or Tantor DBMS.

9. If you use a remote database, please enter consistently:
   a. IP address and database server domain name.

      > **Important!**
      >
      > To install Traffic Monitor on the same server with an already deployed DBMS, specify the address `127.0.0.1`.

   b. Connection port
   c. The name of database to be used, where the scheme is to be added.
10. 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.

11. Select a data storage mode:
    - `Normal` – 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.
12. 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 as t/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 relevant number of paths to daily tablespaces.

    - `Daily tablespaces paths` – path to daily tablespace data storage directory.
13. 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.

> **Note:**
>
> If you will use Data Storage, then, for archiving tablespaces, you need to specify the path to the Data Storage slow disk during the storage installation. For details, see *Installing Platform*.

14. Similar to previous point you can configure the deletion parameters for daily tablespaces. If enabled, the default value for all the parameters – 90 days.
15. You can enable using external storage of binary data – Data Storage.
    In case of positive answer, specify the parameters for connecting to external storage:
    - **`Data Storage hostname`** – hostname or IP address of the server on which the storage is installed
    - **`Data Storage port`** – port for connecting to Data Storage. The 40731 port is used by default
    - **`Data Storage access token`** – Data Storage authorization token

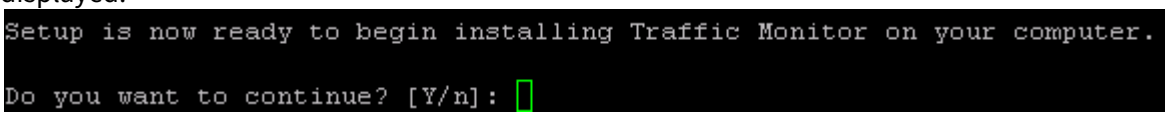
    You can find the actual value of the token:
    - On the Data Storage server, via the command line. For this:
      a. Go to the directory where the Platform distribution kit was extracted.
      b. Run the command:
      `./setup.py tokens list`
      As a result, you will see a list of tokens for connecting to the Platform. The actual Data Storage authorization token will be displayed opposite the *DataStorageUser* identity.
    - In the Platform product management console, in the **Token for Data Storage User** field of the **Global settings** section. Available if the Platform product with web interface is installed on the server with Data Storage and the web interface contains such a setting.
16. 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.
17. 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.
18. 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.

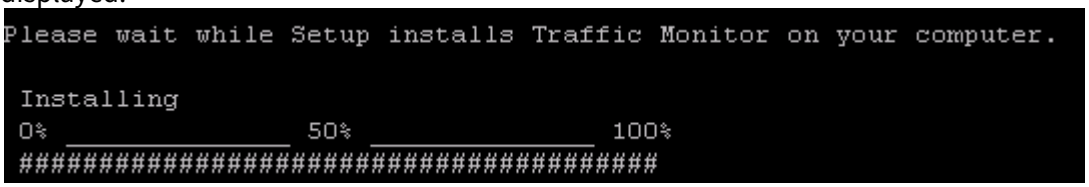
19. If required, you can change the standard configuration of Sphinx service operation. In this case an offer to set a list of languages including morphological support will be displayed. Indexing will be performed according to selected languages. You can specify few languages using a space to separate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

20. You can enable OCR technology. In this case you should select one system to be used:
    - `Content AI ContentReader Engine`;
    - `Tesseract`.
21. If Content AI ContentReader Engine 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 Content AI ContentReader Engine. In case you have no active license, type **N** and press **Enter**. In this case ContentReader Engine will be installed with no license. To use ContentReader Engine you can manually add an active license later. For more details, please see *InfoWatch Traffic Monitor. Administration Guide. Configuring OCR Extractors* article.
22. 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.
23. 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:



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.

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

Installing in graphical mode

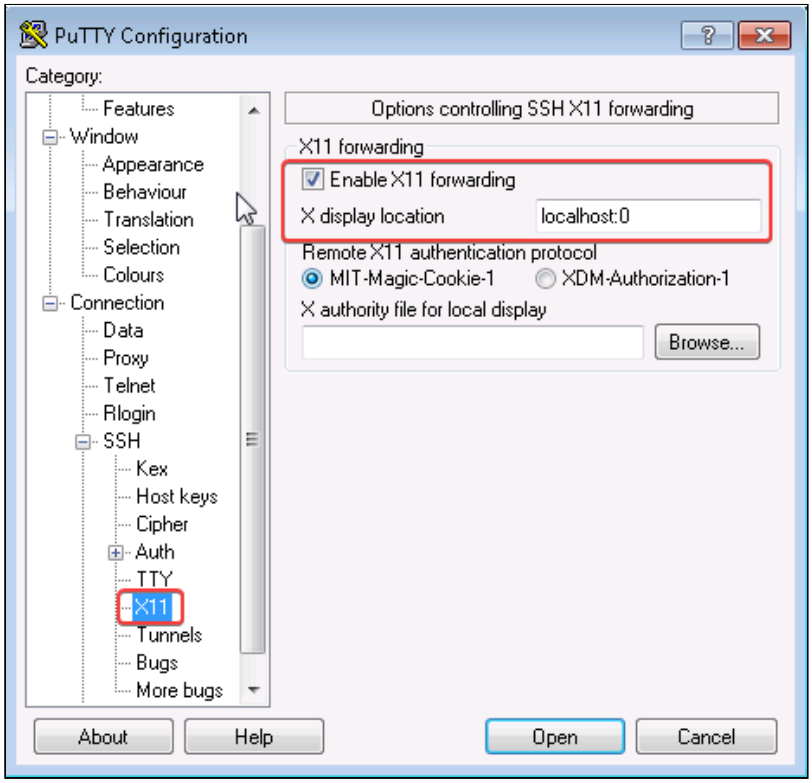
X Window System uses a client - server model. To run the installer in the graphical mode **X11 Forwarding** is used to forward the graphical output of remote system. This let you work directly with Linux graphical applications on the computer which is connected to server. This mode is implemented via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

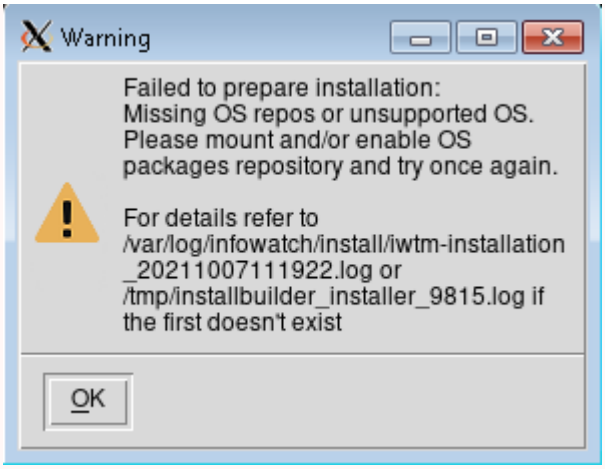
b. To start the installer in the graphical mode you will require an application configured to access to X Window System, for example:
   - Xming application – for OS MS Windows;
   - Gnome 3 shell – for OS Linux.

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-7.15.0.97-rhel7`
   Preparations will be made to start the installation. At this stage the unpacking of Traffic Monitor installation files is not being performed.

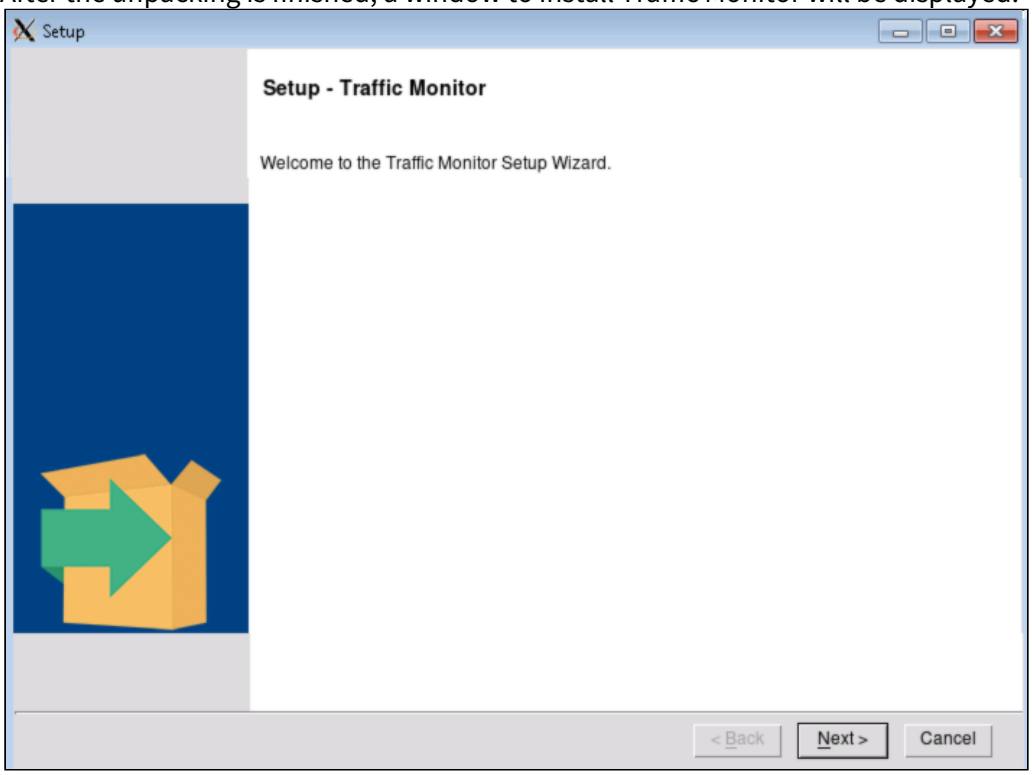
> **Warning!**
>
> If available configured OS repositories are missing, the preparation process will stop with the following alert box:



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

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

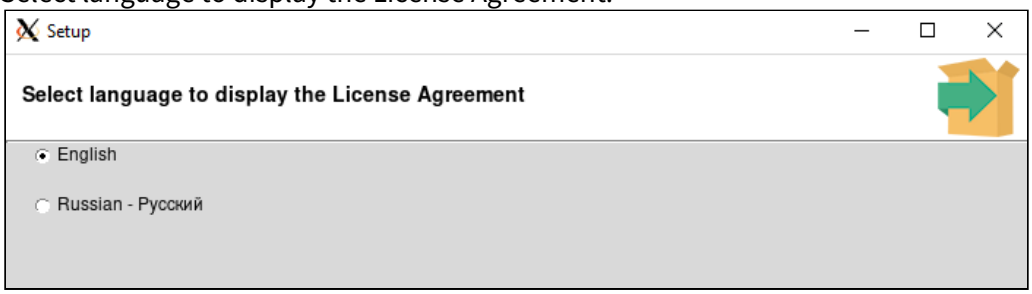
After the unpacking is finished, a window to install Traffic Monitor will be displayed:



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

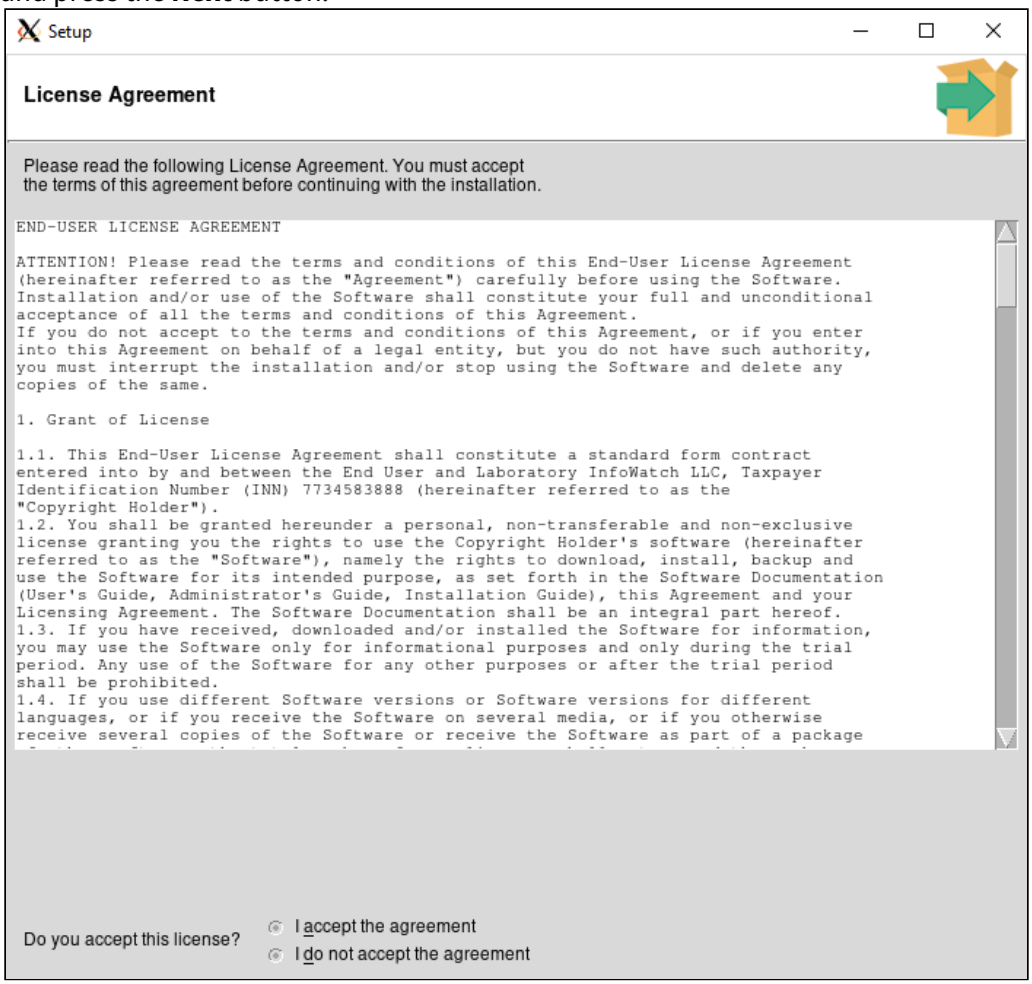
6. You must accept the terms of the License Agreement before continuing with the installation. For this:

a. Select language to display the License Agreement:



- `English`;
- `Russian`.

b. Select one of the following options. For this, click in the checkbox next to the required value and press the **Next** button:



- `I accept the agreement` – to accept the License Agreement and continue the installation process;
- `I do not accept the agreement` – to not accept the License Agreement and abort the installation process.

7. Select Traffic Monitor edition type:

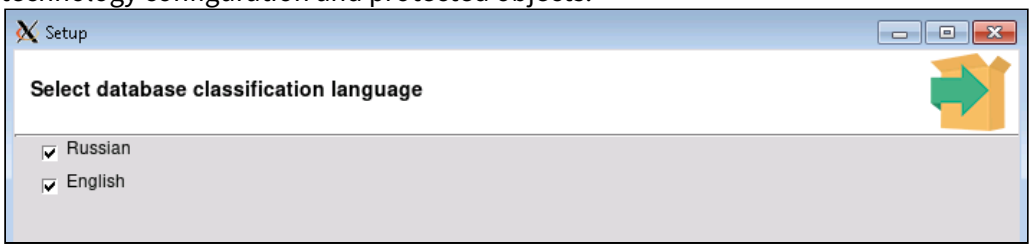


- `Traffic Monitor Enterprise (TME)` to install Enterprise edition;
- `Traffic Monitor Standard (TMS)` to install Standard edition.

Warning!

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

8. If `Traffic Monitor Enterprise (TME)` edition was selected, in the window of installation type select `All-in-one`.
9. Then select the main language of user interface management console, as well as date and time displaying format and preset configuration language:
   - `Russian`;
   - `English`.
10. Select the classification base language. A classification base includes preset policies, elements of technology configuration and protected objects.

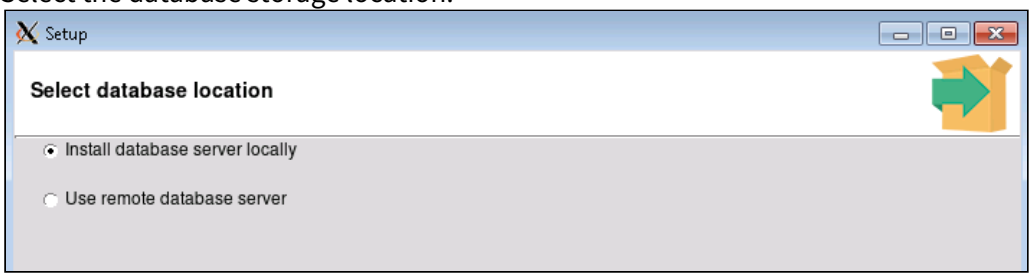


The following languages are available to select:

- `Russian`;
- `English`.

To select both values, mark each required field and press **Next** button. If you do not require to install a classification base, do not select any language.

11. Select the database storage location:



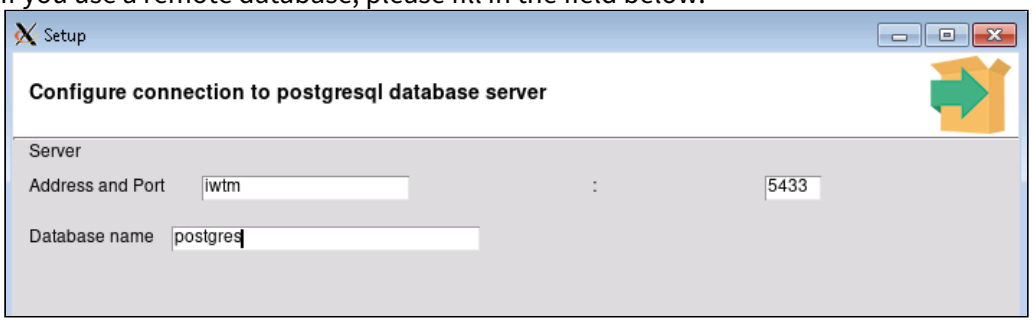
- `Install database server locally` – to install locally on current server;
- `Use remote database server` – to use on remotely deployed database. In this case the Traffic Monitor scheme will be added to remote database.

> **Note:**
>
> `Install database server locally` is supported only for DBMS included in the distribution kit.

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

> **Important!**
>
> Select `PostgreSQL`:
>
> - If you install Traffic Monitor on Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS
>
> and/or
>
> - If you use Postgres Pro Enterprise, Jatoba or Tantor DBMS.

13. 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.

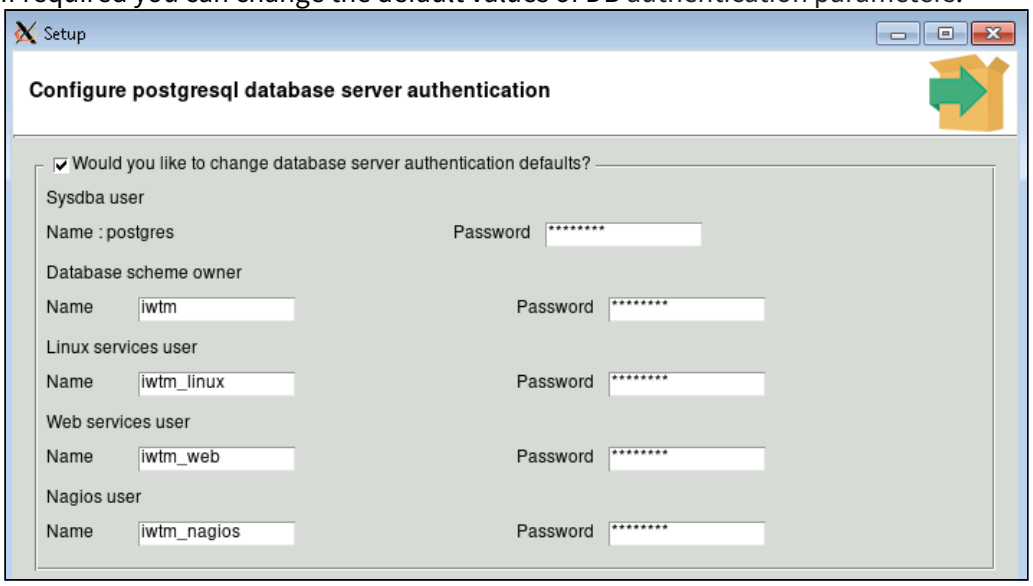
> **Important!**

To install Traffic Monitor on the same server with an already deployed DBMS, specify the address `127.0.0.1`.

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.

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

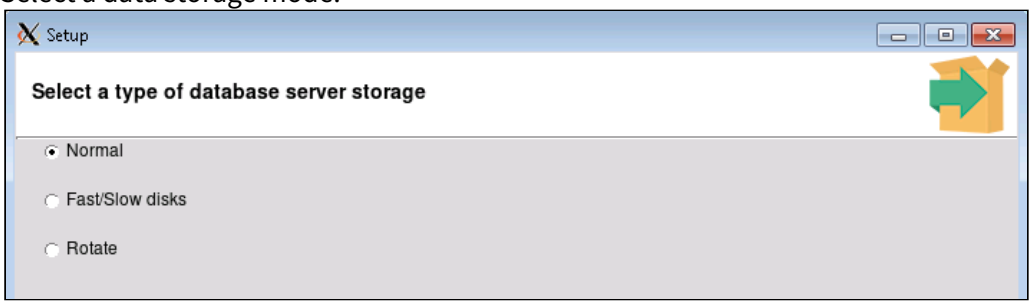


To edit the values mark the field next to question. This will let you edit the following sections:

- **`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.

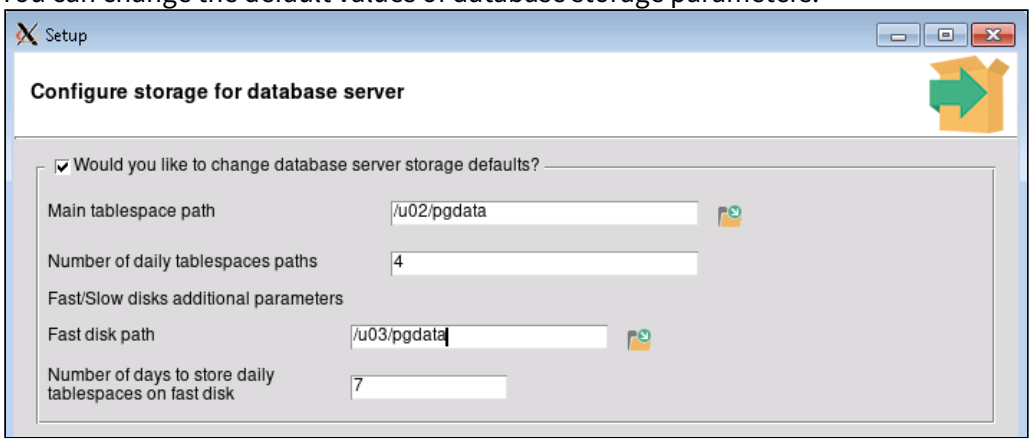
To leave the default values please do not mark the field and press **Next** button. In this case the fields cannot be edited and the installer will use the default parameters.

15. Select a data storage mode:



- **Normal** – 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.

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

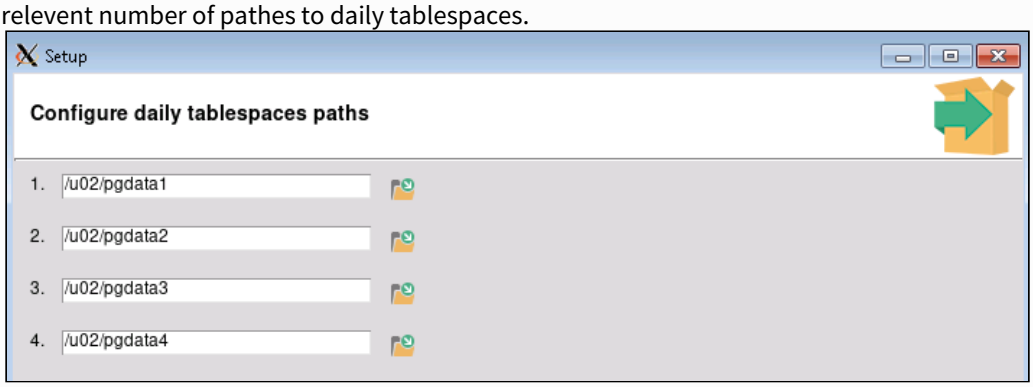


- **Main tablespaces path** – path to main tablespaces data storage directory;

  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 a st/Slow disks** mode;
- **Number of daily tablespaces paths** – number of daily tablespaces paths, a number from 1 to 10;

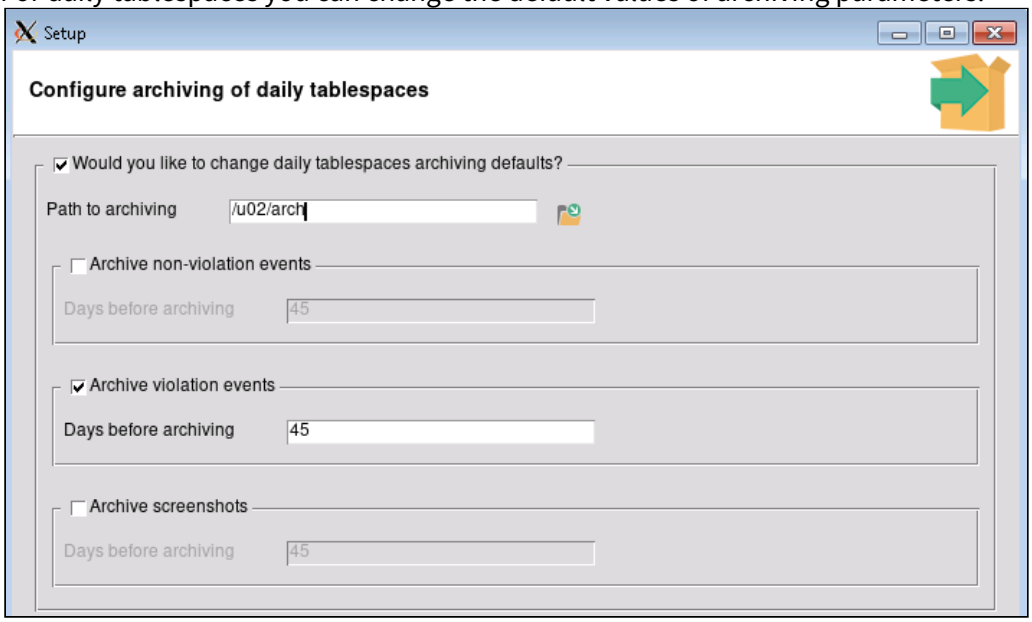
> **Note:**

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.

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



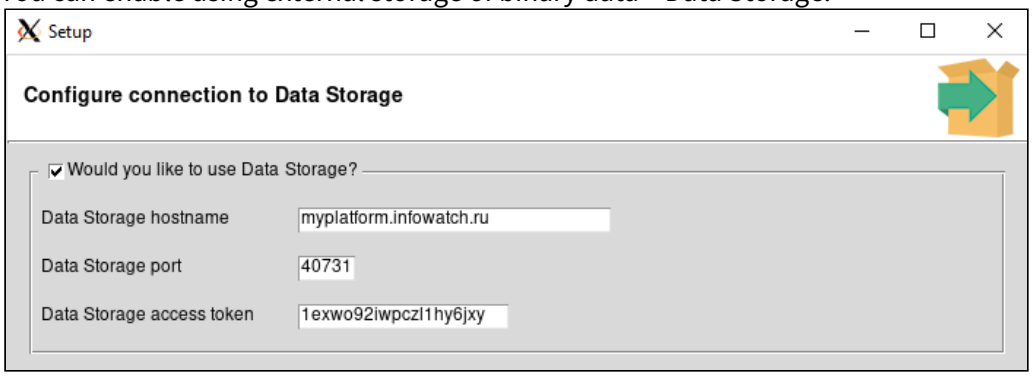
- **Path to archiving** – path to archived tablespaces files storage directory.

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.

> **Note:**
>
> If you will use Data Storage, then, for archiving tablespaces, you need to specify the path to the Data Storage slow disk during the storage installation. For details, see *Installing Platform*.

18. Similar to previous point you can configure the deletion parameters for daily tablespaces. If enabled, the default value for all the parameters – 90 days.
19. You can enable using external storage of binary data – Data Storage.



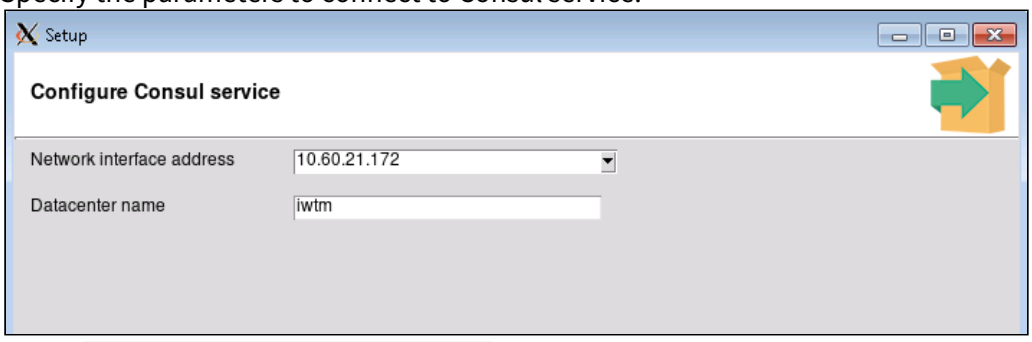
For this, mark the field next to question and specify the parameters for connecting to external storage:

- **`Data Storage hostname`** – hostname or IP address of the server on which the storage is installed
- **`Data Storage port`** – port for connecting to Data Storage. The 40731 port is used by default
- **`Data Storage access token`** – Data Storage authorization token

You can find the actual value of the token:

- On the Data Storage server, via the command line. For this:
  a. Go to the directory where the Platform distribution kit was extracted.
  b. Run the command:
  `./setup.py tokens list`
  As a result, you will see a list of tokens for connecting to the Platform. The actual Data Storage authorization token will be displayed opposite the *DataStorageUser* identity.
- In the Platform product management console, in the **Token for Data Storage User** field of the **Global settings** section. Available if the Platform product with web interface is installed on the server with Data Storage and the web interface contains such a setting.

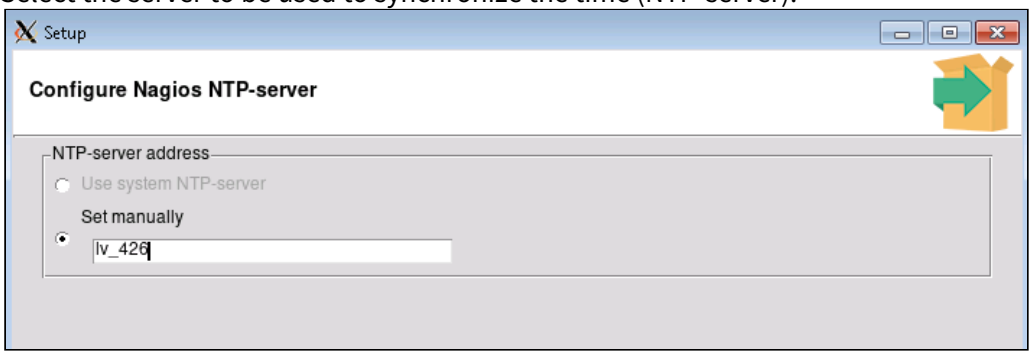
20. Specify the parameters to connect to Consul service:



a. **`Network interface address`** – select IP address of network interface.
To select from the list of parameters click ▼ and select the required value.

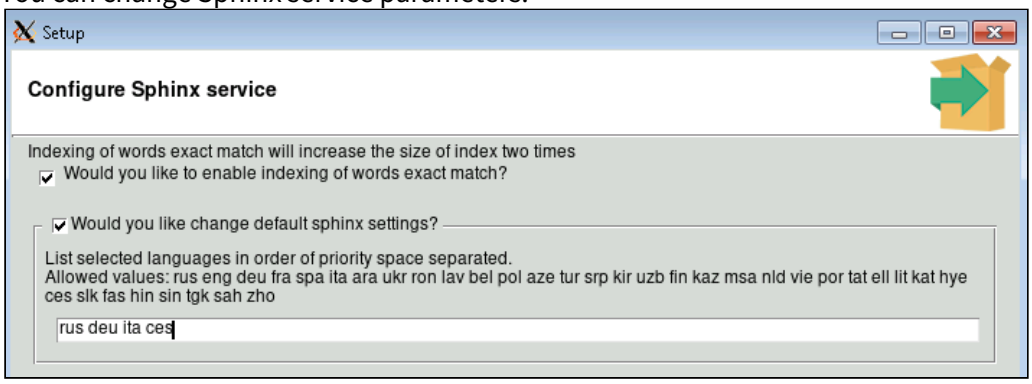
b. **`Datacenter name`** – input name of Consul data center.

21. 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.

22. You can change Sphinx service parameters:



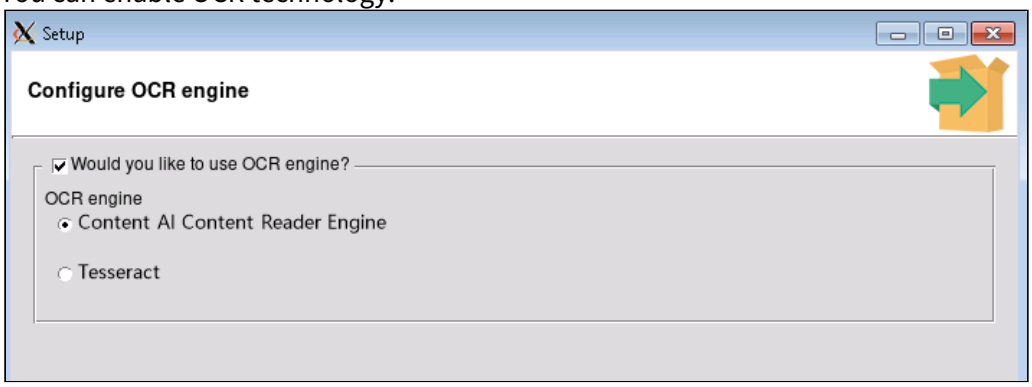
- **`Enable indexing of words exact match`**;

> **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 setting`**). 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.

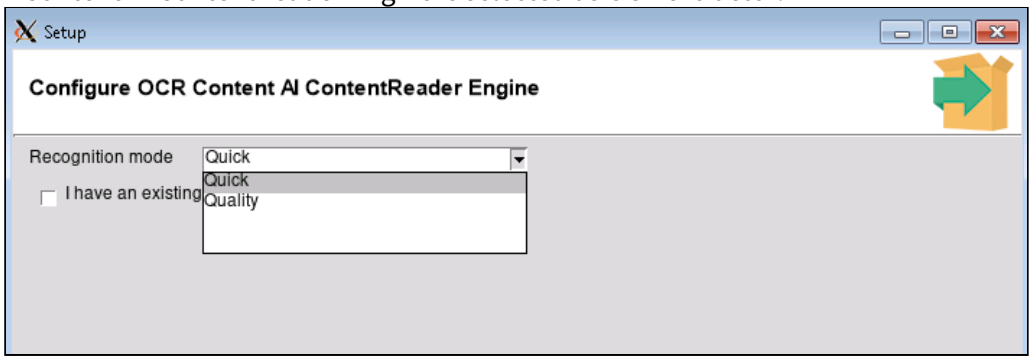
23. You can enable OCR technology.



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

- `Content AI ContentReader Engine`;
- `Tesseract`.

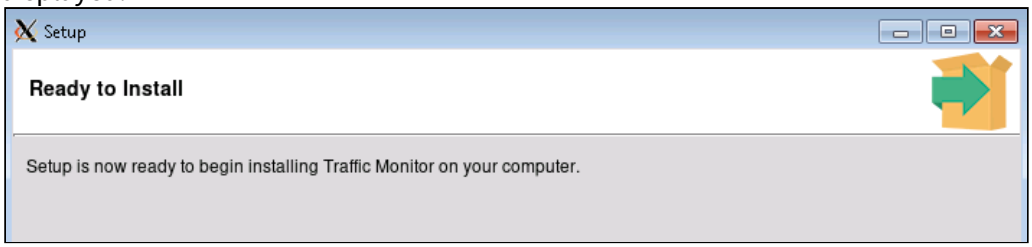
24. If Content AI ContentReader Engine is selected as OCR extractor:



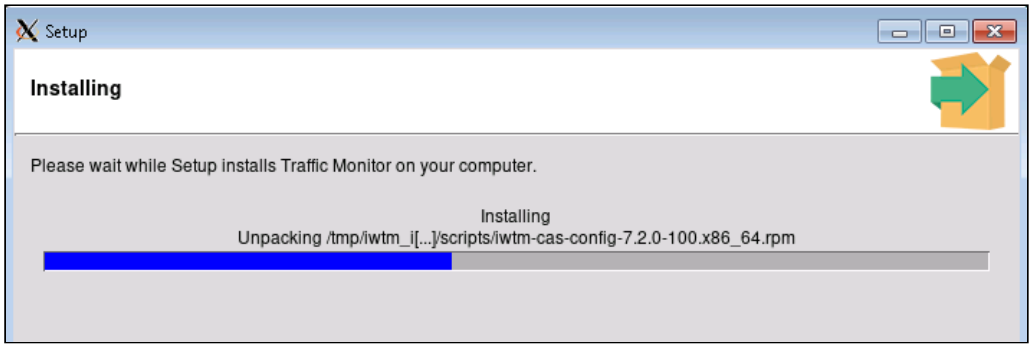
a. Select a recognition mode:
   - `Quick` – a fast mode;
   - `Quality` – a detailed mode providing higher quality of recognition.

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

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



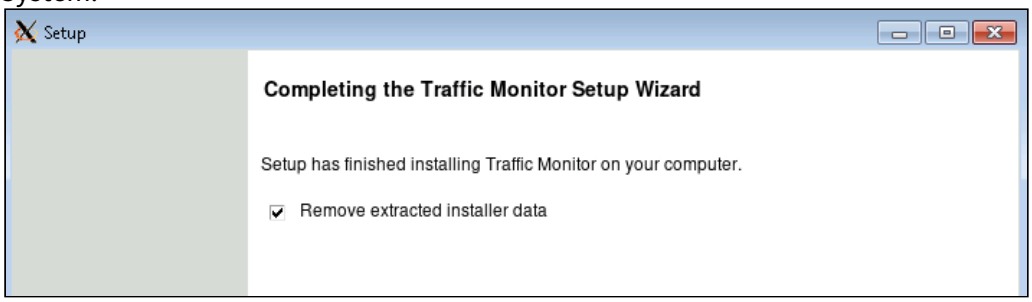
To start the installation and press **Next**.
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed.



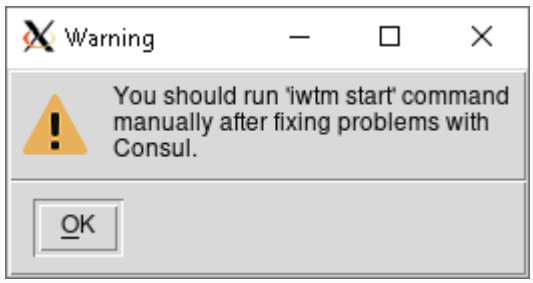
The process may take some time.

> **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.

26. 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 extracted 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.

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

If you installed Traffic Monitor on Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS, recover the original OS release file.

For this:

1. Run the command depending on OS:
   - in Oracle Linux 8:
     ```
     mv /etc/release.bak /etc/oracle-release
     ```
   - in AlmaLinux 8 or Rocky Linux 8:
     ```
     mv /etc/release.bak /etc/redhat-release
     ```
2. Confirm overwriting of the file. For this, enter " `yes` " and press **Enter**.
3. Check that the original release file is succesfully recovered. For this, run the command:
   ```
   lsb_release -a
   ```
   As a result, the information on your OS should be displayed. For example, for AlmaLinux 8 OS, the following will be displayed:
   ```
   Distributor ID: AlmaLinux
   Description:    AlmaLinux release 8.10 (Cerulean Leopard)
   Release:        8.10
   Codename:       CeruleanLeopard
   ```

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

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*.

3.2.2 Distributed Installation of TM Enterprise

The Enterprise edition of Traffic Monitor allows you to deploy the System, so that DBMS modules or web console were installed on different servers. This installation type is used if Traffic Monitor services and DBMS cannot efficiently operate on the same server because of the expected 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 simplify the installation of Traffic Monitor components on several servers, the installer has implemented installation templates, which are used to distribute the load effectively and plan the deployment. For more details about the templates, see *System deployment schemes and installation types*.

There are four available installation templates:

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

The templates can be installed in any 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.

You can install several templates on the same server simultaneously.

Installing all the templates on the same 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 their sequence are similar in both modes.

Regardless of the selected installation mode, take the following general steps:

1. To log into the System, enter login and password (login as `root`).

   > **Warning!**
   >
   > Before running the installation, make sure that the server complies with the *OS and network settings requirements*. Each server should have a unique and correct FQDN.
   >
   > If you are going to use a remote Oracle, PostgreSQL or Postgres Pro Enterprise database (deployed locally or on a separate server), you should *prepare* it first.
   >
   > Before installing, in order to clear memory, we recommend rebooting the server where the database will be deployed.

2. Connect external or local OS repositories.
   For example, you can find instructions on how to configure local Red Hat Enterprise Linux repository at the *official web page*.
   If you install Traffic Monitor on RED OS with no internet access

   a. Disable external repositories.
   On a workstation running RED OS version 7.3.3 and below:

   Run the following commands:
   ```
   echo "enabled=0" >> /etc/yum.repos.d/RedOS-Base.repo
   echo "enabled=0" >> /etc/yum.repos.d/RedOS-Updates.repo
   sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/RedOS-kernels.repo
   ```

   On a workstation running RED OS version 7.3.4 or 7.3.5:

   Run the command:
   ```
   sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/RedOS-*.repo
   ```

   b. Connect the disk with the RED OS distribution kit to the server.
   c. Mount the disk with the RED OS distribution kit using the command:
   `mkdir -p /media/cdrom/ && mount /dev/cdrom /media/cdrom/`
   d. Create the `/etc/yum.repos.d/cdrom.repo` file and specify the the mounted disk as the repository. For this, use the command:
   ```
   cat << EOF > /etc/yum.repos.d/cdrom.repo
   [cdrom]
   name=cdrom
   baseurl=file:///media/cdrom/
   enabled=1
   gpgcheck=0
   EOF
   ```

e. Delete temporary files and make sure that the list of repositories contains the repository on the disk:
`yum clean all && yum repolist`
f. Install `libpq` library and `python2` package:
`yum install libpq python2`
g. Install the following packages:

Package name	Official repository
`lshw-B.02.19.2-1.el7.x86_64.rpm`	*RED OS - Updates*
`lz4-1.9.4-1.el7.x86_64.rpm`	
`python3-psycopg2-2.9.3-1.el7.x86_64.rpm`	
`urw-base35-fonts-legacy-20170801-11.el7.noarch.rpm`	*RED OS – OS*
`libxslt-1.1.34-1.el7.x86_64.rpm`	

For this:
i. Download the specified packages from the official RED OS repository.
ii. Copy them to the server where you are going to install Traffic Monitor.
iii. Go to the directory where the specified packages were copied.
iv. Run the following command:
`yum localinstall lshw-B.02.19.2-1.el7.x86_64.rpm lz4-1.9.4-1.el7.x86_64.rpm python3-psycopg2-2.9.3-1.el7.x86_64.rpm urw-base35-fonts-legacy-20170801-11.el7.noarch.rpm libxslt-1.1.34-1.el7.x86_64.rpm`

> **Note:**
>
> Additionally, you can install utilities for working with the operating system. For this, run the command:
> `yum install mc vim screen telnet bind-utils mlocate net-tools iptraf sysstat iotop rsync`
>
> Or you can install the *htop* utility by downloading it from *the official RED OS repository*.

h. Make sure your network settings are correct (see *Operating System and Network Server Configuration Requirements*) and the `/etc/hosts` file contains instructions for converting a server name to an IP address. If the instructions are missing, run the command:
`sh -c "echo '<IP_адрес> `hostname -f` `hostname -s`' >> /etc/hosts"`

If you install Traffic Monitor on OS Oracle Linux with no internet access:

a. Make sure that, in operating system, the current kernel is Red Hat Compatible Kernel (RHCK), for example, Oracle Linux Server Kernel `3.10.0-xxxx.el7.x86_64`, and the UEK kernel is removed. For details, see *Operating System and Network Server Configuration Requirements*.

b. Disable external repositories by running the following command:
`find /etc/yum.repos.d/ -iname "*.repo" -exec sed -i -e "s/enabled=.*/enabled=0/g" {} \;`
c. Connect the disk with the OS Oracle Linux distributive to the server.
d. Mount the disk with the OS Oracle Linux distributive, using the following command:
`mkdir -p /media/cdrom/ && mount /dev/cdrom /media/cdrom/`
e. Create the `/etc/yum.repos.d/cdrom.repo` file specifying the mounted disk as a repository. For this, run the following command:
```
cat << EOF > /etc/yum.repos.d/cdrom.repo
[cdrom]
name=cdrom
baseurl=file:///media/cdrom/
enabled=1
gpgcheck=0
EOF
```
f. Remove temporary files and make sure that repository list contains the repository from the disk:
`yum clean all && yum repolist`
g. Install `Perl`:
`yum install perl`
h. Install the following packages:
   - `perl-List-MoreUtils-0.33-9.el7.x86_64.rpm` (you can download the package from *the official Oracle Linux 7 Latest repository*)
   - `perl-Dist-CheckConflicts-0.06-2.el7.noarch.rpm` (you can download the package from *the official Oracle Linux 7 Optional Latest repository*)
   - `urw-base35-fonts-legacy-20170801-10.el7.noarch.rpm` (you can download the package from *the official Oracle Linux 7 Optional Latest repository*)
   - `python3-psycopg2-2.7.7-2.el7.x86_64.rpm` (you can download the package from *the official Oracle Linux 7 EPEL repository*)
   - `libzstd-1.5.5-1.el7.x86_64.rpm` (you can download the package from *the official Oracle Linux 7 EPEL repository*)

   For this:
   i. Download the listed packages from the official Oracle Linux repositories.
   ii. Copy them to the server where Traffic Monitor is to be installed.
   iii. Go to the directory where you copied the packages.
   iv. Run the following command for each package:
   `rpm -ivh <package_name>`

   > **Note:**
   >
   > Optionally you can install tools for work in operating system by running the command:
   > `yum install mc vim screen telnet bind-utils mlocate net-tools iptraf sysstat iotop rsync`

i. Make sure you have correctly configured network settings (see *Operating System and Network Server Configuration Requirements*) and the `/etc/hosts` file contains the hostname resolving setting. If it does not, run the command:
`sh -c "echo '<IP_address> `hostname -f` `hostname -s`' >> /etc/hosts"`

3. **If you install Traffic Monitor components on Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS:**

> **Warning!**
>
> Make sure that, in Oracle Linux 8.10 operating system, the current kernel is Red Hat Compatible Kernel (RHCK), for example, Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`, and the UEK kernel is removed. For details, see *Operating System and Network Server Configuration Requirements*.

   a. Install the `redhat-lsb-core` package by running the following command:

```
dnf install redhat-lsb-core
```

   b. Create a backup copy of the OS release file and replace the content of the original file. For this, run the commands depending on OS:
      - in Oracle Linux 8:

```
cp /etc/oracle-release /etc/release.bak

echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/oracle-release
```

      - in AlmaLinux 8 or Rocky Linux 8:

```
cp /etc/redhat-release /etc/release.bak
echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/redhat-release
```

   c. Run the command:

```
lsb_release -a
```

   As a result, the following information should be displayed:

```
Distributor ID: RedHatEnterprise
Description:    Red Hat Enterprise Linux release 8.10 (Ootpa)
Release:        8.10
Codename:       Ootpa
```

> **Note:**
>
> After installing Traffic Monitor, recover the original OS release file. For details, see *below*.

4. 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`
5. Copy the files from InfoWatch Traffic Monitor distributive – installer and archive with DBMS components – into the created directory:

OS	Distribution files

Red Hat Enterprise Linux 7
Oracle Linux 7 [4]
	Installer:
	`iwtm-installer-x.x.x.xxx-rhel7`
	Archive with DBMS components [1] [2]:
	PostgreSQL:
	`iwtm-postgresql-15.14-x.x.x.xxx-rhel7.tar.gz`
	Oracle [3]:
	`iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz`

RED OS	**Installer**:
	`iwtm-installer-x.x.x.xxx-redos-7.3`
	Archive with DBMS components [1] [2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-redos-7.3.tar.gz`

Red Hat Enterprise Linux 8
Oracle Linux 8
AlmaLinux 8
Rocky Linux 8
	Installer:
	`iwtm-installer-x.x.x.xxx-rhel8`
	Archive with DBMS components [1] [2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-rhel8.tar.gz`

Alt Server	**Installer**:
	`iwtm-installer-x.x.x.xxx-altlinux-10`
	Archive with DBMS components [1] [2]:
	`iwtm-postgresql-15.10-x.x.x.xxx-altlinux-10.tar.gz.md5`

Important!

[1] Archive with DBMS components is required *both* when installing DBMS distributed with the product (`local` mode) *and* when using an already deployed DBMS in *remote* mode. See *System Deployment Schemes and Installation Types* for details.

[2] In case you are planning to use an already deployed PostgreSQL-based DBMS, use an archive from PostgreSQL column. For the list of supported PostgreSQL-based DBMS, see *Hardware and Software Requirements*.

[3] If you use Oracle DBMS and network file system (NFS), before launching the installer:

- **When using Oracle Real Application Clusters (RAC):**

  Set the options for mounting in accordance to *the article on the official site*.

- **When not using RAC:**

  Open settings of the mount point (by default, `/etc/fstab`) and make sure that the `noac` option is not used and the `actimeo` parameter has the `0` value.

  For details, see *the article on the official site*.

[4] For Traffic Monitor installed on a server running Oracle Linux 7, Postgres Pro Enterprise DBMS is not supported.

Installation using distributive files for Red Hat Enterprise Linux 7 will be described further. In our example, we need to copy an installer file and an archive with DBMS components:

- Installer:
  `iwtm-installer-7.15.0.97-rhel7`
  where `7.15.0.97` is the build number, `rhel7` is the OS designation;
- Archive with DBMS components:
  - In case of PostgreSQL (or one of supported PostgreSQL-based DBMS):
    `iwtm-postgresql-15.14-7.15.0.97-rhel7.tar.gz`
    where `postgresql-15.14` is the DBMS designation, `7.15.0.97` is the build number, `rhel7` is the OS designation;
  - In case of Oracle DBMS:
    `iwtm-oracle-19.0.0.0.0-7.15.0.97.tar.gz`
    where `oracle-19.0.0.0.0` is the DBMS designation, `7.15.0.97` is the build number.

This instruction is relevant for other supported OS: Oracle Linux, RED OS, AlmaLinux, Rocky Linux and Alt Server.

6. Enter the command to shift to Traffic Monitor distributive directory.
   As per our example:
   ```
   cd /distr
   ```
7. 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-7.15.0.97-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-7.15.0.97-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:

```
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 OS 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 welcoming window will be displayed:

```
Welcome to the Traffic Monitor Setup Wizard.

-------------------------------------------------------------------------
Please read the following License Agreement.
You must accept the terms of this agreement before continuing with the installation.

[1] Show the License Agreement
[2] I accept the License Agreement
[3] I do not accept the License Agreement
Please choose an option [1] :
```

2. You must accept the terms of the License Agreement before continuing with the installtion. Select one of the following options. For this, type the figure specified next to it, and press **Enter**:
   - `Show the License Agreement` - to view the License Agreement;
     If this option is selected:
     a. Select language to display the License Agreement:
        - `English`
        - `Russian`
     b. Read the License Agreement. To go to the next page, press **Enter**.
     c. Accept the License Agreement. For this, type **y** and press **Enter**.
   - `I accept the License Agreement` – to accept the License Agreement without preview;
   - `I do not accept the License Agreement` – to not accept the License Agreement and abort the installation process.

> **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] Show the License Agreement` will be selected.

Also, the default value, which is in square brackets, can be specified with a capital letter.

Example:

```
Select database classification language


Russian [Y/n]:



English [y/N]:
```

3. Select **`Traffic Monitor Enterprise (TME)`** to install Enterprise edition.
4. In the window of installation type select **`Distributed`**.
5. 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.
   The following languages are available to select:
   - **`Russian`**;
   - **`English`**.

   Options will be displayed one by one. You can select both languages. 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.

     Note:

     `Install database server locally` is supported only for DBMS included in the distribution kit.

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

     Important!

     Select **`PostgreSQL`**:

- If you install Traffic Monitor on Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS
  and/or
- If you use Postgres Pro Enterprise, Jatoba or Tantor DBMS.

5. I f you use a remote database, please enter consistently:
   a. IP address and database server domain name.

   Important!

   To install Traffic Monitor on the same server with an already deployed DBMS, specify the address `127.0.0.1`.

   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.

> **Note:**
>
> If you will use Data Storage, then, for archiving tablespaces, you need to specify the path to the Data Storage slow disk during the storage installation. For details, see *Installing Platform*.

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. You can enable using external storage of binary data – Data Storage.
In case of positive answer, specify the parameters for connecting to external storage:
    - **`Data Storage hostname`** – hostname or IP address of the server on which the storage is installed
    - **`Data Storage port`** – port for connecting to Data Storage. The 40731 port is used by default
    - **`Data Storage access token`** – Data Storage authorization token

    You can find the actual value of the token:
    - On the Data Storage server, via the command line. For this:
        a. Go to the directory where the Platform distribution kit was extracted.
        b. Run the command:
        `./setup.py tokens list`

As a result, you will see a list of tokens for connecting to the Platform. The actual Data Storage authorization token will be displayed opposite the *DataStorageUser* identity.

- In the Platform product management console, in the **Token for Data Storage User** field of the **Global settings** section. Available if the Platform product with web interface is installed on the server with Data Storage and the web interface contains such a setting.

12. 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 the field empty.
    f. `Consul retryjoin port` – connection port to specified Consul servers.
13. 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.
14. 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.

15. 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.

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 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.

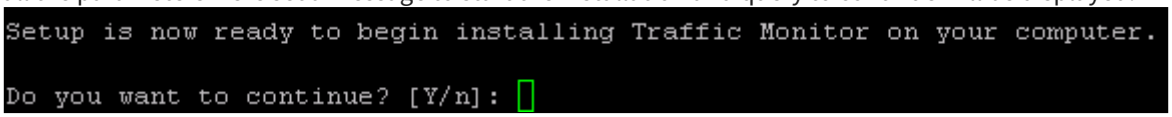
- Then you can enable indexing of words exact match for Sphinx service.

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

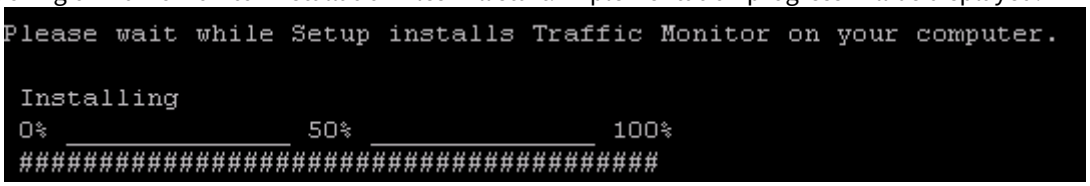
- If required, you can change the standard configuration of Sphinx service operation. In this case specify a list of languages including morphological support. Indexing will be performed according to selected languages. You can specify few languages using a space to separate them.

> **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.



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.

- 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 e nable 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.

```
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.

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 the 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:
   - **`Content AI ContentReader Engine`**;
   - **`Tesseract`**.

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

7. If Content AI ContentReader Engine 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 Content AI ContentReader Engine. In case you have no active license, type **N** and press **Enter**. In this case ContentReader Engine will be installed with no license. To use ContentReader Engine, you can manually add an active license later. For more details, please see *InfoWatch Traffic Monitor. Administration 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.

```
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.

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 following steps:

1. On the server, where Traffic Monitor components are planned to install:
   a. Install xauth utility using the command:
   - On a server running Red Hat Enterprise Linux, Oracle Linux, AlmaLinux, Rocky Linux or RED OS:
     `yum install xauth`
   - On a server running Alt Server:
     `sudo apt-get install xauth`

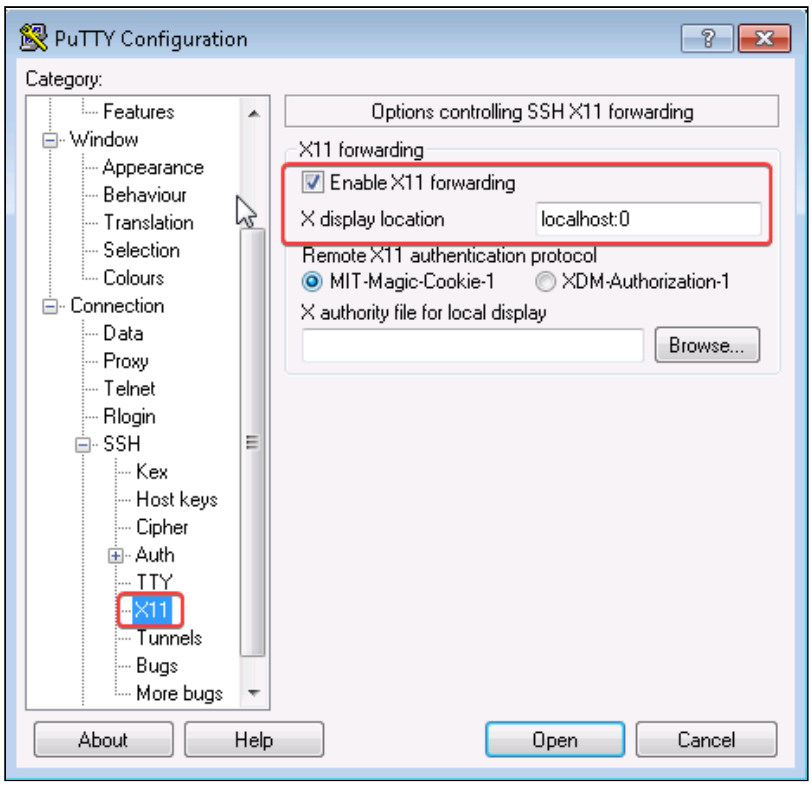
   b.Make sure that in the `/etc/ssh/sshd_config` file:
   - the " `X11Forwarding` " parameter value is " `yes` ";
   - the line with the " `X11Forwarding` " parameter is uncommented, i.e. it does not contain `#` character.

   c. Save changes in the 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:

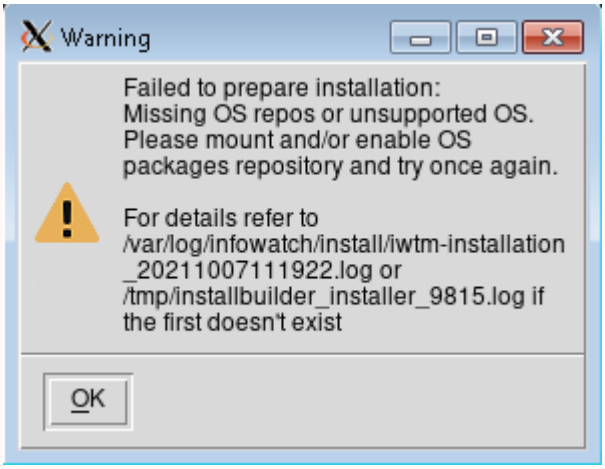
- Xming application - for OS MS Windows;
- Gnome 3 shell - for OS Linux.

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-7.15.0.97-rhel7`
Preparations will be made to start the installation. At this stage the unpacking of Traffic Monitor installation files is not being performed.

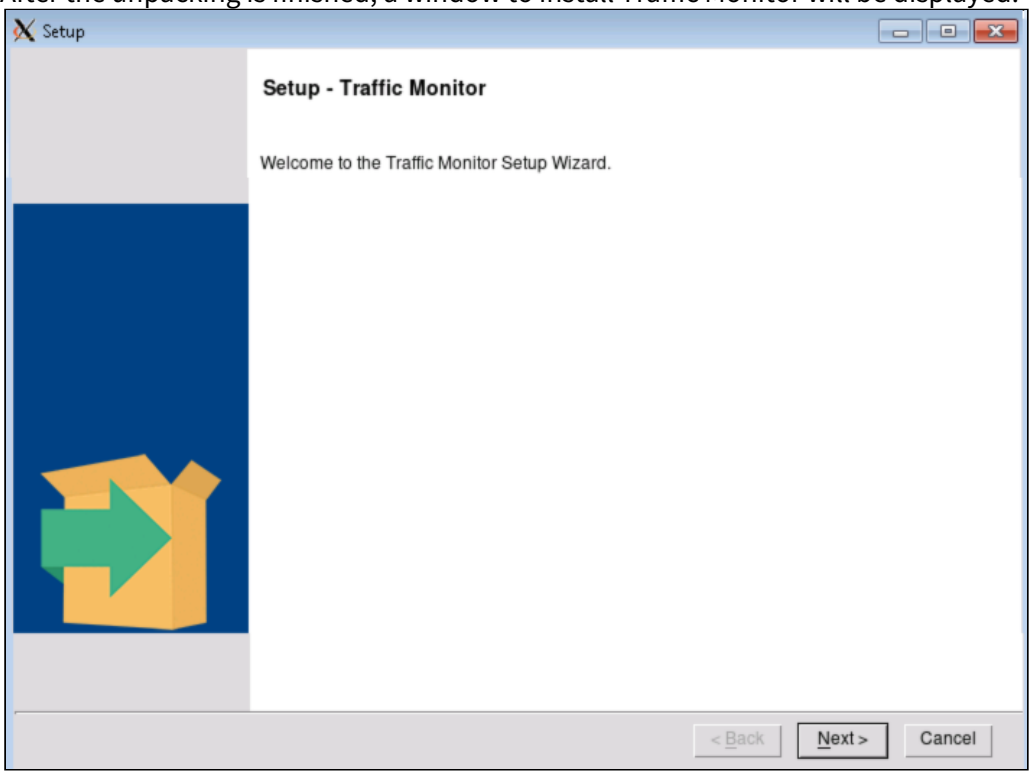
> **Warning!**
>
> If available configured OS repositories are missing, the preparation process will stop with the following alert box:



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

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

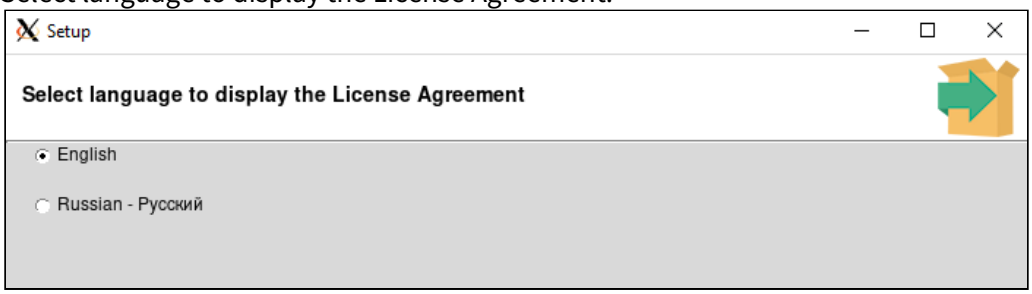
After the unpacking is finished, a window to install Traffic Monitor will be displayed:



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

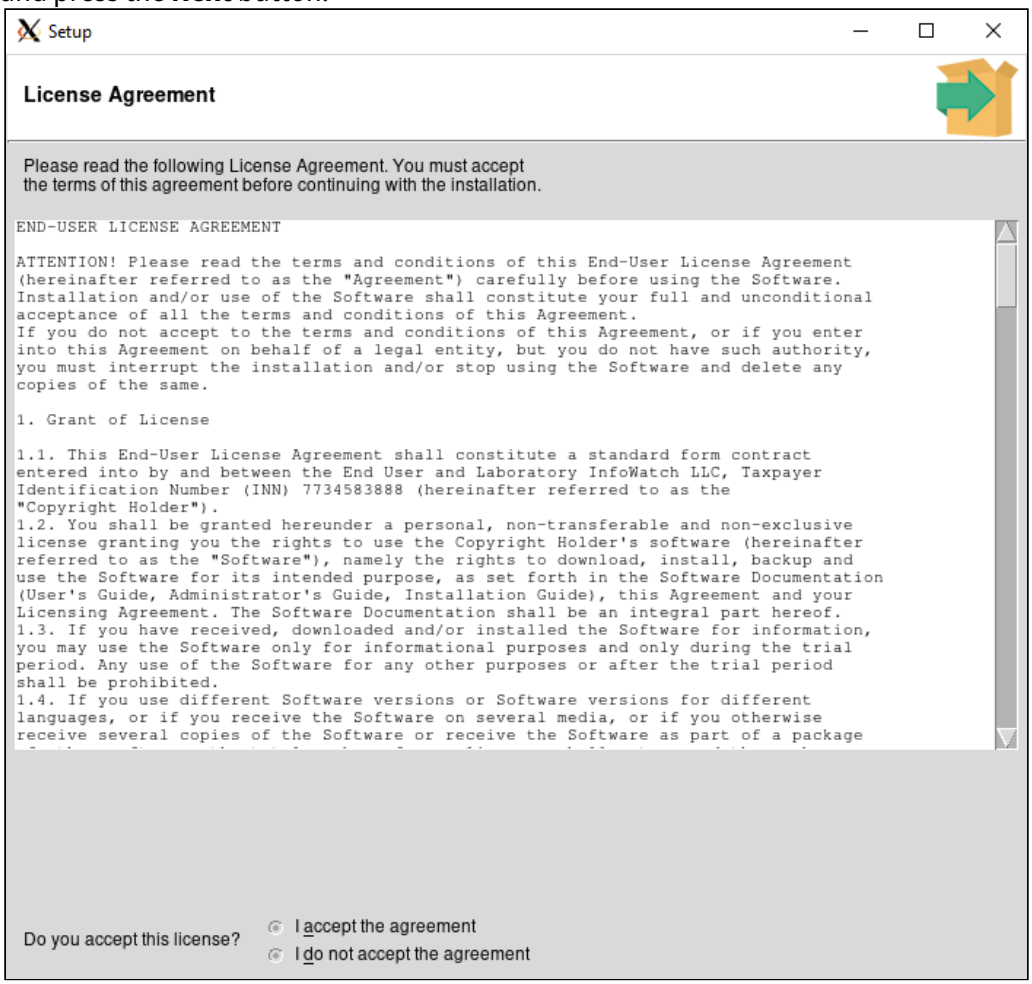
6. You must accept the terms of the License Agreement before continuing with the installation. For this:

a. Select language to display the License Agreement:



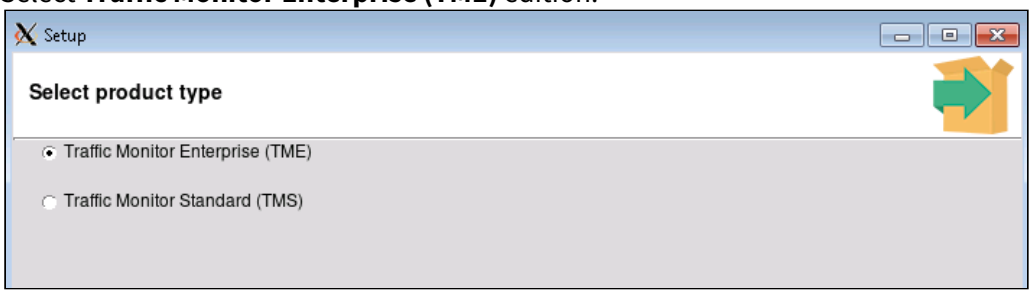
- `English`
- `Russian`

b. Select one of the following options. For this, click in the checkbox next to the required value and press the **Next** button:



- `I accept the agreement` – to accept the License Agreement and continue the installation process;
- `I do not accept the agreement` – to not accept the License Agreement and abort the installation process.

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



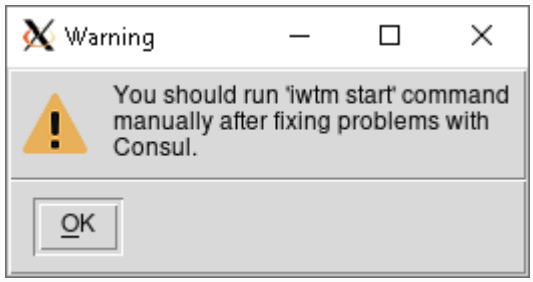
In the window of installation type select `Distributed`.

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).

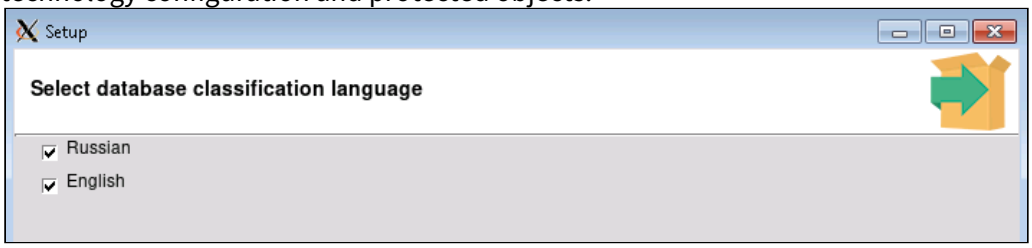
If the error occurs, the installer will not launch Traffic Monitor services when the installation is finished, so you need to start them manually.

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.

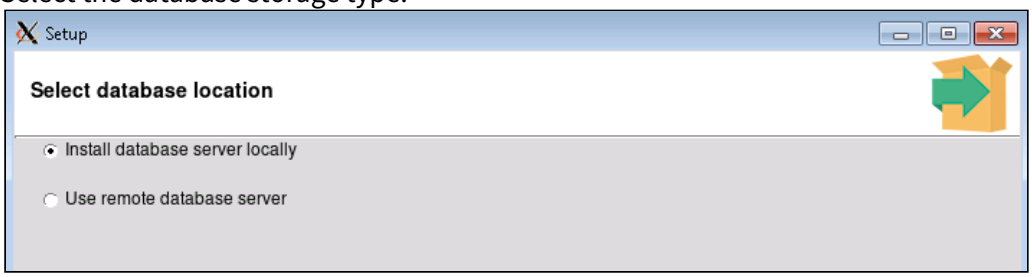


The following languages are available to select:

- **`Russian`**;
- **`English`**.

To select both values, mark each required field and press **Next** button. If you do not require to install a classification base, do not select any language.

3. Select the database storage type:



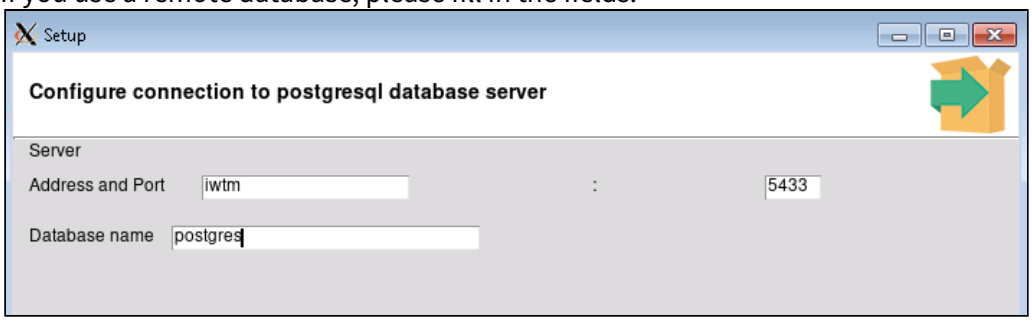
- `Install database server locally` – to install locally on current server;
- `Use remote database server` – to use on remotely deployed database. In this case the Traffic Monitor scheme will be added to remote database.

> **Note:**
>
> `Install database server locally` is supported only for DBMS included in the distribution kit.

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

> **Important!**
>
> Select `PostgreSQL`:
>
> - If you install Traffic Monitor on Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS
>
> and/or
>
> - If you use Postgres Pro Enterprise, Jatoba or Tantor DBMS.

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



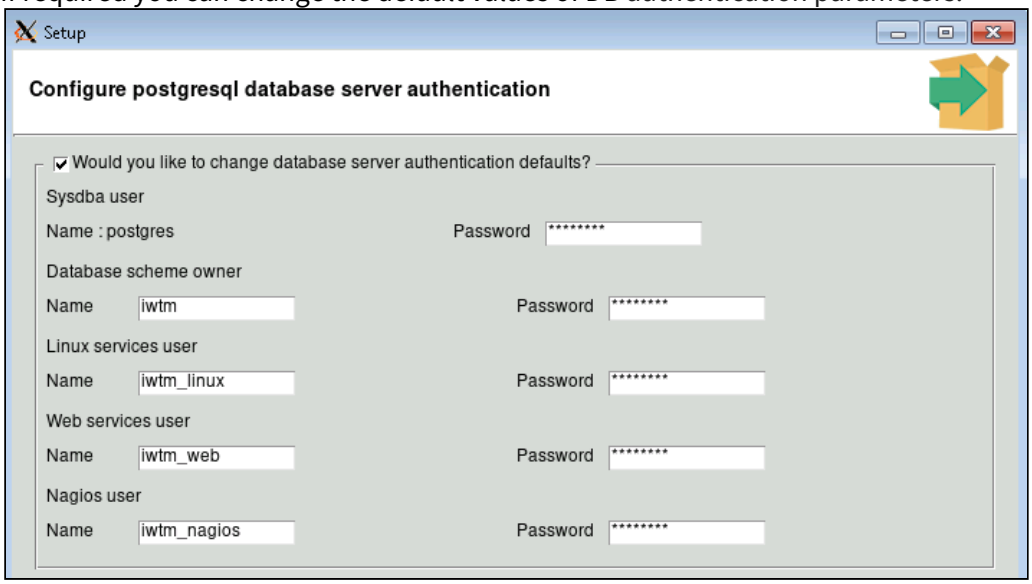
- `Address and Port` – IP address and database server domain name and connection port.

> **Important!**
>
> To install Traffic Monitor on the same server with an already deployed DBMS, specify the address `127.0.0.1`.

- **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.

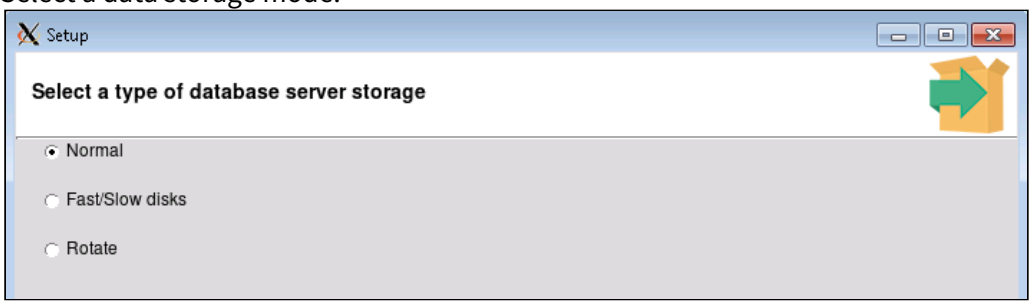
6. If required you can change the default values of DB authentication parameters.



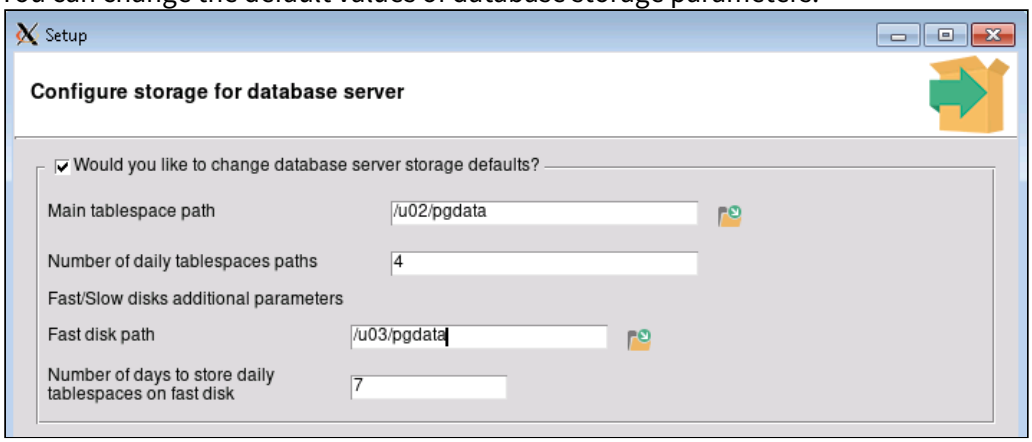
To edit the values mark the field next to question. This will let you edit the following sections:

- **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.

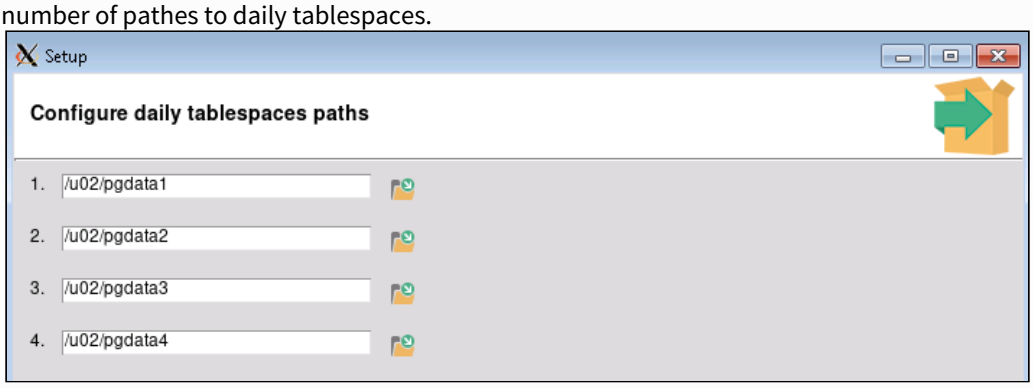


   - **Main tablespaces path** - path to main tablespaces data storage directory;

     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 as t/Slow disks** mode;
   - **Number of daily tablespaces paths** - number of daily tablespaces paths, a number from 1 to 10;

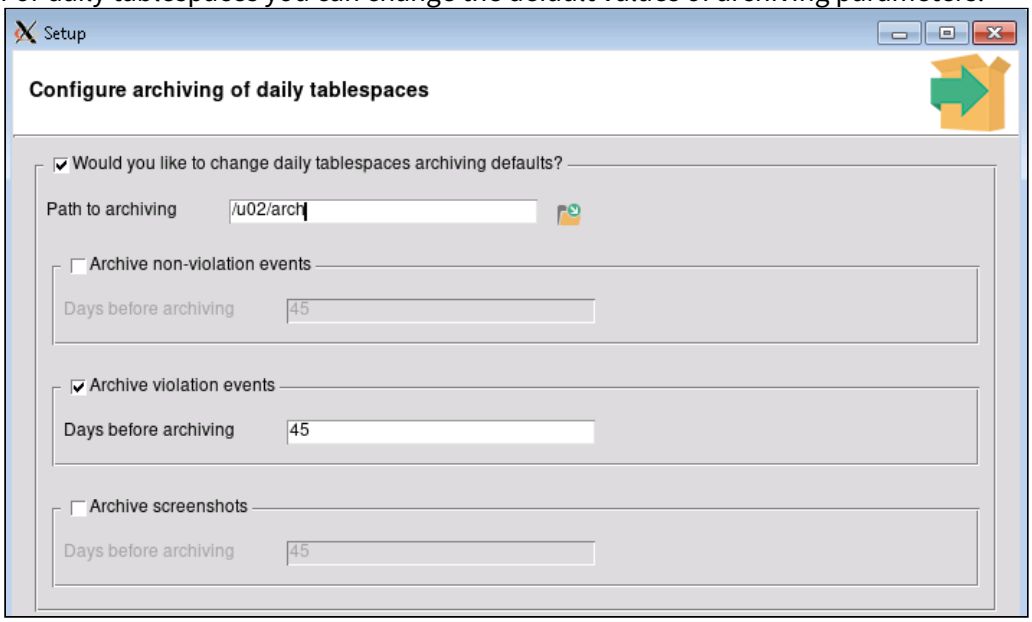
> **Note:**

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.



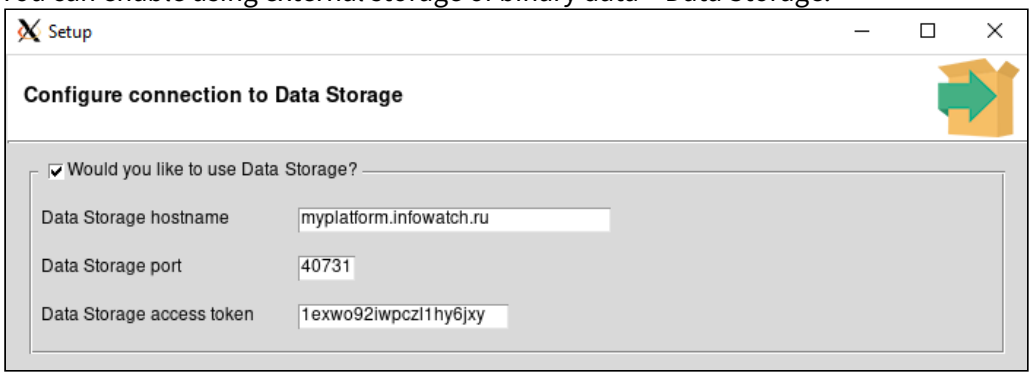
- **Path to archiving** - path to archived tablespaces files storage directory.

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.

> **Note:**
>
> If you will use Data Storage, then, for archiving tablespaces, you need to specify the path to the Data Storage slow disk during the storage installation. For details, see *Installing Platform*.

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. You can enable using external storage of binary data – Data Storage.



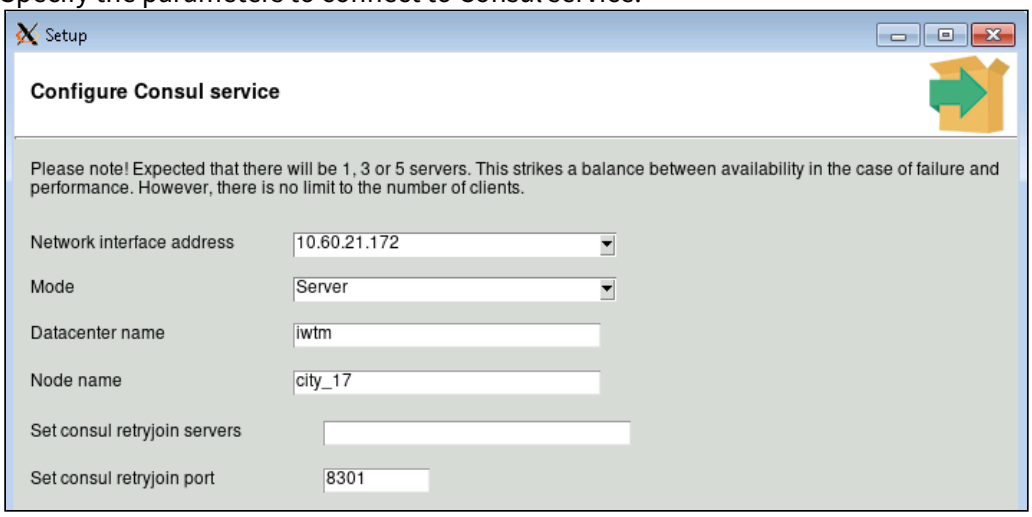
For this, mark the field next to question and specify the parameters for connecting to external storage:

- **`Data Storage hostname`** – hostname or IP address of the server on which the storage is installed
- **`Data Storage port`** – port for connecting to Data Storage. The 40731 port is used by default
- **`Data Storage access token`** – Data Storage authorization token

You can find the actual value of the token:

- On the Data Storage server, via the command line. For this:
  a. Go to the directory where the Platform distribution kit was extracted.
  b. Run the command:
  `./setup.py tokens list`
  As a result, you will see a list of tokens for connecting to the Platform. The actual Data Storage authorization token will be displayed opposite the *DataStorageUser* identity.
- In the Platform product management console, in the **Token for Data Storage User** field of the **Global settings** section. Available if the Platform product with web interface is installed on the server with Data Storage and the web interface contains such a setting.

12. 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. 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.

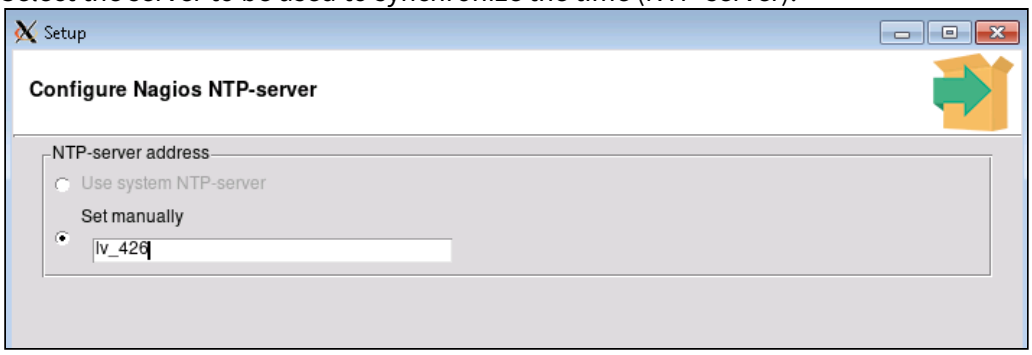
c. **`Database name`** - The name of database to be used, where the scheme is to be added.

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.

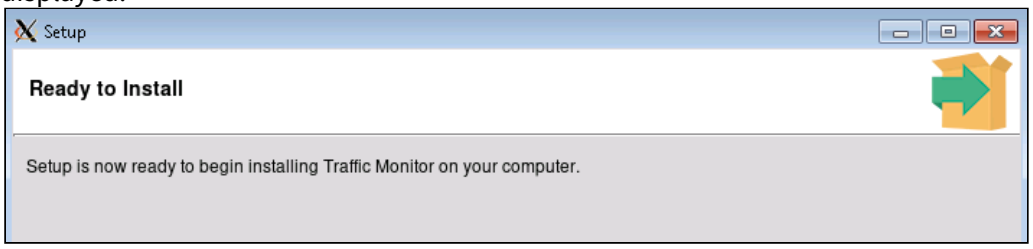
f. **`Consul retryjoin port –`** connection port to specified Consul servers.

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

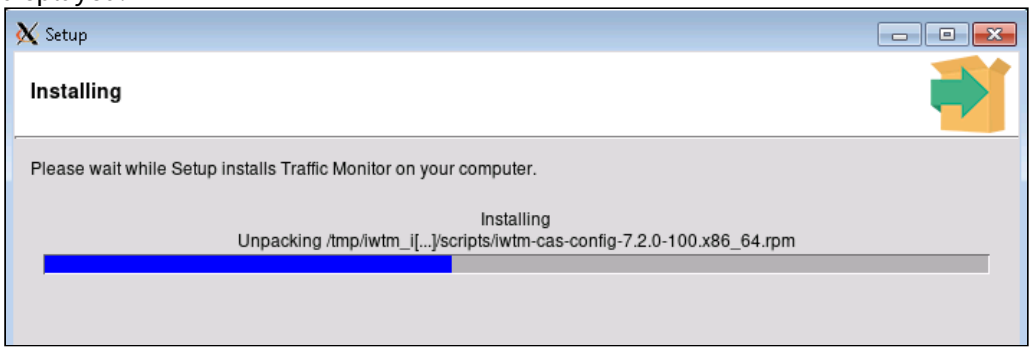


- `Use system NTP-server`;
- `Set manually` - you can manually specify NTP server name. If selected, you should input IP address or NTP server available.

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



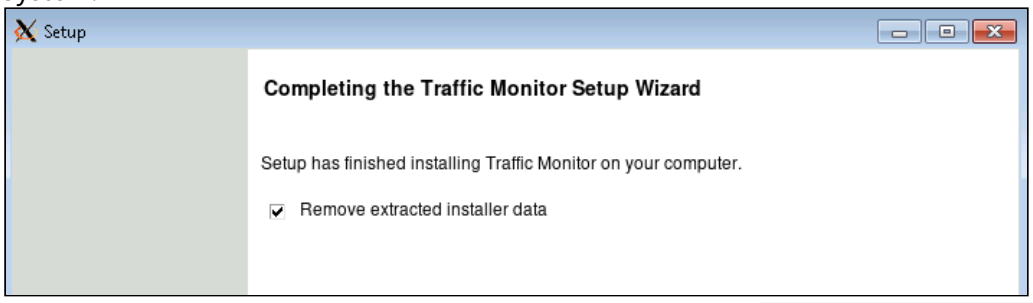
To start the installation and press **Nex**t
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed.



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.

15. 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`.

16. To finalise the installation press **Finish**.
17. To apply the environment change you should certainly log off the System and log in again or restart the server.

18. If you require the list of Traffic Monitor services to be displayed enter the command as follows:
`iwtm status`

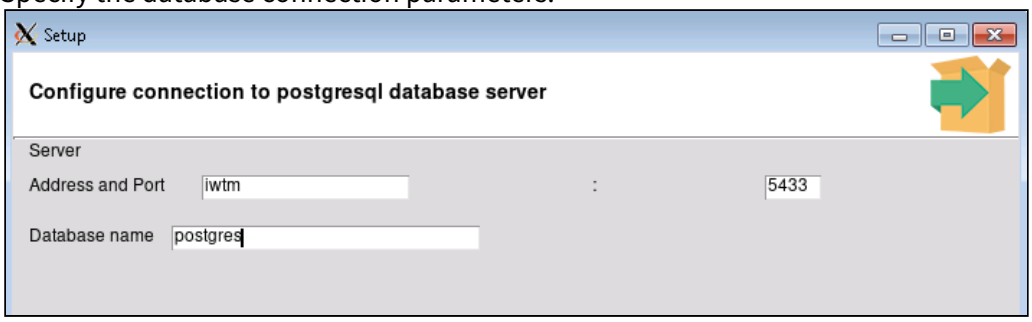
Installing Indexer template

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.

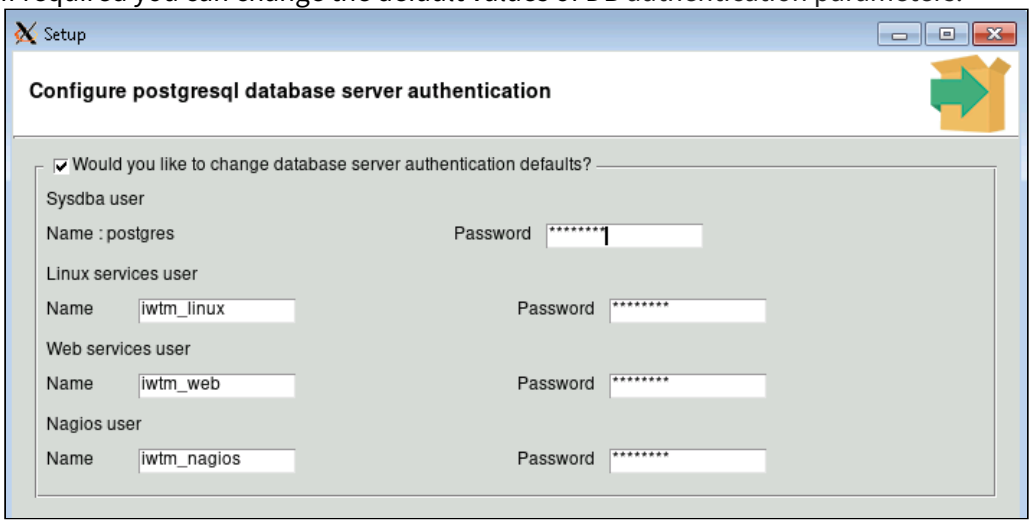
2. Specify the database connection parameters:



   - **`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.

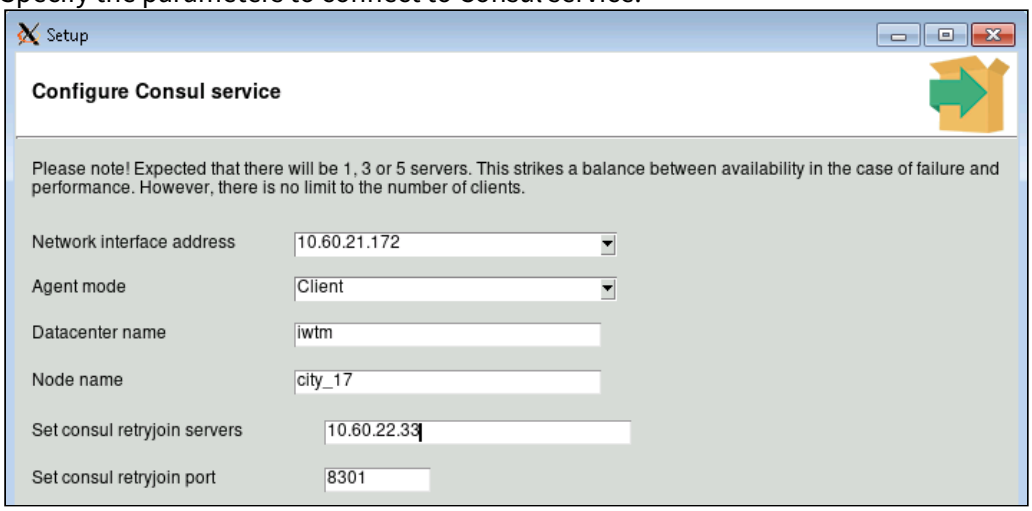
3. If required you can change the default values of DB authentication parameters.



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:

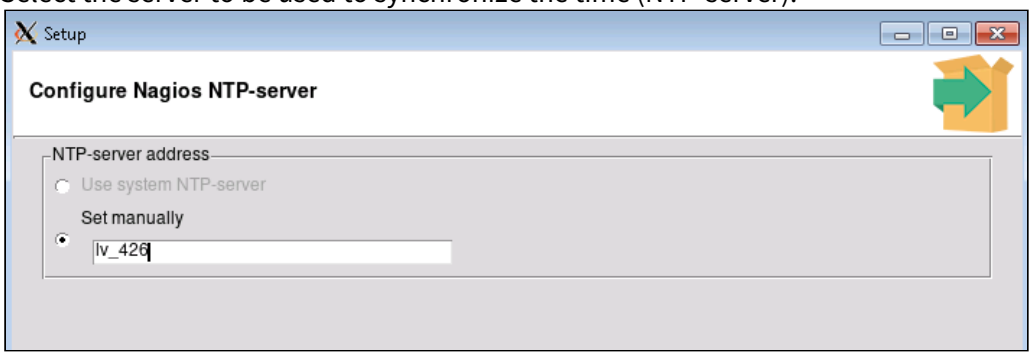


a. **Network interface address** - select IP address of network interface. To select from the list of parameters click ▼ and select the required value.
b. Consul operation mode. Two modes are available:
   - **Server**
   - **Client**

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

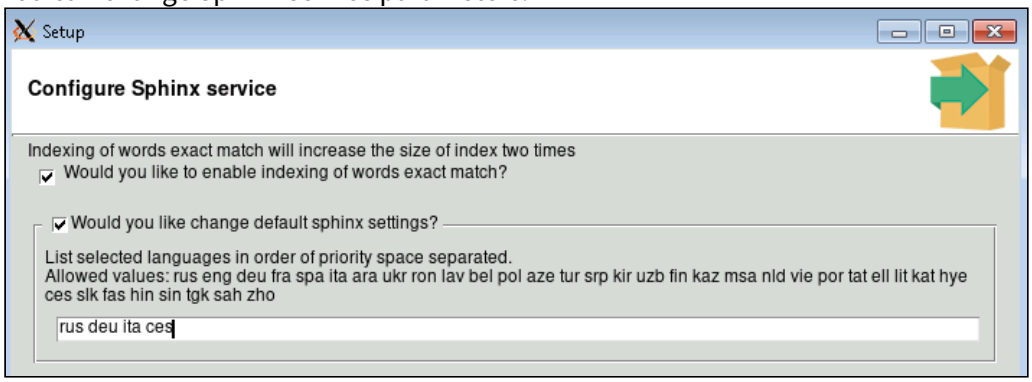
c. **Database name** - The name of database to be used, where the scheme is to be added.
d. **Node name** - server name, where Traffic Monitor components are installed.
e. **Consul retryjoin servers** - list of Consul servers, which are required to connect to. Input values via comma separated list. If 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 change Sphinx service parameters:



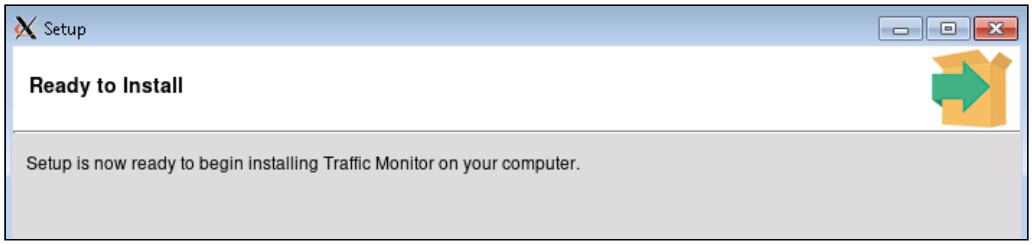
- `Enable indexing of words exact match`;

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

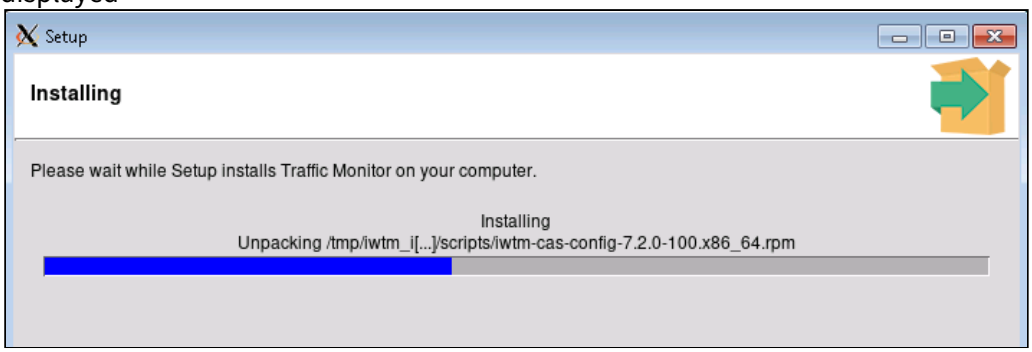
- If required, you can change the standard configuration of Sphinx service operation (`default sphinx settings`). In this case specify a list of languages including morphological support. Indexing will be performed according to selected languages. You can specify few languages using a space to separate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



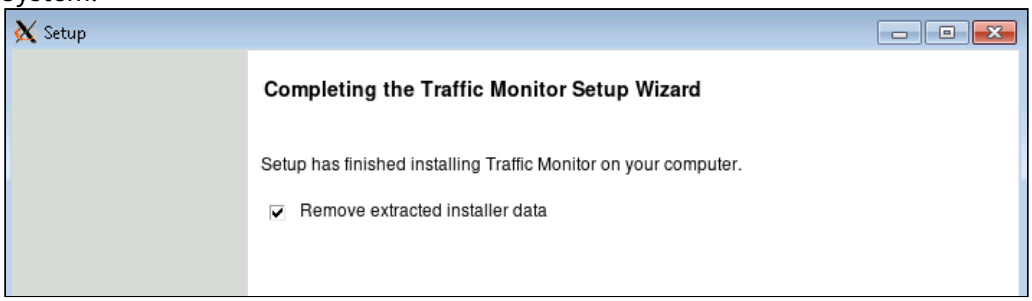
To start the installation and press **Nex**t
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed



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

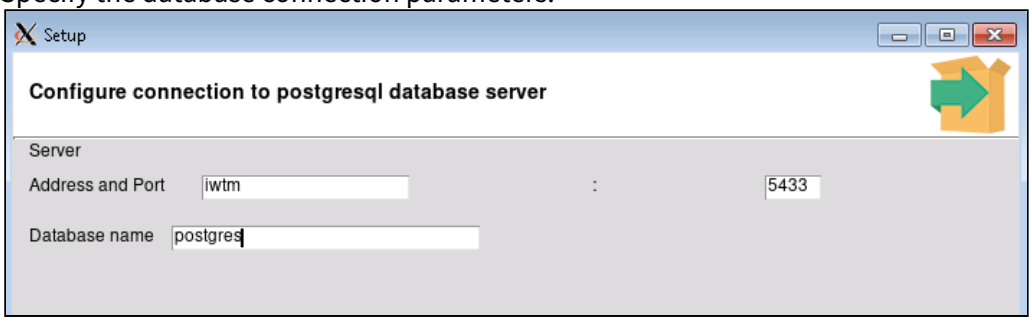
If you've selected Interceptors installation template:

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.

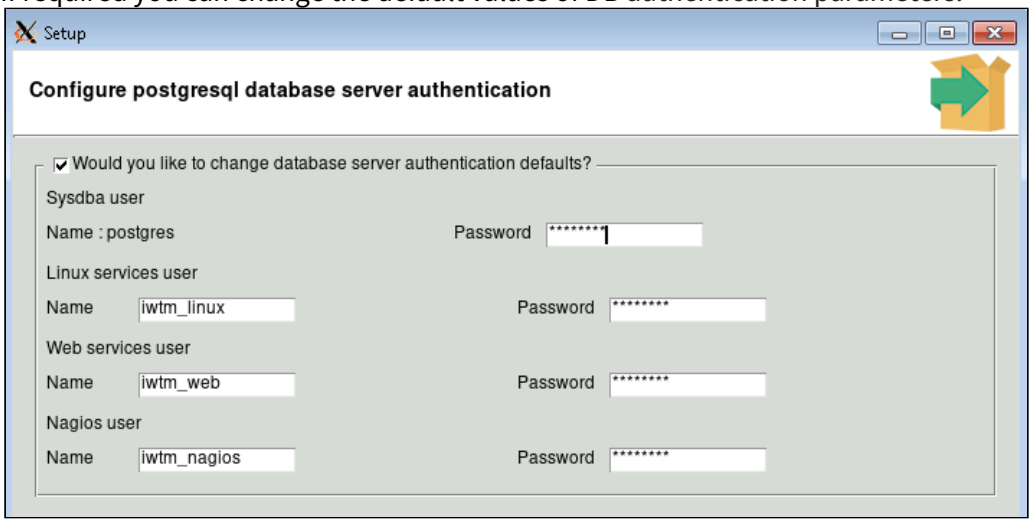
2. Specify the database connection parameters:



- **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.

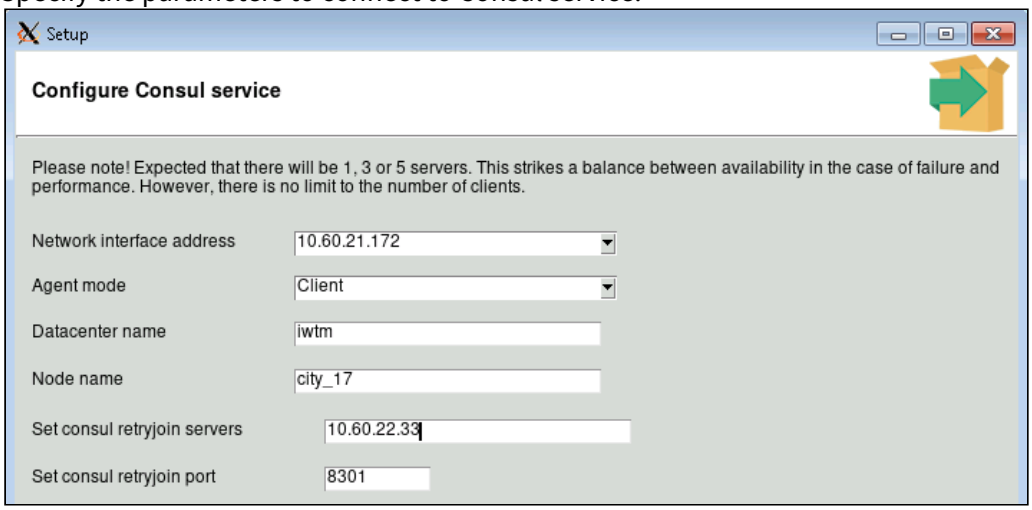


To edit the values mark the field next to question. This will let you edit the following sections:

- **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:

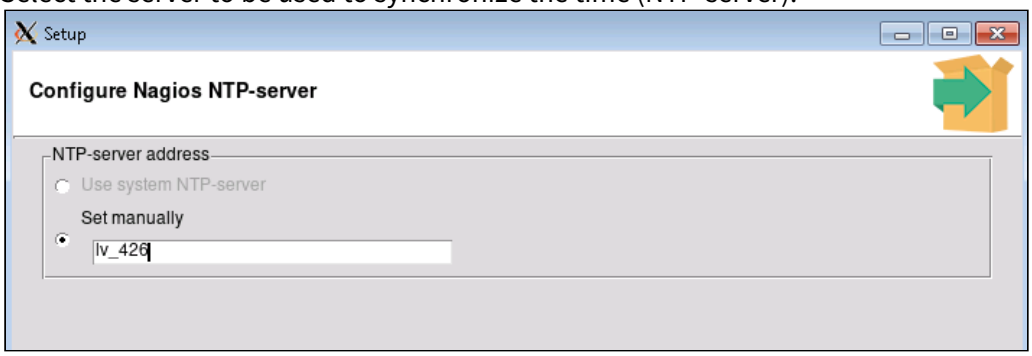


- **Network interface address** - select IP address of network interface. To select from the list of parameters click ▼ and select the required value.
- Consul operation mode. Two modes are available:
  - **Server**
  - **Client**

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

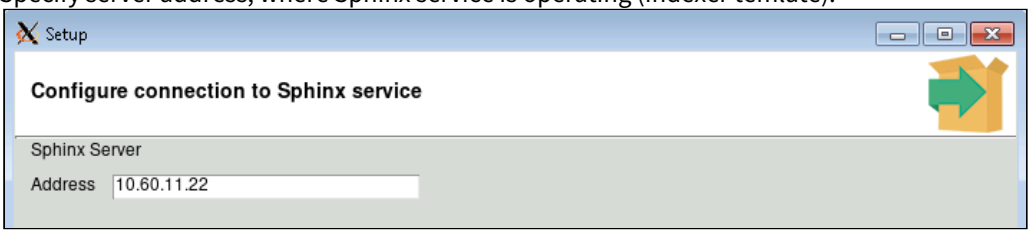
- **Database name** - The name of database to be used, where the scheme is to be added.
- **Node name** - server name, where Traffic Monitor components are installed.
- **Consul retryjoin servers** - list of Consul servers, which are required to connect to. Input values via comma separated list. If you 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).



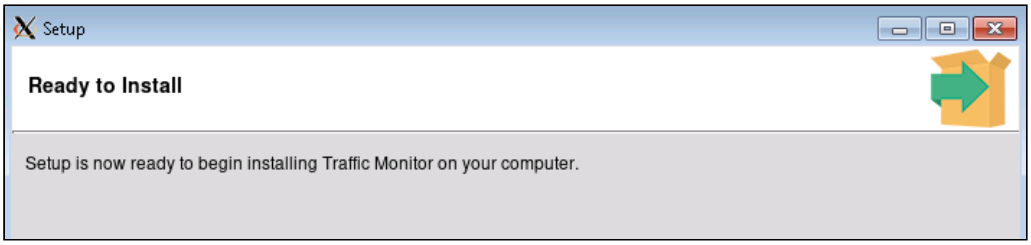
> **Note:**
>
> In case Indexer and Web console templates are installed on one server, this parameter will not be requested by installer.

- You can enable OCR technology.

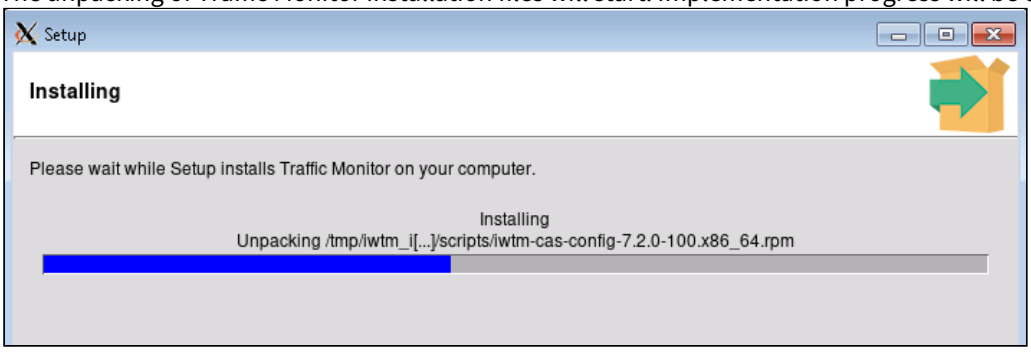


> **Note:**
>
> OCR is to be selected when installing Interceptors template.

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



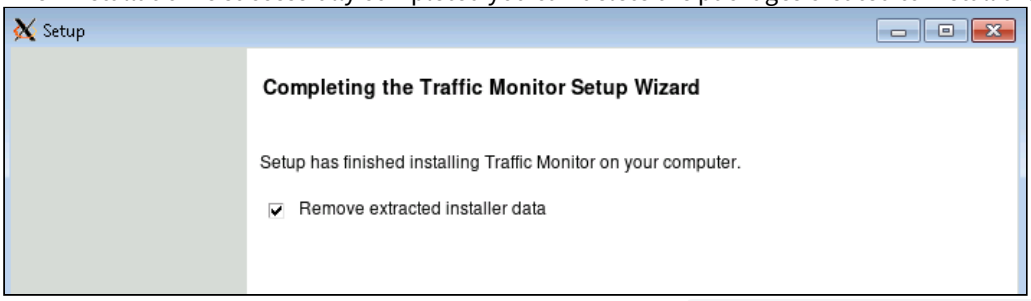
To start the installation and press **Nex**t
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed



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

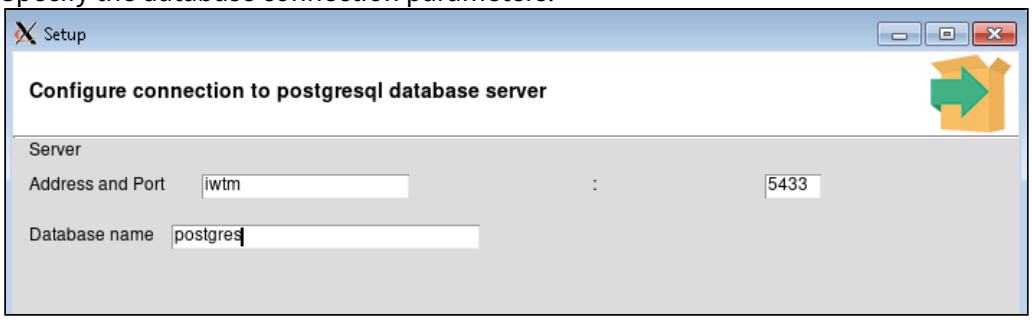
If you've selected Interceptors installation template:

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.

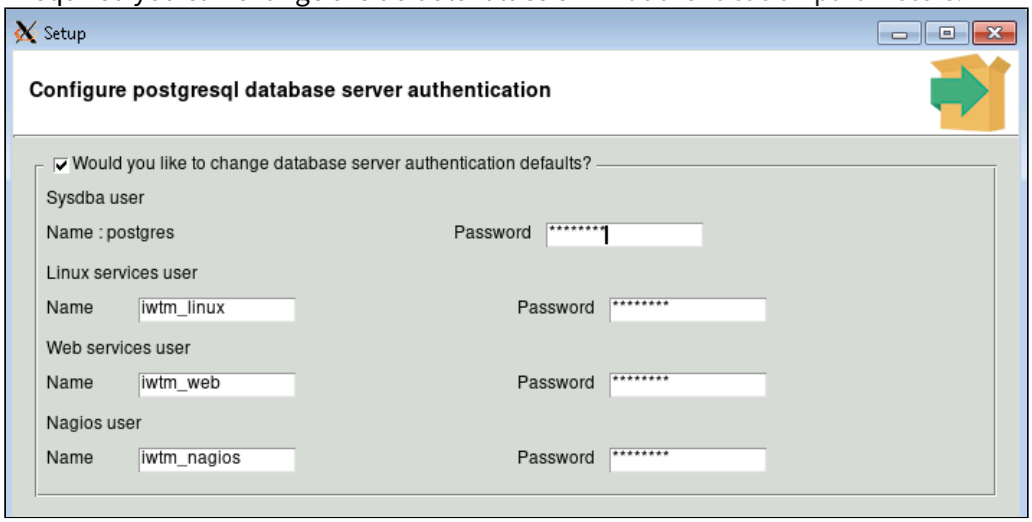
2. Specify the database connection parameters:



- **`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.

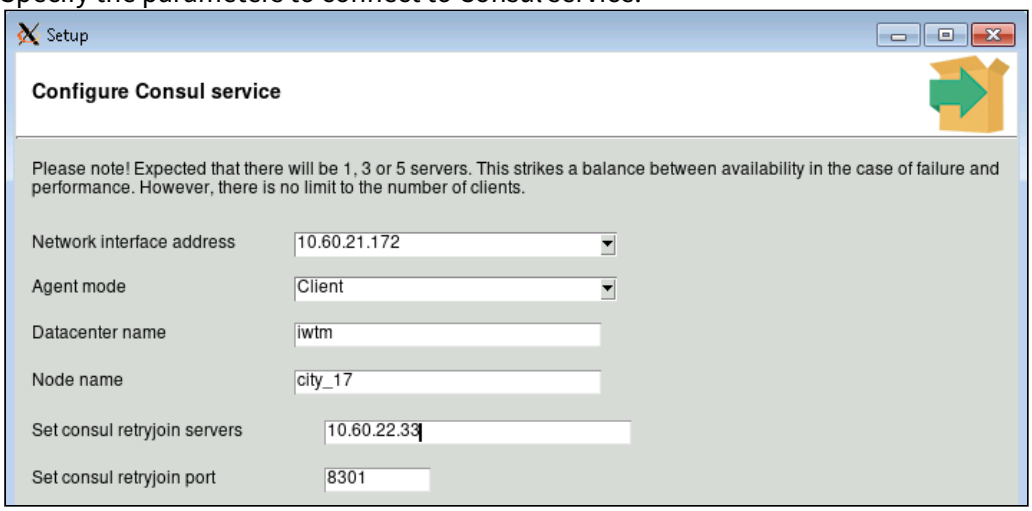
3. If required you can change the default values of DB authentication parameters.



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:

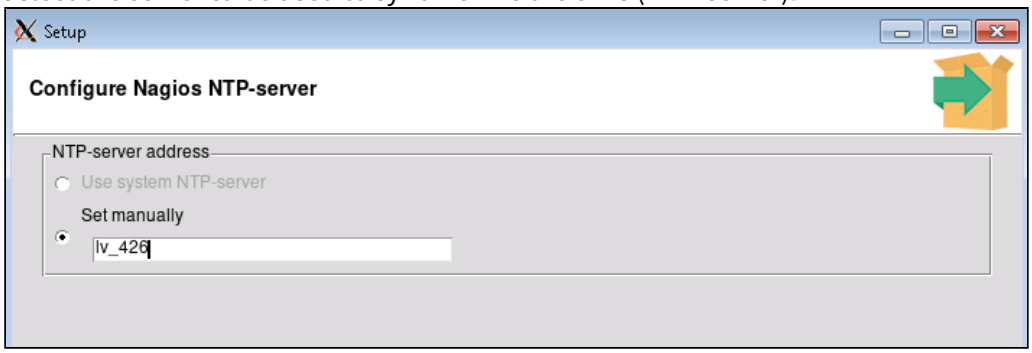


- **`Network interface address`** - select IP address of network interface. To select from the list of parameters click ▼ and select the required value.
- Consul operation mode. Two modes are available:
  - **`Server`**
  - **`Client`**

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

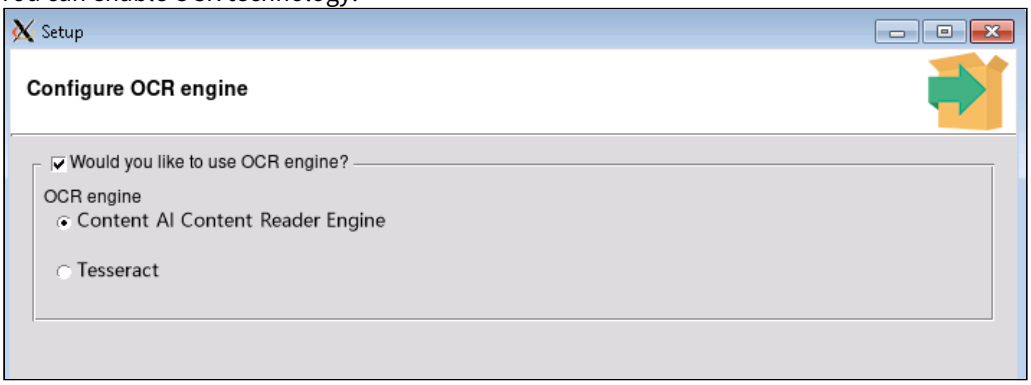
- **`Database name`** - The name of database to be used, where the scheme is to be added.
- **`Node name`** - server name, where Traffic Monitor components are installed.
- **`Consul retryjoin servers`** - list of Consul servers, which are required to connect to. Input values via comma separated list. 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.

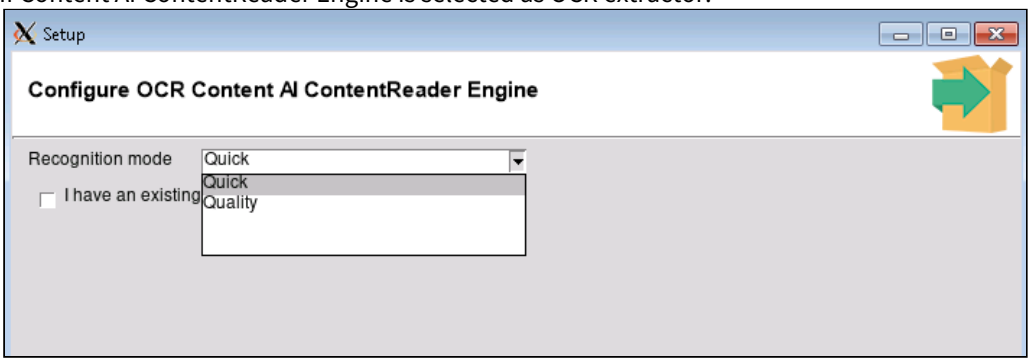


In this case you should select one system to be used:

- `Content AI ContentReader Engine`;
- `Tesseract`.

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

- If Content AI ContentReader Engine is selected as OCR extractor:

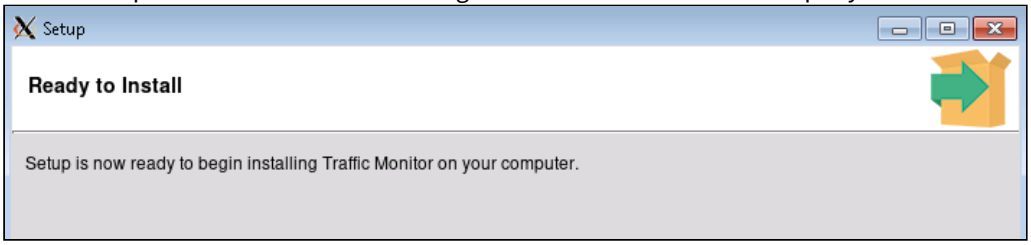


Select a recognition mode:

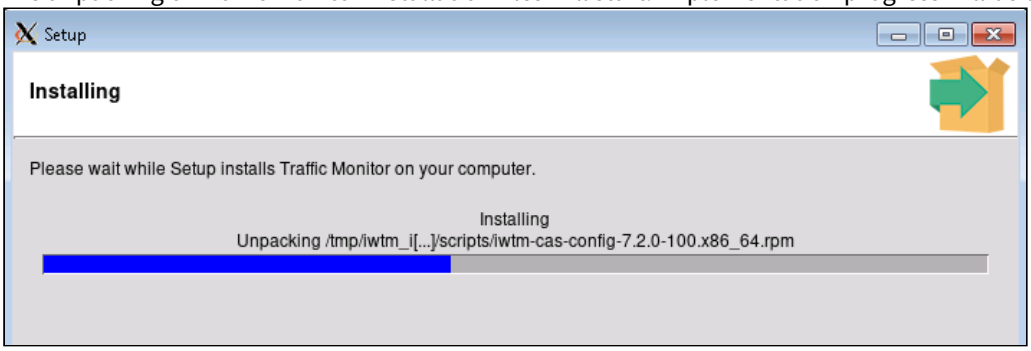
- `Quick` – a fast mode;
- `Quality` – a detailed mode providing higher quality of recognition.

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

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



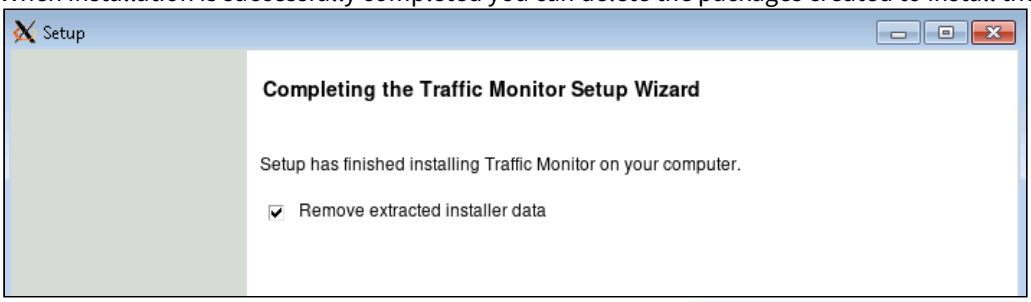
To start the installation and press **Next**.
The unpacking of Traffic Monitor installation files will start. Implementation progress will be displayed.



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.

- 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`

If you installed Traffic Monitor components on Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS, recover the original OS release file.

For this:

1. Run the command depending on OS:
   - in Oracle Linux 8:
     `mv /etc/release.bak /etc/oracle-release`
   - in AlmaLinux 8 or Rocky Linux 8:

     ```
     mv /etc/release.bak /etc/redhat-release
     ```
2. Confirm overwriting of the file. For this, enter " `yes` " and press **Enter**.
3. Check that the original release file is successfully recovered. For this, run the command:

   ```
   lsb_release -a
   ```

As a result, the information on your OS should be displayed. For example, for AlmaLinux 8 OS, the following will be displayed:

```
Distributor ID: AlmaLinux
Description:    AlmaLinux release 8.10 (Cerulean Leopard)
Release:        8.10
Codename:       CeruleanLeopard
```

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

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 and 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*.

The list of processes to be run on one server only 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 *InfoWatch Traffic Monitor. Administration Guide. 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.

3.2.3 Installing the System in Silent Mode Using Parameter File

The silent installation mode allows you to minimize involvement in the installation process. In this mode Traffic Monitor can be installed using default parameters.

The installer allows you to use an option file. In this file, you can set required installation parameters. When starting the installation with an option file, the values specified in this file will be considered the default parameters.

Thus, using the silent mode and the prepared option file allows you to install Traffic Monitor with little or no user intervention.

> **Warning!**
>
> By default, installing the System is not allowed on a server whose name begins with a number. If you want to allow numbers at the beginning of the server name, use the command line to set the `--allow_digits_at_hostname_begin` parameter value to `1`. In this case, it is necessary that the network check is activated, i.e. the `--skip_check_network` parameter value is set to `0` (by default, the check is disabled).

Before starting the installation, perform general steps:

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

Warning!

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

Warning!

If you plan using a remote database (deployed locally or on a separate server), you should *prepare* it first.

Before the installation, in order to clear memory, we recommend rebooting the server where the database will be deployed.

2. Connect external or local OS repositories.
   For example, you can find instructions on how to configure local Red Hat Enterprise Linux repository at the *official web page*.
   If you install Traffic Monitor on RED OS with no internet access

   a. Disable external repositories.
      On a workstation running RED OS version 7.3.3 and below:

      Run the following commands:
      ```
      echo "enabled=0" >> /etc/yum.repos.d/RedOS-Base.repo
      echo "enabled=0" >> /etc/yum.repos.d/RedOS-Updates.repo
      sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/RedOS-kernels.repo
      ```

      On a workstation running RED OS version 7.3.4 or 7.3.5:

      Run the command:
      ```
      sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/RedOS-*.repo
      ```

   b. Connect the disk with the RED OS distribution kit to the server.
   c. Mount the disk with the RED OS distribution kit using the command:
      `mkdir -p /media/cdrom/ && mount /dev/cdrom /media/cdrom/`
   d. Create the `/etc/yum.repos.d/cdrom.repo` file and specify the the mounted disk as the repository. For this, use the command:
      ```
      cat << EOF > /etc/yum.repos.d/cdrom.repo
      [cdrom]
      name=cdrom
      baseurl=file:///media/cdrom/
      enabled=1
      gpgcheck=0
      EOF
      ```
   e. Delete the temporary files and make sure that the list of repositories contains the repository on the disk:
      `yum clean all && yum repolist`
   f. Install `libpq` library and `python2` package:
      `yum install libpq python2`
   g. Install the following packages:

Package name	Official repository
`lshw-B.02.19.2-1.el7.x86_64.rpm`	*RED OS - Updates*
`lz4-1.9.4-1.el7.x86_64.rpm`	
`python3-psycopg2-2.9.3-1.el7.x86_64.rpm`	
`urw-base35-fonts-legacy-20170801-11.el7.noarch.rpm`	*RED OS – OS*
`libxslt-1.1.34-1.el7.x86_64.rpm`	

For this:

i. Download the specified packages from the official RED OS repository.
ii. Copy them to the server where you are going to install Traffic Monitor.
iii. Go to the directory where the specified packages were copied.
iv. Run the following command:
`yum localinstall lshw-B.02.19.2-1.el7.x86_64.rpm lz4-1.9.4-1.el7.x86_64.rpm python3-psycopg2-2.9.3-1.el7.x86_64.rpm urw-base35-fonts-legacy-20170801-11.el7.noarch.rpm libxslt-1.1.34-1.el7.x86_64.rpm`

> **Note:**
>
> Additionally, you can install utilities for working with the operating system. For this, run the command:
> `yum install mc vim screen telnet bind-utils mlocate net-tools iptraf sysstat iotop rsync`
>
> Or you can install the *htop* utility by downloading it from *the official RED OS repository*.

h. Make sure your network settings are correct (see *Operating System and Network Server Configuration Requirements*) and the `/etc/hosts` file contains instructions for converting a server name to an IP address. If the instructions are missing, run the command:
`sh -c "echo '<IP_адрес> `hostname -f` `hostname -s`' >> /etc/hosts"`

If you install Traffic Monitor on OS Oracle Linux with no internet access:

a. Make sure that, in operating system, the current kernel is Red Hat Compatible Kernel (RHCK), for example, Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`, and the UEK kernel is removed. For details, see *Operating System and Network Server Configuration Requirements*.
b. Disable external repositories by running the following command:
`find /etc/yum.repos.d/ -iname "*.repo" -exec sed -i -e "s/enabled=.*/enabled=0/g" {} \;`
c. Connect the disk with the OS Oracle Linux distributive to the server.

d. Mount the disk with the OS Oracle Linux distributive, using the following command:
`mkdir -p /media/cdrom/ && mount /dev/cdrom /media/cdrom/`
e. Create the `/etc/yum.repos.d/cdrom.repo` file specifying the mounted disk as a repository. For this, run the following command:
```
cat << EOF > /etc/yum.repos.d/cdrom.repo
[cdrom]
name=cdrom
baseurl=file:///media/cdrom/
enabled=1
gpgcheck=0
EOF
```
f. Remove temporary files and make sure that repository list contains the repository from the disk:
`yum clean all && yum repolist`
g. Install `Perl`:
`yum install perl`
h. Install the following packages:
   - `perl-List-MoreUtils-0.33-9.el7.x86_64.rpm` (you can download the package from *the official Oracle Linux 7 Latest repository*)
   - `perl-Dist-CheckConflicts-0.06-2.el7.noarch.rpm` (you can download the package from *the official Oracle Linux 7 Optional Latest repository*)
   - `urw-base35-fonts-legacy-20170801-10.el7.noarch.rpm` (you can download the package from *the official Oracle Linux 7 Optional Latest repository*)

   For this:
   i. Download the listed packages from the official Oracle Linux repositories.
   ii. Copy them to the server where Traffic Monitor is to be installed.
   iii. Go to the directory where you copied the packages.
   iv. Run the following command for each package:
   `rpm -ivh <package_name>`

   > **Note:**
   >
   > Optionally you can install tools for work in operating system by running the command:
   > `yum install mc vim screen telnet bind-utils mlocate net-tools iptraf sysstat iotop rsync`

i. Make sure you have correctly configured network settings (see *Operating System and Network Server Configuration Requirements*) and the `/etc/hosts` file contains the hostname resolving setting. If it does not, run the command:
`sh -c "echo '<IP_address> `hostname -f` `hostname -s`' >> /etc/hosts"`

If you install Traffic Monitor on Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS:

> **Warning!**

Make sure that, in Oracle Linux 8.10 operating system, the current kernel is Red Hat Compatible Kernel (RHCK), for example, Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`, and the UEK kernel is removed. For details, see *Operating System and Network Server Configuration Requirements*.

a. Install the `redhat-lsb-core` package by running the following command:

```
dnf install redhat-lsb-core
```

b. Create a backup copy of the OS release file and replace the content of the original file. For this, run the commands depending on OS:
   - in Oracle Linux 8:

```
cp /etc/oracle-release /etc/release.bak

echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/oracle-release
```

   - in AlmaLinux 8 or Rocky Linux 8:

```
cp /etc/redhat-release /etc/release.bak
echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/redhat-release
```

c. Run the command:

```
lsb_release -a
```

As a result, the following information should be displayed:

```
Distributor ID: RedHatEnterprise
Description:    Red Hat Enterprise Linux release 8.10 (Ootpa)
Release:        8.10
Codename:       Ootpa
```

> **Note:**
>
> After installing Traffic Monitor, recover the original OS release file. For details, see *below*.

3. 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`
4. Copy the files from InfoWatch Traffic Monitor distributive – installer and archive with DBMS components – into the created directory:

OS	Distribution files
Red Hat Enterprise Linux 7	**Installer**: `iwtm-installer-x.x.x.xxx-rhel7`

OS	Distribution files

Oracle Linux 7 [4]	**Archive with DBMS components** [1] [2]:
	PostgreSQL:
	`iwtm-postgresql-15.14-x.x.x.xxx-rhel7.tar.gz`
	Oracle [3]:
	`iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz`

RED OS	**Installer**:
	`iwtm-installer-x.x.x.xxx-redos-7.3`
	Archive with DBMS components [1] [2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-redos-7.3.tar.gz`

Red Hat Enterprise Linux 8
Oracle Linux 8
AlmaLinux 8
Rocky Linux 8
	Installer:
	`iwtm-installer-x.x.x.xxx-rhel8`
	Archive with DBMS components [1] [2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-rhel8.tar.gz`

Alt Server	**Installer**:
	`iwtm-installer-x.x.x.xxx-altlinux-10`
	Archive with DBMS components [1] [2]:
	`iwtm-postgresql-15.10-x.x.x.xxx-altlinux-10.tar.gz.md5`

Important!

[1] Archive with DBMS components is required *both* when installing DBMS distributed with the product (`local` mode) *and* when using an already deployed DBMS in *remote* mode. See *System Deployment Schemes and Installation Types* for details.

[2] In case you are planning to use an already deployed PostgreSQL-based DBMS, use an archive from PostgreSQL column. For the list of supported PostgreSQL-based DBMS, see *Hardware and Software Requirements*.

[3] If you use Oracle DBMS and network file system (NFS), before launching the installer:

- **When not using RAC:**

  Open settings of the mount point (by default, `/etc/fstab`) and make sure that the `noac` option is not used and the `actimeo` parameter has the `0` value.

  For details, see *the article on the official site*.

- **When using Oracle Real Application Clusters (RAC):**

Set the options for mounting in accordance to *the article on the official site*.

[4] For Traffic Monitor installed on a server running Oracle Linux 7, Postgres Pro Enterprise DBMS is not supported.

Installation using distributive files for Red Hat Enterprise Linux 7 will be described further. In our example, we need to copy an installer file and an archive with DBMS components:

- Installer:
  `iwtm-installer-7.15.0.97-rhel7`
  `where 7.15.0.97` is the build number, `rhel7` is the OS designation;
- Archive with DBMS components:
  - In case of PostgreSQL (or one of supported PostgreSQL-based DBMS):
    `iwtm-postgresql-15.14-7.15.0.97-rhel7.tar.gz`
    where `postgresql-15.14` is the DBMS designation, `7.15.0.97` is the build number, `rhel7` is the OS designation;
  - In case of Oracle DBMS:
    `iwtm-oracle-19.0.0.0.0-7.15.0.97.tar.gz`
    where `oracle-19.0.0.0.0` is the DBMS designation, `7.15.0.97` is the build number.

This instruction is relevant for other supported OS: Oracle Linux, RED OS, AlmaLinux, Rocky Linux and Alt Server.

5. Enter the command to shift to Traffic Monitor distributive directory.
   As per our example:
   `cd /distr`
6. 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-7.15.0.97-rhel7`

Parameter file (option file)

In the file, parameters are described as follows:

`<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
use_data_storage=1
ds_set_host=example.host.com
ds_set_port=40731
```

```
ds_set_token=hcb90t4it745zl1hycg43
```

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.
- Connection to the external storage of binary data.

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` and specifying the file which was previously created.

Example of using parameter file:

```
./iwtm-installer-7.15.0.97-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:

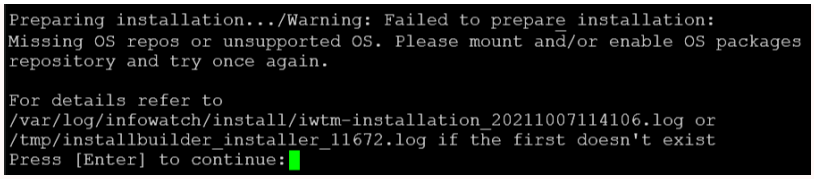
- `none` – no information displayed while installing and no interaction is required;
- `minimal` – status of implementation is displayed while installing, no interaction is required;
- `minimalWithDialogs` – status of implementation is displayed while installing, pop-up windows can be displayed and interaction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

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

```
./iwtm-installer-7.15.0.97-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 OS 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:



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.

After Traffic Monitor is installed on Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS, recover the original OS release file.

For this:

1. Run the command depending on OS:
   - in Oracle Linux 8:
     `mv /etc/release.bak /etc/oracle-release`

- in AlmaLinux 8 or Rocky Linux 8:

```
mv /etc/release.bak /etc/redhat-release
```

2. Confirm overwriting of the file. For this, enter " `yes` " and press **Enter**.
3. Check that the original release file is succesfully recovered. For this, run the command:

```
lsb_release -a
```

As a result, the information on your OS should be displayed. For example, for AlmaLinux 8 OS, the following will be displayed:

```
Distributor ID: AlmaLinux
Description:    AlmaLinux release 8.10 (Cerulean Leopard)
Release:        8.10
Codename:       CeruleanLeopard
```

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, Postgres Pro, Jatoba or Tantor DBMS.

Name	Description
`use_debug`	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 occurred while the installer operation. Values: `0` (default), `1`

Name	Description
`skip_check_swap`	Disabling the check of Swap space volume Values: `0` (default), `1`
`skip_check_space`	Disabling the check of free space volume on disk Values: `0` (default), `1`
`skip_check_ram`	Disabling the check of RAM volume Values: `0` (default), `1`
`skip_check_network`	Disabling the check of available network Values: `0` (default), `1`
`skip_check_tmp`	Disabling the check of temporary directory Values: `0` (default), `1`
`skip_check_home`	Disabling the check of home directory Values: `0` (default), `1`
`setup_cron_jobs`	Set targets for cron planner Values: `0` , `1` (default)

Name	Description
`log_dir`	Path to log files directory Default value: `/var/log/infowatch/install`
`eula`	Values: • `show` to display the License Agreement text • `accept` to accept the License Agreement without preview If you run the installation not in the unattended mode and do not specify the parameter, then the License Agreement text will be displayed. You will be asked to accept the agreement. If you run the installation in the unattended mode, this parameter value is ignored and the License Agreement is accepted by default

Name	Description
`product_type`	Traffic Monitor edition type: • `tme` (default) • `tms`
`product_language`	Main product language: • `rus` (default) • `eng`
`installation_type`	Installation type The parameter is used in case Traffic Monitor Enterprise edition is selected (`product_type=tme`). Values: • `distributed` • `all_in_one` (default)
`template_database`	Install Database template The parameter is used in case distributed installation is selected (`installation_type=distributed`). Values: `0` (default), `1`

Name	Description
`template_indexer`	Install Indexer template The parameter is used in case distributed installation is selected (`installation_type=distributed`). Values: `0` (default), `1`
`template_web`	Install Web console template The parameter is used in case distributed installation is selected (`installation_type=distributed`). Values: `0` (default), `1`
`template_interceptors`	Install Interceptors template The parameter is used in case distributed installation is selected (`installation_type=distributed`). Values: `0` (default), `1`
`db_classification_lang_ru`	Set Russian for classification base

Name	Description
	The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Values: 1, `0` (default)
`db_classification_lang_en`	Set English for classification base The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Values: `0` (default), `1`
`db_installation_type`	Database location The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database

Name	Description
	template (`template_database=1`) is selected. Values: `local` (default), `remote` The option `local` is supported only for DBMS included in the distribution kit.
`db_type`	Selecting DBMS The parameter is used in case edition type is Traffic Monitor Enterprise `(product_type=tme)`. Values: `postgresql` (default), `oracle` Select `postgresql`: • If you install Traffic Monitor on Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS and/or • If you use Postgres Pro Enterprise

Name	Description
	, Jatoba or Tantor DBMS.
`db_server_address`	Server address with Database template or remote database server address The parameter is used: • 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`) Default value: `iwtm` To install Traffic Monitor on the same server with already deployed DBMS Postgres Pro Enterprise, specify the address: `127.0.0.1` .

Name	Description
`db_server_port`	Server port with database The parameter is used: • 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_name`	Database name: `postgres` or `iwtm` (according to `db_type` parameter) The parameter is used: • For Indexer, Interceptors and Web console templates • For All-in-One installation type and

Name	Description
	Database template when using a remote database (`db_installation_type=remote`)
`db_sysdba_password`	Password of SYSDBA user Default value: `xxXX1234`
`db_scheme_owner_name`	Name of database security scheme owner The parameter is used 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. Default value: `iwtm`
`db_scheme_owner_password`	Password for database scheme owner

Name	Description
	The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Default value: `xxXX1234`
`db_linux_user_name`	Name of Linux services user Default value: `iwtm_linux`
`db_linux_user_password`	Password of Linux services user Default value: `xxXX1234`
`db_web_user_name`	Name of web services user Default value: `iwtm_web`
`db_web_user_password`	Password of web services user Default value: `xxXX1234`
`db_nagios_user`	Name of nagios user Default value: `iwtm_nagios`
`db_nagios_password`	Password of nagios user

Name	Description
	Default value: `xxXX1234`
`db_auth_change_defaults`	Change the default database connection parameters Values: `0` (default), `1`
`db_storage_type`	Data storage mode Values: `normal` (default), `fast_slow`, `rotate`
`db_storage_main_tbs_path`	Path to main tablespace Default value: `/u02/<ora|pg>data`
`db_storage_dtbs_paths_number`	Number of paths to daily tablespaces Values: `1` - `10` Default value: `1`
`db_storage_fast_disk_path`	Path to directory where daily tablespaces are stored on fast drive The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database

Name	Description
	template (`template_database=1`) and `fast_slow` data storage mode (`db_storage_type=fast_slow`) are selected. Default value: `/u03/<ora|pg>data`
`db_storage_dtbs_days_on_fast_disk`	Storage period of daily tablespaces data on fast drives, in days The parameter is used 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_type=fast_slow`) are selected. Default value: `7`
`db_storage_change_defaults`	Change the database

Name	Description
	storage parameters Values: `0` (default), `1`
`db_storage_dtbs_path_1`	Path to daily tablespace #1 The parameter (as well as other parameters specifying paths to daily tablespaces) is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Also depends on the `db_storage_dtbs_paths_number` parameter value. Default value: `/u02/<ora|pg>data1`
`db_storage_dtbs_path_2`	Path to daily tablespace #2 Default value: `/u02/<ora|pg>data2`
`db_storage_dtbs_path_3`	Path to daily tablespace #3 Default value: `/u02/<ora|pg>data3`

Name	Description
`db_storage_dtbs_path_4`	Path to daily tablespace #4 Default value: `/u02/<ora|pg>data4`
`db_storage_dtbs_path_5`	Path to daily tablespace #5 Default value: `/u02/<ora|pg>data5`
`db_storage_dtbs_path_6`	Path to daily tablespace #6 Default value: `/u02/<ora|pg>data6`
`db_storage_dtbs_path_7`	Path to daily tablespace #7 Default value: `/u02/<ora|pg>data7`
`db_storage_dtbs_path_8`	Path to daily tablespace #8 Default value: `/u02/<ora|pg>data8`
`db_storage_dtbs_path_9`	Path to daily tablespace #9 Default value: `/u02/<ora|pg>data9`
`db_storage_dtbs_path_10`	Path to daily tablespace #10 Default value: `/u02/<ora|pg>data10`
`db_archiving_dtbs_path`	Path to directory where archived

Name	Description
	tablespaces are stored The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Default value: `/u02/arch` **Note:** If you will use Data Storage, then, for archiving tablespaces, you need to specify the path to the Data Storage slow disk during the storage installation. For details, see *Installing Platform*.
`db_days_before_archiving_nonviolations`	Number of days to store events without violations before archiving The parameter is used in case All-in-One installation type (`installation_type=all`

Name	Description
	`_in_one`) or Database template (`template_database=1`) is selected, and `db_archive_nonviolations=1` . Default value: `45`
`db_archive_nonviolations`	Archive events without violations The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Values: `0` (default), `1`
`db_days_before_archiving_violations`	Number of days to store events with violations before archiving The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_d`

Name	Description
	`atabase=1`) is selected, and `db_archive_violations=1` . Default value: `45`
`db_archive_violations`	Archive events with violations The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Values: `0` (default), `1`
`db_days_before_archiving_screenshots`	Number of days to store screenshots before archiving The parameter is used 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` .

Name	Description
	Default value: `45`
`db_archive_screenshots`	Archive screenshot events The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Values: `0` (default), `1`
`db_archiving_dtbs_change_defaults`	Change default archiving parameters Values: `0` (default), `1`
`db_days_before_removing_nonviolations`	Number of days to store events without violations before deleting The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected, and `db_remove_`

Name	Description
	`nonviolations=1`. Default value: `90`
`db_remove_nonviolations`	Delete events without violations The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Values: `0` (default), `1`
`db_days_before_removing_violations`	Number of days to store events with violations before deleting The parameter is used 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`. Default value: `90`

Name	Description
`db_remove_violations`	Delete events with violations The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Values: `0` (default), `1`
`db_days_before_removing_screenshots`	Number of days to store screenshot events before deleting The parameter is used 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` . Default value: `90`
`db_remove_screenshots`	Delete screenshot events The parameter is used in case All-in-One installation

Name	Description
	type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Values: `0` (default), `1`
`db_removing_dtbs_change_defaults`	Change default deleting parameters Values: `0` (default), `1`
`use_data_storage`	Use external storage of binary data – Data Storage The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected Values: `0` , `1` (default) **Important!** Make sure the connection parameter values (address, port and token; see the description below) are correct.
`ds_set_host`	Hostname or IP address of the server on which

Name	Description
	the storage is installed The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. **Important!** The parameter is **required**. In case you do not wish to establish connection with Data Storage, assign `any_data` value.
`ds_set_port`	Port for connecting to Data Storage The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Default value: `40731`
`ds_set_token`	Data Storage authorization token The parameter is used in case All-in-One

Name	Description
	installation type (`installation_type=all_in_one`) or Database template (`template_database=1`) is selected. Default value: `1exwo92iwpczl1hy6jxy` You can find the actual value of the token: • On the Data Storage server, via the command line. For this: 1. Go to the directory where the Platform distribution kit was extracted. 2. Run the command : `./setup.py tokens list` As a result, you will see a list of tokens for connecting to the Platform. The actual Data Storage

Name	Description
	authorization token will be displayed opposite the *DataStorageUser* identity. • In the Platform product management console, in the **Token for Data Storage User** field of the **Global settings** section. Available if the Platform product with web interface is installed on the server with Data Storage and the web interface contains such a setting.
`consul_bind_addr`	Consul network interface address Default value: `<list of ip_addresses>`

Name	Description
`consul_mode`	Consul operation mode, server and client Values: • `server` – for Database template and All-in-One installation type • `client` – for the rest of templates
`consul_datacenter_name`	Consul data center name Default value: `iwtm`
`consul_node_name`	Node name Default value: `<hostname>`
`consul_retryjoin_manual`	List of Consul servers to which agents should connect
`consul_retryjoin_port`	Port to connect Consul agents Default value: `8301`
`ntp_manual_addr`	NTP server address The parameter is used in case NTP server manual specification is selected (`ntp_mode=n`

Name	Description
	`tp_manual_addr`).
`ntp_mode`	NTP server type: • `ntp_use_system` – use system NTP-server (default); • `ntp_manual_addr` – specify NTP server manually.
`sphinx_server_address`	Sphinx server address The parameter is used in case Web console template (`template_web=1`) is selected and Indexer template (`template_indexer=0`) is not selected.
`sphinx_exact_match_words`	Enable exact word match indexing The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or

Name	Description
	Indexer template (`template_indexer=1`) is selected. Values: `0` (default), `1`
`sphinx_change_language_settings`	Change list of sphinx languages Values: `0` (default), `1`
`sphinx_langs`	List of sphinx languages. Sequence of languages defines the priority Values: 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 Default values: `rus`
`ocr_enabled`	Enable OCR using The parameter is used in case All-in-One installation type (`installation_type=all_in_one`), Interceptors template (`template_interceptors`

Name	Description
	`=1`) or Web console template (`template_web=1`) are selected. Values: `0` , `1` (default)
`ocr_type`	Selecting OCR extractor: • `fre` – Content AI ContentReader Engine; • `ts` – Tesseract. The parameter is used in case All-in-One installation type (`installation_type=all_in_one`) or Interceptors template (`template_interceptors=1`) is selected.
`ocr_contentai_mode`	OCR Content AI ContentReader Engine operation mode The parameter is used in case OCR Content AI ContentReader Engine (`ocr_type=f`

Name	Description
	`re`) is selected. Values: `quick` , `quality` (default)
`ocr_contentai_have_license`	License issued for OCR Content AI ContentReader Engine The parameter is used in case OCR Content AI ContentReader Engine (`ocr_type=fre`) is selected. Values: `0` , `1` (default)
`db_unpack_dir`	DB archive will be unpacked to directory Directory will be created automatically. You can specify an existing directory. In case the installation completes without errors, the directory will be removed automatically. Default value: `/tmp/iwtm_installer/database`
`packages_unpack_dir`	Traffic Monitor installation packages will

Name	Description
	be unpacked to directory Directory will be created automatically. You can specify an existing directory. In case the installation completes without errors, the directory will be removed automatically. Default value: `/tmp/iwtm_installer/packages`

3.3 Pre-installed Server Parameters

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

System installation directories:

- Traffic Monitor server components – `/opt/iw`
- Database components – `/u01` and `/u02`

> **Note:**
>
> The directories can be placed on different servers.

After the System is installed, **change the passwords** for:

- `oracle` or `postgres` user, depending on the database you are using;
- Linux account (see details in *InfoWatch Traffic Monitor. Administration Guide. Changing the Preset Password*).

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

Parameters of the Traffic Monitor database:

`oinstall` – a group of the DBMS instance owner, which includes the following users:

- `iwtm`, `oracle` – for Oracle DB
- `iwtm`, `root` – for PostgreSQL DB

Linux accounts:

Purpose	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`	Not set*
User on whose behalf Oracle database server processes will be executed **Note:** this account is not created during installation of PostgreSQL database	`oracle`	Not set*
User on whose behalf PostgreSQL database server processes will be executed **Note:** this account is not created during installation of Oracle database	`postgres`	Not set*

Database accounts:

> **Note:**
>
> The accounts are available after running:
>
> - `sqlplus` – for Oracle
> - `psql` – for PostgreSQL

Purpose	Oracle account name	PostgreSQL account name	Password
Database scheme owner	`iwtm`	`iwtm`	xxXX1234
Accounts for database administration	`sys`	`postgres`	`xxXX1234`
	`system`		
Account for Linux processes to access the database	`iwtm_linux`	`iwtm_linux`	`xxXX1234`
Account for the Web Console to access the database	`iwtm_web`	`iwtm_web`	`xxXX1234`

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

Sphinx index directory `/var/lib/sphinx`:

Purpose	Name	Password
Linux user on whose behalf binary files and Sphinx indexes will be executed	`iwtm`	Not set*

Note:

* These users have limited access to the System:

- The `iwtm` account privileges are limited to running Traffic Monitor processes, binary files, and Sphinx indexes. The account cannot be edited.
- The list of groups which contain `postgres` / `oracle` user is limited to this user's groups

Web Console accounts:

Purpose	Name	Password
Administrator of users	`administrator`	`xxXX1234`
Security officer	`officer`	`xxXX1234`

4 Updating the System

Important!

- Traffic Monitor can be updated to version 7.15.x from versions 7.13.x and 7.14.x. For the history of releases, check the article *InfoWatch Traffic Monitor Documentation*.
- Traffic Monitor update is not supported when connecting to server via HP Integrated Lights Out (ILO).
- During the update, events are neither intercepted nor analyzed.

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 OS. In other words, a repository is a storage from which programs can be installed or updated. Before using the repository, you need to connect it so that the OS could access it.You can find a Guide on how to work with the repository on the *Red Hat Enterprise Linux official website*.

Note:

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

when using the Oracle DBMS

- `iwtm_logon_trg` trigger creation that is needed to provide `iwtm_linux` and `iwtm_web` users with access to objects of the `iwtm` scheme;
- creation of the `sp_iwtm_execute_os_command` procedure to run OS commands when creating, deleting, archiving, and restoring tablespace files;
- setting user profile by default (password lifetime, password change limit and connection attempts limit);
- setting service windows of `dbms_scheduler`;
- disabling access to XDB using HTTP protocol;
- disabling `dispatcher`, as a particular server is used;
- providing `iwtm` user with:

- DB scheme installation, update, and uninstallation rights;
- tablespaces creation, deletion, archiving, and restoring rights;
- rights that are used in InfoWatch Traffic Monitor code;
- rights to access DB statistics.

when using the PostgreSQL DBMS

- creation of wraper functions to read files, stop and terminate sessions, create tablespaces and provide `iwtm` with rights for them;
- removing all views (`view`) and functions from the `iwtm` scheme to create the required ones in the new version using the update;
- providing `iwtm` user with:
  - rights to create DB objects;
  - rights to install, update, and uninstall the DB scheme;

- rights to create, remove, archive, and restore tablespaces;
- rights to clear `postgres` server statistics that are used in the `pgstat` diagnostics script;
- rights for statistic views (`view`) 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 (`job`).

4.1 Before the update

Take the following actions:

- Apply the configuration. If the configuration is not applied before the update, it will be forcefully applied.
- If the Password Disclosure Adapter (PDA) is installed and running in the System, stop its processes before updating the TM. To learn more, see the *InfoWatch Password Disclosure Adapter. Installation and configuration guide. Diagnostics and removal of the InfoWatch Password Disclosure Adapter*.

- Make sure that you have:
  - the ISO image of the distribution disk of the OS on which Traffic Monitor is installed. For supported OS versions, see *Hardware and Software Requirements*;
  - 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.
- 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 scheme and server components;
  - the server where `web-gui` is installed – this information is required to clear the server cache after updating the database scheme.
    Tip: the package is installed on the server to which the Traffic Monitor Management console is connected.

> **Note:**
>
> In case `sudo -i` command was used when installing the product, make sure you use the same command to update the System in RED OS.

- Run the script to define duplicates of graphical objects in the System and delete them.
- 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 the **Power On** command (see the example below).

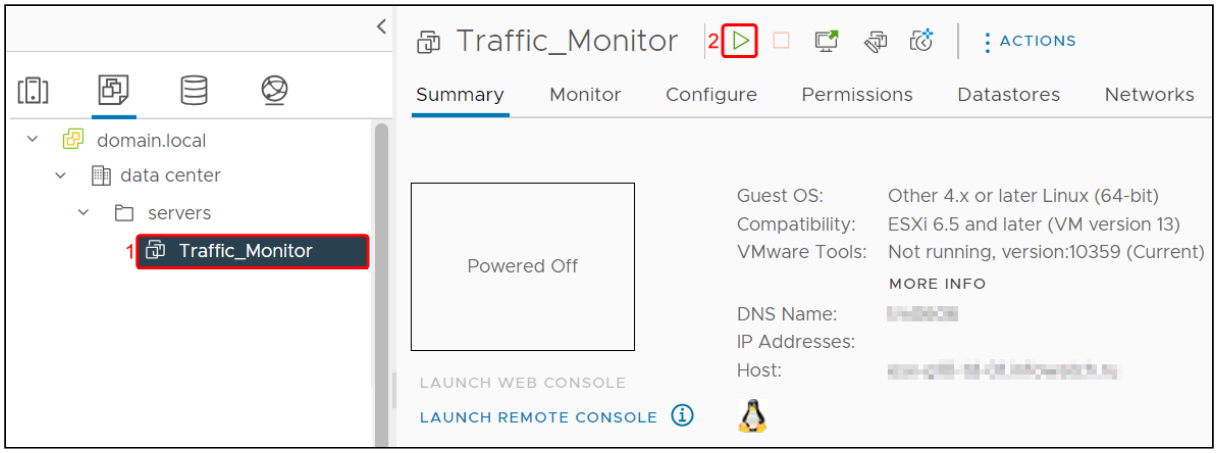
Example of running a virtual server:

Note:

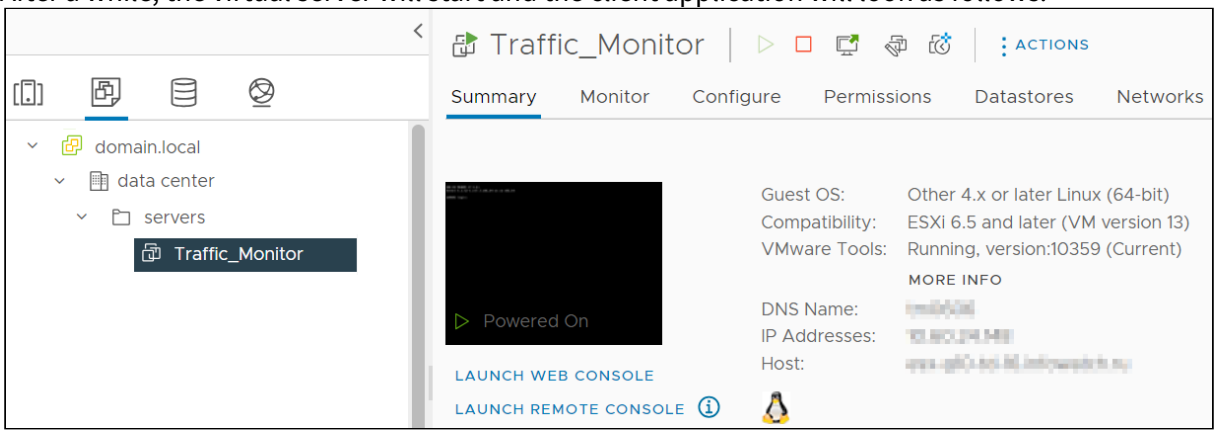
This instruction contains examples of working with a virtual server in the web version of a client application of one of the most common virtualization environments – VMware vSphere (VMware vSphere Client).

In frames, you can see interface areas that you need to click in the specified order to achieve the desired results.

1. Run the web version of the VMware vSphere Client application. Authorize in the application using the login and password issued by the administrator of your network.
2. Consistently expand all the nodes on the left side of the workspace until you see the required virtual server.
3. Turn on the virtual server:



4. After a while, the virtual server will start and the client application will look as follows:



4.2 Updating the System

Update the servers according to the instructions:

- *Updating TM All-in-One Enterprise and Standard* – updating the server with "All-in-One" installation type;
- *Updating TM in case of Distributed Installation* – updating the server with a distributed installation type.

If you use Data Storage, we recommend updating it. Instruction: *Updating Data Storage*.

For information on how to update the Device Monitor subsystem, see *InfoWatch Device Monitor. Installation, Configuration and Administration Guide* or *InfoWatch Device Monitor for Linux. Installation Guide*.

After the update

Consider the following:

- after the System is updated, preinstalled privileges for complete requests and reports management are unavailable for users with the *Security officer* and *Administrator* roles;
- when using DB unloadings, you should wait for 7 minutes after the update is complete to ensure the correct operation of the analysis technology. In case you cannot wait, add one element of DB unloading technology and apply the configuration. You can delete the added element right after this.

4.3 Duplicate-defining script

Before starting the update to version 7.15.x, run the script to define the duplicates of graphical objects in the System and delete them. To do this, run the following script in the PostgreSQL DBMS console:

```
//Automatic deletion of duplicate graphic object imprints
with fingerprint_to_delete as (
   with duplicate_contents as (
     select content_id, count(f2c.fingerprint_id) cnt
     from fingerprint_to_content_sb f2c
     left join fingerprint_sb f on f.fingerprint_id=f2c.fingerprint_id
     where f.type =  'image_classifier'
     group by content_id
     having count(f2c.fingerprint_id) >  1
   )
   select f2c.fingerprint_id
   from duplicate_contents dc
   left join fingerprint_to_content_sb f2c on f2c.content_id = dc.content_id
   where f2c.fingerprint_id not in (
     select (select fingerprint_id from fingerprint_to_content_sb where content_id=dc.content_id limit  1 )
     from duplicate_contents dc
   )
order by dc.content_id
)
delete from fingerprint_sb
where fingerprint_id in (select fingerprint_id from fingerprint_to_delete);
```

In case there are no duplicates, the System will inform you to start the update.

After the script execution has been completed, logout from the database.

4.4 Updating TM All-in-One Enterprise and Standard

Warning!

Before updating Traffic Monitor, 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 without involving the user is also available.

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

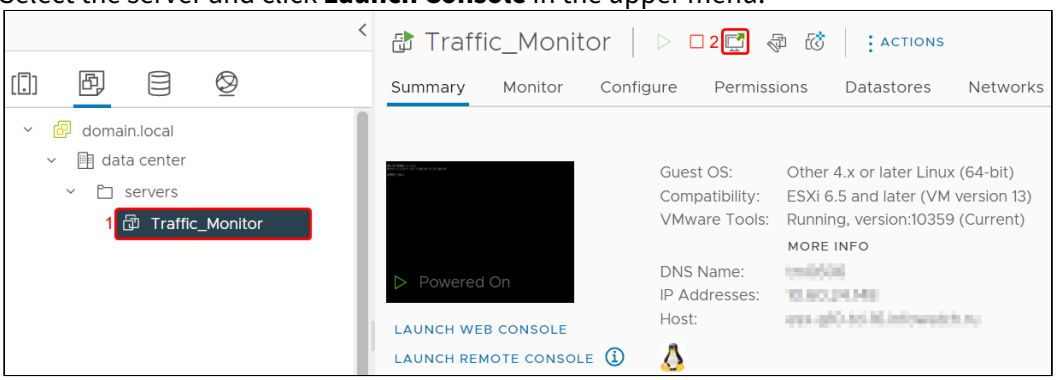
During the update all the Traffic Monitor packages will be installed, but after the update is over the installer will start only the services which were not disabled before the update.

> **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.
>
> Statuses of new services will comply with statuses of initial installation.

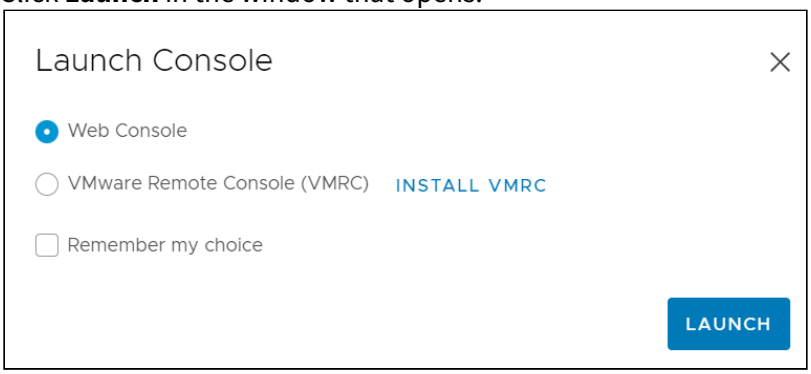
Unpacking packages will not begin when the installer is started, but right before the update.

Before updating the System, perform the following steps:

1. Open the console of the server being updated:
   - In 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 Console** command (see example below):
     Example of launching a virtual server console in the web version of client application VMWare vSphere Client:
     a. Select the server and click **Launch Console** in the upper menu:



b. Click **Launch** in the window that opens.



A window with the server console will open. Enter the user password there.

2. To log in to the System, enter the login and password (you need to enter as the `root` user).

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

3. **If you update Traffic Monitor on Oracle Linux 8, AlmaLinux 8, or Rocky Linux 8 OS:**

> **Warning!**
>
> Make sure that, in Oracle Linux 8.10 operating system, the current kernel is Red Hat Compatible Kernel (RHCK). For example, Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64` , and the UEK kernel is removed. For details, see *Operating System and Network Server Configuration Requirements*.

a. Install the `redhat-lsb-core` package by running the following command:
`dnf install redhat-lsb-core`

b. Create a backup copy of the OS release file and replace the content of the original file. For this, run the commands depending on OS:

- in Oracle Linux 8:

```
cp /etc/oracle-release /etc/release.bak

                  echo "Red Hat Enterprise Linux release 8.10
(Ootpa)" > /etc/oracle-release
```

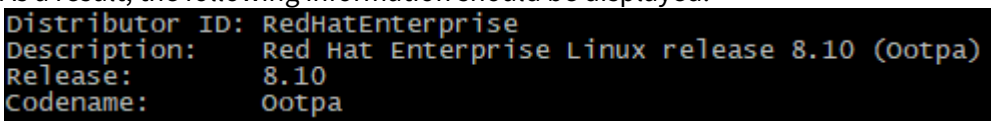
- in AlmaLinux 8 or Rocky Linux 8:

```
cp /etc/redhat-release /etc/release.bak
echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/
redhat-release
```

c. Run the command:

```
lsb_release -a
```

As a result, the following information should be displayed:



> **Note:**
>
> After updating Traffic Monitor, recover the original OS release file. For details, see below.

4. Check the version, edition, and installation type of the server you need to update. Run the command:
`cat /opt/iw/tm5/install_mode`

Example of install_mode content file:

```
{
  "product_type": "tme",
  "version": "7.14.0.150",
  "all_in_one": true,
  "templates": {
    "db": {
      "local": true
    },
    "indexer": {},
    "web": {},
    "interceptors": {}
  },
  "upgrade": {
    "previous_version": "7.13.0.136",
    "state": "done"
  }
}
```

The example is given for a Traffic Monitor server with *All-in-One* installation type, *Enterprise* edition, and version *7.14.0.150*.

5. Update the server OS in case its version is not listed among supported versions in the *Hardware and Software Requirements* article.

> **Warning!**
>
> Before updating the System, make sure that the server complies with the *OS and network settings requirements*.
>
> After the update, the parameters of the `systemd` initialization system's unit files will return to their 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 need to copy the files with their **rights, users, and groups** saved.

   To do this, copy files into the **Linux file system** only (for example, 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: `iwtm stop`
   b. Perform the backup:
      i. Depending on the database you are using, enter the command to stop the database:
         - for **Oracle DBMS**: `systemctl stop oracle`
         - for **PostgreSQL DBMS** version 13: `systemctl stop postgresql-13`
         - for **PostgreSQL DBMS** version 15: `systemctl stop postgresql-15`
      ii. Create your database backup. By default, the database is stored in the directories `/u01`, `/u02`, and so on.
      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 the file `indexer.conf` file to view it.
         2. In the parameter `"SphinxBaseDir",` you can see the path to the directory 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 the `"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/` – all files in the directory
     - `/etc/default/iwtm`
     - `/etc/profile.d/iw-oracle-env.sh`
     - `/etc/logrotate.d/iwtm-oracle-conf-server`
     - `/opt/iw/tm5/etc/oracle.conf`
   - **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-13.conf` or `/etc/pgagent/pgagent-15.conf` depending on the DBMS version
     - `/opt/iw/tm5/etc/postgresql/` – all files in the directory
     - `/opt/iw/tm5/etc/postgres.conf`

   Note:

   In the directory `/tmp/iwtm_db_configs_backup` the installer automatically creates copies of files of environment settings. To make it easier for the user, the installer recreates in the directory the paths of original files. Use the paths when you need to copy the files to restore their initial state.

   The backup copies created by the installer are stored untill uptate. They will be deleted after the update is complete.

Depending on the update mode, select the instruction:

- Updating the System over the installed one;
- Updating the System via installation and restoring data from the backup copy (for PostgreSQL).

Updating the System over the installed one:

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 files from InfoWatch Traffic Monitor distribution kit to `/root` directory. See the list of files for different OS and DBMS in *All-in-One Installation Mode of TM Enterprise and TM Standard*, step 5.
   The following instruction uses installer for Red Hat Enterprise Linux.
   This instruction is relevant for other supported OS: Oracle Linux, RED OS, AlmaLinux, Rocky Linux and Alt Server.
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-7.15.0.97-rhel7`
3. Connect external or local OS repositories.
   For example, you can find instructions on how to configure local Red Hat Enterprise Linux repository at the *official web page*.
4. To update all packages except `pgagent`, run the command:
   `yum upgrade --exclude="pgagent*"`
   The following request will be displayed:
   ```
   Total download size: 473 M
   Is this ok [y/N]:
   ```
   To continue, type **Y** and then press **Enter**.
5. Install the additional packages `python3-psycopg2` and `libzstd` by running the command:
   `yum install python3-psycopg2 libzstd`
   In case of error, download the packages from the EPEL repository and install them manually.
6. If you use a remote database:
   a. Make sure the DBMS version you use is supported by Traffic Monitor. See *Hardware and Software Requirements*.
   b. If DBMS version is actual, please skip this action.
   If DBMS needs to be upgraded:
      i. To stop Traffic Monitor services, run the command:
      `iwtm stop`
      ii. Stop the DBMS.
      iii. Upgrade the DBMS to supported version. To do this, use the official instructions.

      Note:

      For PostgresSQL and PostgreSQL Pro you should also upgrade the service in use `pgagent`.

      iv. After upgrade is complete, run the DBMS but do not start Traffic Monitor services.
7. If the Traffic Monitor server being updated interacts with Data Discovery 2.0 or later, then stop the technologies pod, which creates database connections to access the configuration.
   To stop the pod:

a. Connect to the terminal of any node of the Investigation Centre cluster with installed Data Discovery, which connects to the Traffic Monitor database.
b. The pod name contains the label of the node on which the pod is installed. To determine the pod name, run the command:
`kubectl get pods -A -o wide | grep technolog`

Example command line output after the command:

```
root@lv-426:~# kubectl get pods -A -o wide | grep technolog
infowatch      technologies-central-71cb89dd54-bgwn6      3/3     Running   0
18h   10.244.0.86   lv-426   <none>           <none>
```

Here, the node label is `central`.
c. To stop the pod, run the following command on the node with the `central` label:
`kubectl scale -n infowatch --replicas=0 deployment/technologies-central`
d. Connect to the terminal of the server with Traffic Monitor again.

8. If Password Disclosure Adapter is installed and running in the System, then before updating Traffic Monitor, stop the adapter processes. For details, see the *InfoWatch Password Disclosure Adapter. Installation and Configuration Guide. Diagnostics and Removal of InfoWatch Password Disclosure Adapter* article.
9. If you have the Prometheus system installed, then to stop the service you should run the following command:
`systemctl stop iwtm-postgres_exporter` – for **PostgreSQL DBMS**
`systemctl stop iwtm-oracledb_exporter` – for **Oracle DBMS**
10. 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:
>
> - for **Oracle DBMS**:
> `service oracle start`
> - for **PostgreSQL DBMS** version 13:
> `systemctl start postgresql-13`
> - for **PostgreSQL DBMS** version 15:
> `systemctl start postgresql-15`

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

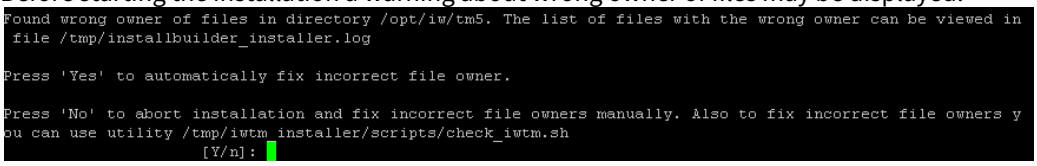
> **Warning!**
>
> Automatic merging applies only to Traffic Monitor configuration files with the `.conf` extension that are located in the `/opt/iw/tm5/etc` directory.
> Before merging, backup copies for source configuration files are created in the `/opt/iw/tm5/etc_conf_backup_<date_time>` directory. An example of the directory name: `/opt/iw/tm5/etc_conf_backup_06.07.2024_09:26:33`.
> After merging, files with the `.rpmnew` extension, which relate to merged configuration files, will be

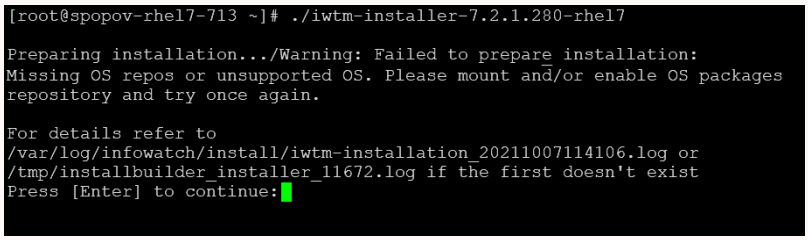
deleted.
All steps will be logged in the `/var/log/infowatch/iwtm-install-<version>-<date>_<time>.log` file. An example of the log file name: `/var/log/iwtm-install-7.15.0.97-2024-09-07_09-56-25.log`.
You can also find information on the merge process in the `/var/log/infowatch/config_merge/` directory.
If during operations with a configuration file, some errors occur, the process will be stopped until the user corrects the errors. Restart the update after the errors are corrected.

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

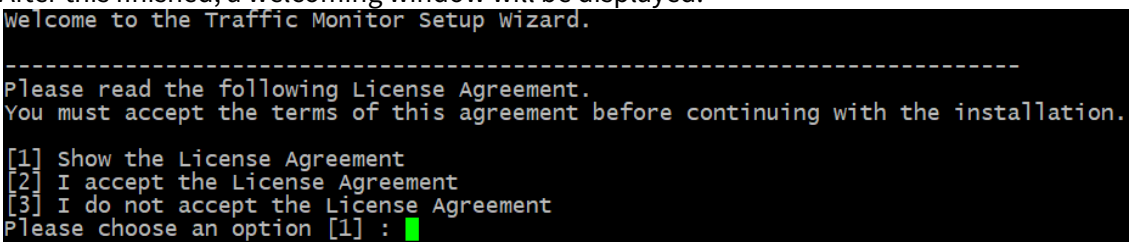
To update Traffic Monitor using server console, take the following steps:

a. Start the Traffic Monitor installer running the command:
`./iwtm-installer-x.x.x.xxx-rhel7`
Our example command:
`./iwtm-installer-7.15.0.97-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 OS 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:

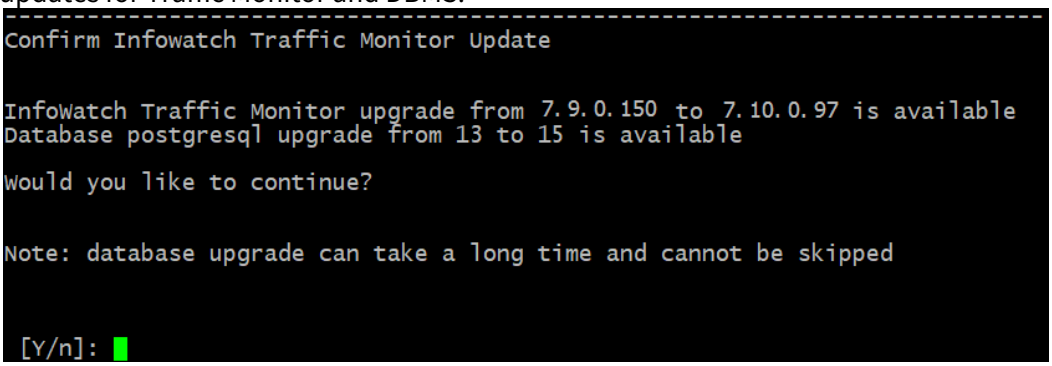


b. You must accept the terms of the License Agreement before continuing with the update. Select one of the following options. For this, type the figure specified next to it and press **Enter**:

- `Show the License Agreement` – to view the License Agreement;
  If this option is selected:
  i. Select language to display the License Agreement:
     - `English`
     - `Russian`
  ii. Read the License Agreement. To go to the next page, press **Enter**.
  iii. Accept the License Agreement. For this, type **y** and press **Enter**.
- `I accept the License Agreement` – to accept the License Agreement without preview;
- `I do not accept the License Agreement` – to not accept the License Agreement and abort the update process.

> **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**.
>
> **Example:**
>
> If you do not input a value as per picture above and press Enter, the item `[1] Show the License Agreement` will be selected.

Then update confirmation window will be displayed. It will contain all available updates for Traffic Monitor and DBMS.



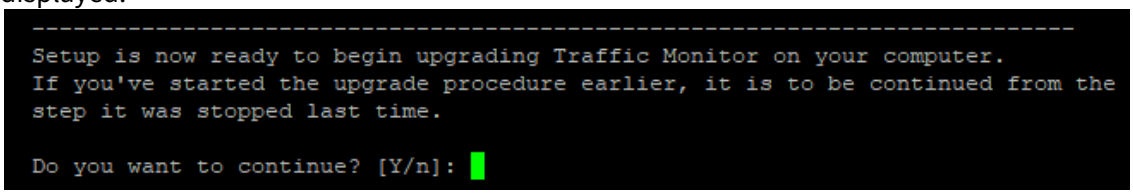
c. To continue, type **Y** and press **Enter**. To exit the installer type **n** and press **Enter**.

d. 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.
e. 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.

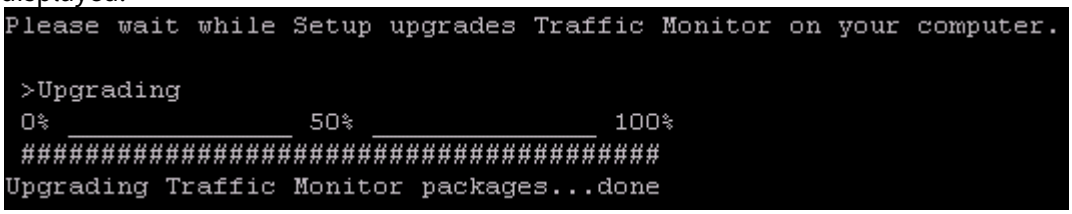
   To make a choice please enter the figure specified next to option selected, and press **Enter**.

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

f. 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.
g. 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.

h. 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`

Warning!

In case `luaengined.conf` configuration file contains `SmtpTmBccList` parameter, before starting services make sure there are no angle brackets (`<` and `>`) in the parameter's value. Otherwise, remove the brackets.

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

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

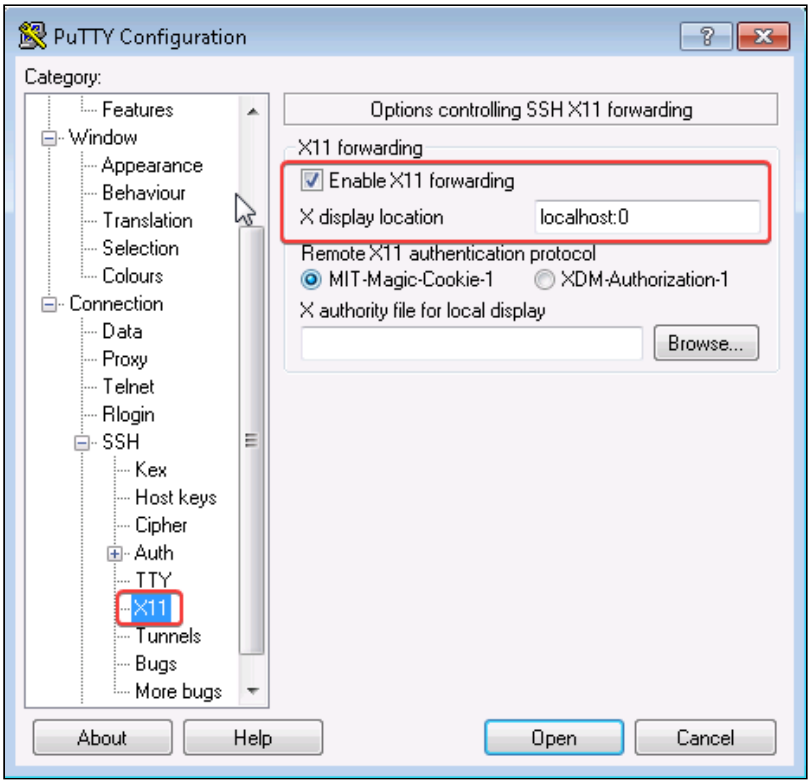
i. Before completing the update the installer will offer deleting the packages created to update the System.
   When update is successfully completed, this data is recommended to delete.
j. Wait till completion of installer operation.

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 following 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

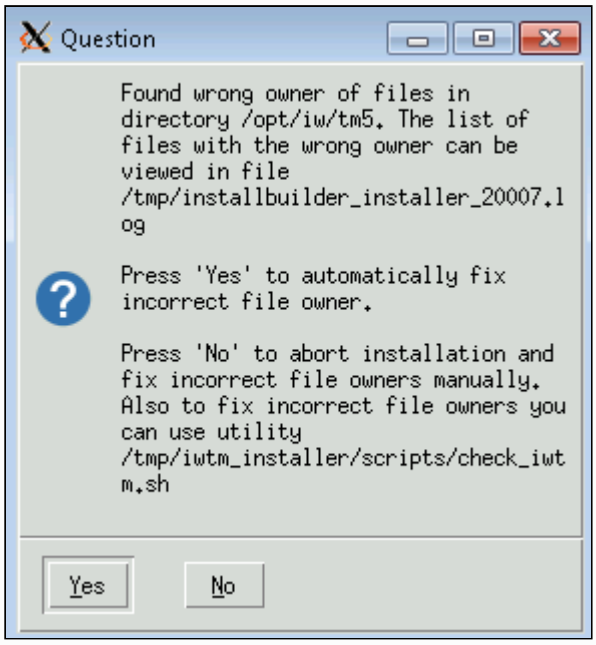


e. Run the installer using the command:
   `./iwtm-installer-x.x.x.xxx-rhel7`
   As per our example:

`./iwtm-installer-7.15.0.97-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.

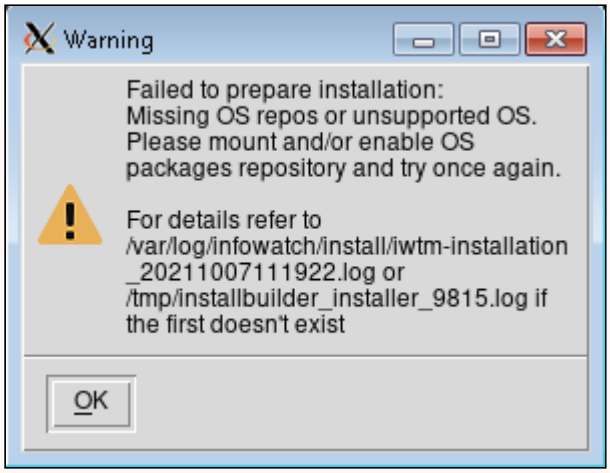


Press **Yes** to change the owner of files and continue running.

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!

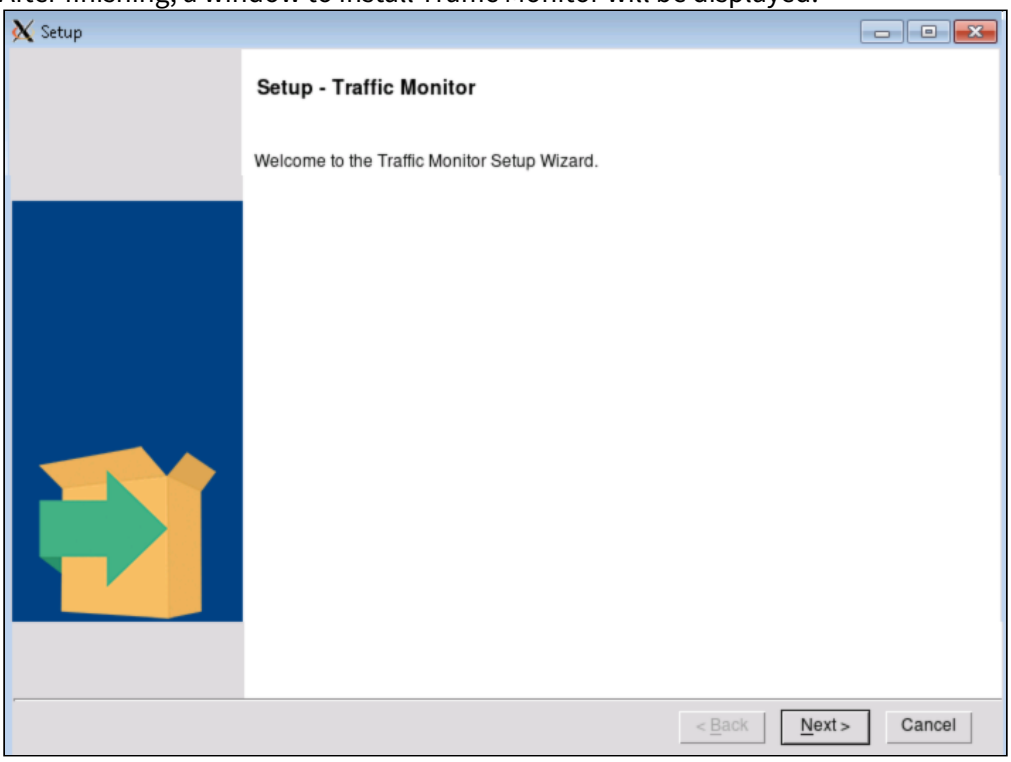
If available configured OS repositories are missing, the preparation process will stop with the following error message:



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

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

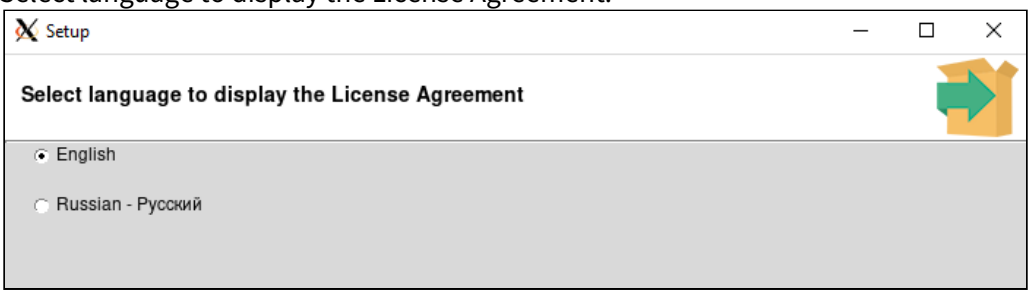
After finishing, a window to install Traffic Monitor will be displayed:



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

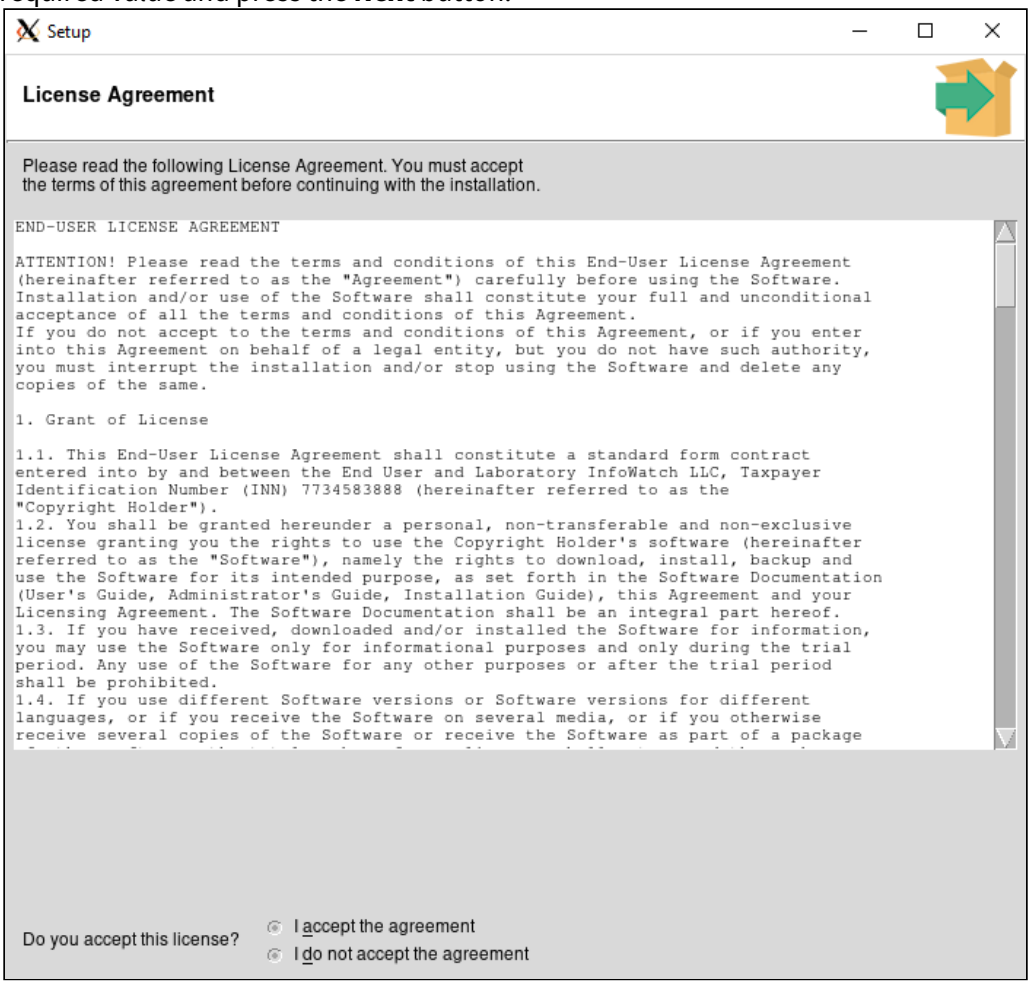
f. You must accept the terms of the License Agreement before continuing with the update. For this:

i. Select language to display the License Agreement:



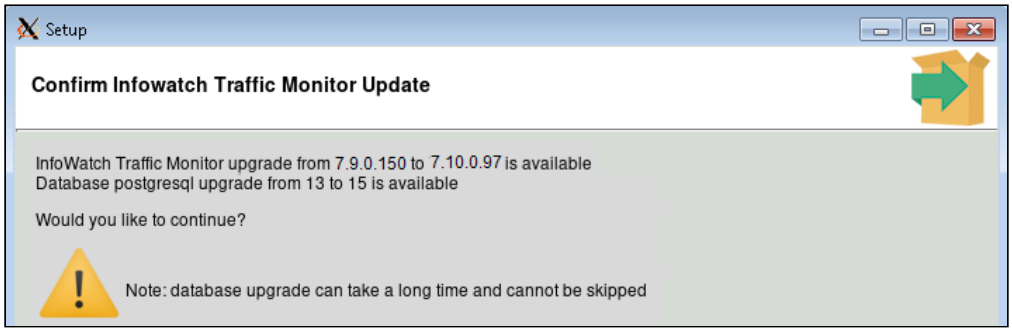
- `English`
- `Russian`

ii. Select one of the following options. For this, click in the checkbox next to the required value and press the **Next** button:



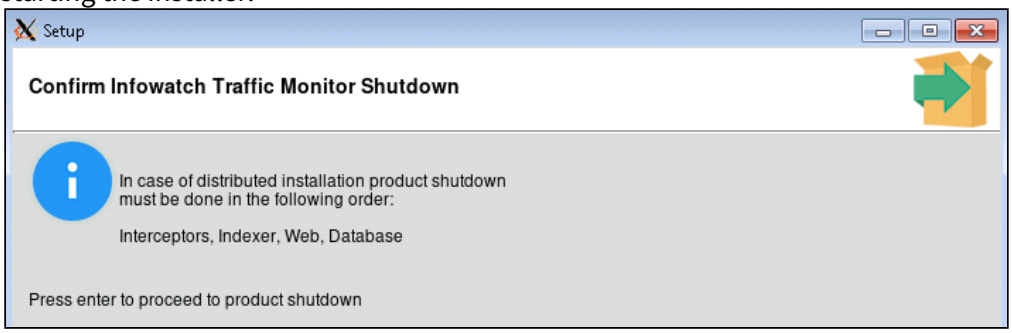
- `I accept the agreement` – to accept the License Agreement and continue the update process;
- `I do not accept the agreement` – to not accept the License Agreement and abort the update process.

g. The next window will contain data related to available upgrades for Traffic Monitor and DBMS.

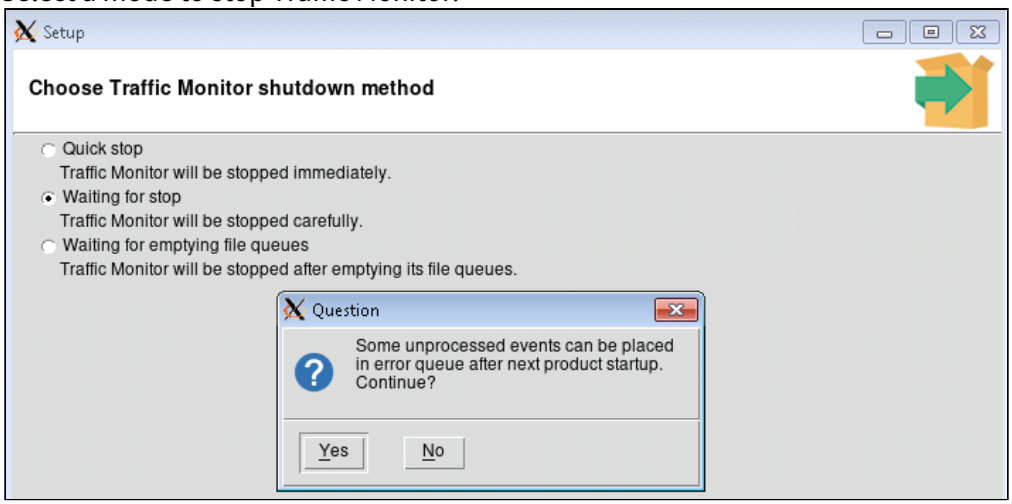


To continue press **Next**.

h. 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.



i. Select a mode to stop Traffic Monitor:



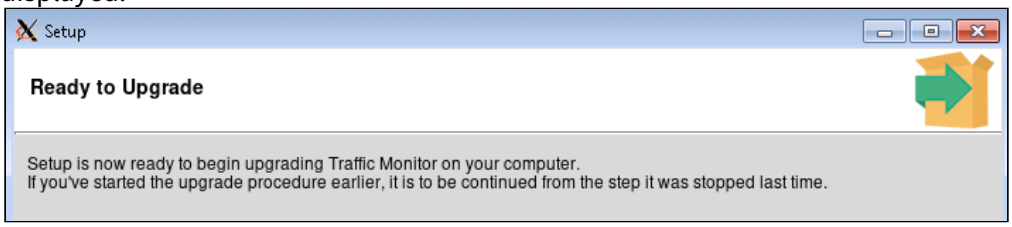
- `Quick stop` – quick stop without events processing;
- `Waiting for stop` – wait till the current processing of events is finished;
- `Waiting for emptying file queues` – wait till all the events are processed and all the file queues are empty before stopping.

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

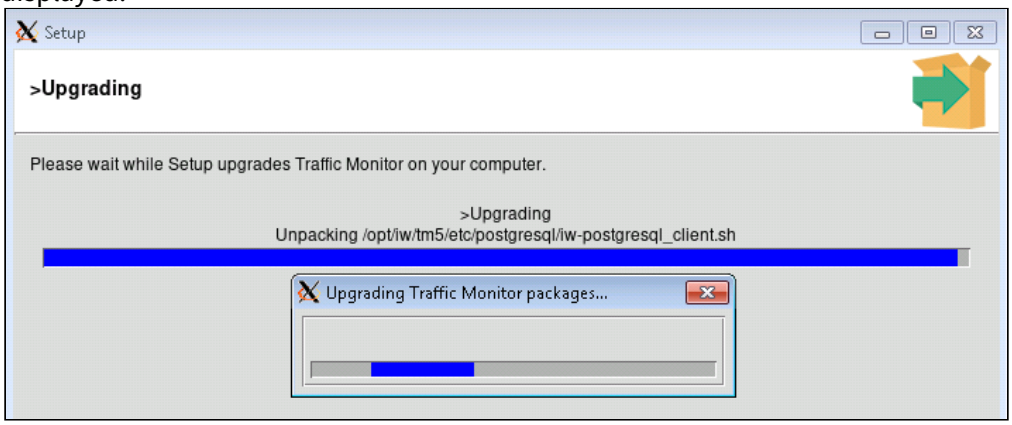
> **Note:**
>
> In case `Quick stop` is selected, the stopped services will have `failed` status before the update.

j. 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 processing progress will be displayed.

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



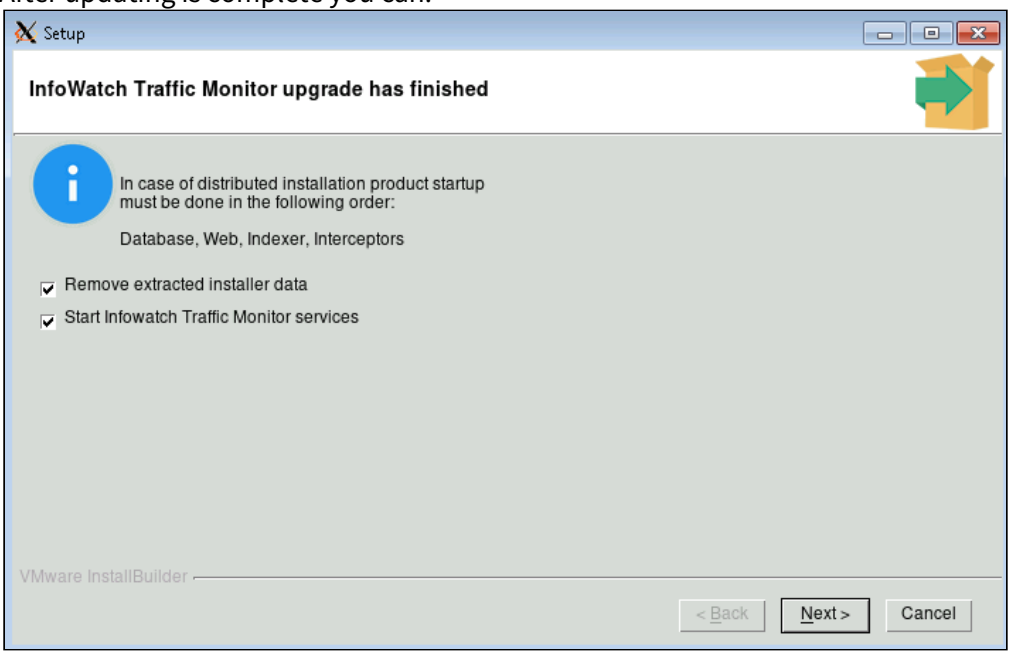
To start the updating press **Yes** button.
The unpacking of Traffic Monitor updating files will start. Implementation progress will be displayed.



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.

l. 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.
- **`Start Infowatch Traffic Monitor services`** – start the stopped services. Otherwise, you need to restore System availability manually later.

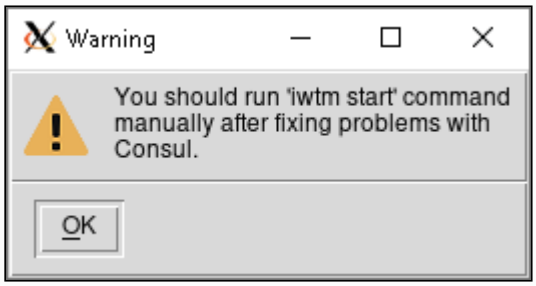
> **Warning!**
>
> After update is complete Nagios monitoring system configuration will be changed to default values. In case you've edited Nagios configuration files before the update, its copies will be created in `/etc/infowatch/nagios/iwmon` as `.saved` files. Before starting the Traffic Monitor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

> **Warning!**
>
> In case `luaengined.conf` configuration file contains `SmtpTmBccList` parameter, before starting services make sure there are no angle brackets (`<` and `>`) in the parameter's value. Otherwise, remove the brackets.

Mark the checkboxes to select the actions you need:

> **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.

m. To finalise the installation press **Next**.

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.

4.4.1 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-7.15.0.97-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.

4.4.2 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-7.15.0.97-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 OS 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**.

Check and configure cluster of Consul service for correct work of the System:

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.

4.4.3 Full composition of parameter file

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

Name	Description
`force_upgrade`	Forcible switch to updating mode, even if the versions do not match Values: `0` (default), `1`
`fix_incorrect_file_owners`	The parameter defines if the wrong owner of files should be changed before the update Values: `0` (default), `1` If the files to be updated have a wrong owner, the update will be interrupted.
`cleanup_way`	Select the mode to stop services: • `quick_stop`. No events processing; • `wait_stop` (default). Wait until current events processing is complete; • `clean_fq`. Before

Name	Description
	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`).

Name	Description
`start_services_after_upgrade`	The parameter defines if the installer should run the services after update Values: `0`, `1` (default) 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-

Name	Description
	nagios service. For example, to check Nagios status use the command: `systemctl status iwtm-nagios` If `luaengined.conf` configuration file contains `SmtpTmBccList` parameter, and there are angle brackets (`<` and `>`) in the parameter's value, remove the brackets before starting services. In this case, you should not set `start_services_after_upgrade` to `1` .

Name	Description
`eula`	Values: • `show` – display the License Agreement text • `accept` – accept the License Agreement without preview If you run the installation not in the unattended mode and do not specify the parameter, then the License Agreement text will be displayed. You will be asked to accept the agreement. If you run the installation in the unattended mode, this parameter value is ignored and the License Agreement is accepted by default.

12. Enter the command to find files with **`.rpmnew`** extension, except backups of configuration files:
`find / -name "*rpmnew*" -not -path "/opt/iw/tm5/etc_conf_backup*" -print`
If the files have been found, they are displayed at the console. In this case, you should correctly merge them 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

13. Check the contents of `/opt/iw/tm5/etc/scripts/` **`iwssid.lua`**. If it was not changed before the update, it is recommended to not change it. Otherwise, properly merge it with the configuration file **`iwssid.lua.rpmnew`** (see *Merging Configuration Files*).
14. If the installer has not complete its work before, select start of services and finish the update. If the installer has completed its work without running the services, start them manually or reboot the server to start all stopped services.
To reboot the server:
`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

```
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**

Error record

```
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
4 Diagnostic information.
5 /sandbox/src/cas3/handler.cpp(682): Throw in function
 cas::Handler::LoadedConfigData
cas::Handler::GetLoadedConfigData(const prop::Property&, const Ptr&)
6 Dynamic exception type:
boost::exception_detail::clone_impl<tech::ExceptionTechLoadConfig>
7 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.

15. In Traffic Monitor, we have extended the list of default tasks that automatically delete obsolete tasks.
    Tasks for the `cron` scheduler are now specified in the `/etc/cron.d/iwtm_cleanup` file (file contents are described in the *Automatic deletion of unnecessary files in Traffic Monitor* article).
    For new tasks to work correctly:
    a. Delete obsolete tasks by editing the `cron` configuration file:
       `sudo crontab -e`
    b. Save changes and exit the configuration file editor.
    c. Restart the service:
       `systemctl reload crond`
16. If you haven't edited the previous `/etc/cron.d/iwtm_error_queue` file with tasks before the update, then skip this step.
    Otherwise, the `/etc/cron.d/iwtm_error_queue` file will be deleted and its contents will be saved in the `/etc/cron.d/iwtm_error_queue.rpmsave` file.
    For earlier added tasks to start working again, create a file for your tasks in the `/etc/cron.d/` directory and copy required tasks from `/etc/cron.d/iwtm_error_queue.rpmsave` to this file.

> **Note:**
>
> You can add your tasks to the `/etc/cron.d/iwtm_cleanup` file. On the next update, this file will be renamed to `/etc/cron.d/iwtm_cleanup.rpmnew` and replaced with a file with default content. After the next update, you will need to move added tasks from the `/etc/cron.d/iwtm_cleanup.rpmnew` file to a new `/etc/cron.d/iwtm_cleanup` file.
> To avoid moving tasks every time, you can create a separate file with your tasks in the `/etc/cron.d/` directory.

17. If you have the Prometheus system installed and in case the server has not been rebooted to stop the service you should run the following command:
    `systemctl start iwtm-postgres_exporter` – for **PostgreSQL DBMS**
    `systemctl start iwtm-oracledb_exporter` – for **Oracle DBMS**
18. If the Traffic Monitor server being updated interacts with Data Discovery 2.0 or later, then earlier you stopped the `technologies` pod. Run the pod again. For this:

a. Connect to the node of the Intestigation Centre cluster.
b. To start the pod, on the node with the `central` label, run the command:
`kubectl scale -n infowatch --replicas=1 deployment/technologies-central`
c. Connect to the terminal of the server with Traffic Monitor again.

19. If you previously stopped the processes of Password Disclosure Adapter, start these processes. For details, see the *InfoWatch Password Disclosure Adapter. Installation and Configuration Guide. Diagnostics and Removal of InfoWatch Password Disclosure Adapter* article.
20. Enter the command to clear cache of packages manager:
`yum clean all`
21. Enter the command to test processes' start:
`iwtm status`
A list of processes and their statuses will be displayed.

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

Note:

After the DBMS was successfully updated you can remove files which belong 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 postgresql13*`
`/u01/postgres/tmp/delete_old_cluster.sh the`
- 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 entities after update is completed, you should run the synchronization 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 via installation and restoring data from the backup copy (for PostgreSQL)

> **Warning!**
>
> We strongly recommend backing up the System, cloning it, and updating on this particular testing machine.
> If you do not want to copy the data because you will mount the disk or the section containing your data, we recommend to backup them anyway.
> After clear installation of the System you will need to set the configuration files of Traffic Monitor again. We recommend to store them so you can configure settings after the update.
>
> In case `luaengined.conf` configuration file contains `SmtpTmBccList` parameter, and there are angle brackets (`<` and `>`) in the parameter's value, remove the brackets before starting services.

1. To stop Traffic Monitor services, run the command:
   `iwtm stop`
2. Check the number of events DB contains. For this, run the command:
   `psql postgres iwtm -c "select count(1) from object;"`
3. Complete *database and indexes backup*.
4. Install a new version of Traffic Monitor.

   > **Warning!**
   >
   > If the backup copies of your DB are stored on external devices, do not connect them during the update. You need to do it before restoring and updating the DB.
   >
   > When the update is complete, do not remove the packages created by the installer during the process of update (the point **Remove extracted installer data**).

   Perform the following steps on the server where you have installed the new version of Traffic Monitor.
5. To stop services, run the commands:
   `iwtm stop`
6. Enter the command to stop the DB:
   `systemctl stop postgresql-13`

   > **Note:**
   >
   > To restore the initial state of clean installation, you can copy the directories `u01` and `u02` .

7. To change the access rights to the directory, enter the command:
   `chmod 777 /var/log/infowatch/update`
8. Copy reserve DB copy so that it was located the same way it was placed initially.
9. Change the owner of the directories by running the commands:
   `chown -R postgres:postgres /u01/`
   `chown -R postgres:postgres /u02/`
10. Enter the command to go to the directory that contains scripts:
    `cd /tmp/iwtm_installer/scripts`

11. From the directory run the script to update the DBMS by using the command:
`./install_postgres.sh --distrib_path=<directory_with_DBMS_distributive> --tm_version=<new_version_of_Traffic_Monitor> --update`
As per our example:
`./install_postgres.sh --distrib_path=/root --tm_version=7.15.0.97 --update`

> **Note:**
>
> In the example the distributive `iwtm-postgresql-15.14-x.x.x.xxx-rhel7.tar.gz` is located in the `/root` directory.
> To view the version of Traffic Monitor you have installed, enter the command:
> `cat /opt/iw/tm5/version`

12. After the successfull update complete the command to check the status of DBMS service:
`systemctl status postgresql-15`
13. Run the script to update the data scheme by using the command:
`./install_dbschema.sh --tm_version=<new_version_of_Traffic_Monitor> --db_type=postgres --update`
As per our example:
`./install_dbschema.sh --tm_version=7.15.0.97 --db_type=postgres --update`
14. Complete the step 2 of the instruction to compare the number of events in the DB before and after the update.
15. Copy the backup copies of indexes and configurations of `iw_adlibitum` service so that they were located the same way it was placed initially.
If the initial location is not the default one, then you will have to specify it in the corresponding sections of the configuration files (see *steps biii and biv*).
16. Change the owner of the directories by running the commands:
`chown -R iwtm:iwtm /var/lib/sphinx/`
`chown -R iwtm:iwtm /opt/iw/tm5/etc/adlibitum/`
17. Run the commands:
`sudo -u iwtm touch /opt/iw/tm5/www/backend/protected/runtime/first_run`
`iwtm restart kicker`
18. Run the command to reboot the server:
`reboot`
Wait until the server is rebooted, then log in again by completing the steps 1-3 of the instruction before the update.
19. Enter the command to check statuses of the processes:
`iwtm status`
The list of processes and their statuses will be displayed.

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

> **Note:**
>
> Clear cache of your browser before starting the works, so the Console is displayed correctly. You can do it by using the standard tools of your browser.

If you updated Traffic Monitor on Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS, recover the original OS release file.

For this:

1. Run the command depending on OS:
   - in Oracle Linux 8:
     `mv /etc/release.bak /etc/oracle-release`
   - in AlmaLinux 8 or Rocky Linux 8:

     ```
     mv /etc/release.bak /etc/redhat-release
     ```
2. Confirm overwriting of the file. For this, enter "`yes`" and press **Enter**.
3. Check that the original release file is succesfully recovered. For this, run the command:

   ```
   lsb_release -a
   ```

   As a result, the information on your OS should be displayed. For example, for AlmaLinux 8 OS, the following will be displayed:

   ```
   Distributor ID: AlmaLinux
   Description:    AlmaLinux release 8.10 (Cerulean Leopard)
   Release:        8.10
   Codename:       CeruleanLeopard
   ```

Important!

In Traffic Monitor 7.14, we have updated the supplied certificates and the public key that are used for connecting to the XAPI service via SSL. By default, the certificates and the key are stored in the folder `/opt/iw/tm5/etc/cert`.

If you are updating Traffic Monitor from version 7.13 or earlier, and Data Discovery, Device Monitor, adapters, or other third-party services within your perimeter interact with Traffic Monitor using the XAPI service, make sure you factor in such a replacing of certificates and the public key.

If you previously:

- **Used your own** certificates and the key with **names other** than the default file names, the update **will not affect** the interaction of the services, because the files you added will not be deleted.
- **Deleted the files supplied** with the product and used **your own** certificates and the key **with similar names**, after updating, **replace the certificates in Traffic Monitor** with those you generated.
- **Copied** the certificates and the key **supplied** with Traffic Monitor to the folders of other products, adapters, or services, after updating, **copy them again** from the `/opt/iw/tm5/etc/cert` folder.

To learn about installing or changing certificates:

- In **Device Monitor Windows**, see *InfoWatch Device Monitor. Installation, Configuration and Administration Guide. Configuring validation of the remote server certificates*
- In **Device Monitor Linux**, see *InfoWatch Device Monitor for Linux. Installation guide*
- In **Data Discovery**, see *InfoWatch Data Discovery. Administration Guide. Zones and Servers*

Важно!

In case before updating Traffic Monitor to version 7.15 service encryption was enabled, make sure your settings correspond to the actual instruction. See *InfoWatch Traffic Monitor. Administration Guide. SSL Thrift Encryption*.

4.5 Updating TM in case of Distributed Installation

Warning!

Before updating the Traffic Monitor server, we recommend updating the DM server first.

Traffic Monitor installation kit 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**

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.

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

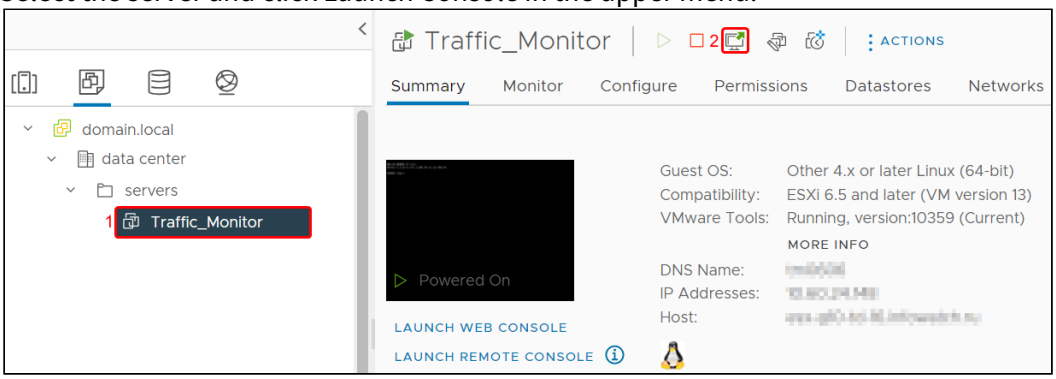
Warning!

Each server should have a unique correct FQDN.

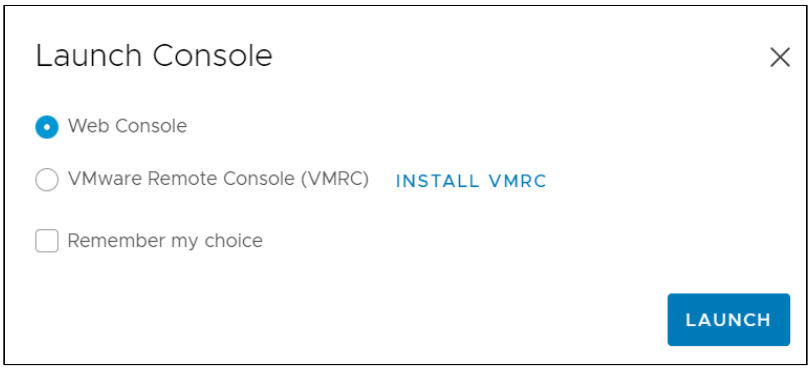
Before updating the System, perform the following steps:

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 Console** command (see an example below).
     Example of launching a virtual server console in the web version of client application VMWare vSphere Client:

     a. Select the server and click Launch Console in the upper menu.



     b. Click Launch.



     A window with the server console will open. Enter the user password there.

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. **If you update Traffic Monitor components on Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS:**

> **Warning!**
>
> Make sure that, in Oracle Linux 8.10 operating system, the current kernel is Red Hat Compatible Kernel (RHCK), for example, Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`, and the UEK kernel is removed. For details, see *Operating System and Network Server Configuration Requirements*.

   a. Install the `redhat-lsb-core` package by running the following command:

```
dnf install redhat-lsb-core
```

   b. Create a backup copy of the OS release file and replace the content of the original file. For this, run the commands depending on OS:
      - in Oracle Linux 8:

```
cp /etc/oracle-release /etc/release.bak

echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/oracle-release
```

      - in AlmaLinux 8 or Rocky Linux 8:

```
cp /etc/redhat-release /etc/release.bak
echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/redhat-release
```

   c. Run the command:

```
lsb_release -a
```

   As a result, the following information should be displayed:

```
Distributor ID: RedHatEnterprise
Description:    Red Hat Enterprise Linux release 8.10 (Ootpa)
Release:        8.10
Codename:       Ootpa
```

> **Note:**
>
> After updating Traffic Monitor, recover the original OS release file. For details, see *below*.

4. Check the installation parameters of the server to be updated. Run the command:
`cat /opt/iw/tm5/install_mode`

Example of content

```
{
  "product_type": "tme",
  "version": "7.14.0.150",
  "all_in_one": false,
  "templates": {
    "db": {
      "local": true
    },
    "indexer": {},
  }
}
```

Record from the example corresponds to a Traffic Monitor server with the following parameters:
- *Enterprise* edition;
- Version 7.14.0.150;
- *Distributed* installation type;
- *Database* and *Indexer* templates are activated;
- *Local* database is used.

5. Update the OS in case its version is not listed among supported versions in *Hardware and Software Requirements* article.

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 all servers stop TM services:
`iwtm stop`
b. On the server installed with Web console template, create the backup of `iw_adlibitum` service. For this:
   i. Go to `/opt/iw/tm5/etc` and open the file **`adlibitum. conf`** to view.
   ii. 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.
c. On the server installed with Indexer template, create the indexer backup copy:
   i. Go to `/opt/iw/tm5/etc` and open the file **`indexer.conf`** to view.
   ii. In "`SphinxBaseDir`" parameter you can see a relative path to the directory where the indexes are. In "`ArchiveDir`" parameter you can see a relative path to the indexers archive. The path is specified in relation to the content of `"NookDir"` parameter. Copy the directories to a separate section of server or to another server or to an external device.
d. On DBMS server:
   i. Depending on the DBMS you use and the version of Traffic Monitor, enter tha command to stop the database:
      - for DBMS **Oracle**:
        `systemctl stop oracle`
      - for **DBMS PostgreSQL** version 13:
        `systemctl stop postgresql-13`
      - for **DBMS PostgreSQL** version 15:
        `systemctl stop postgresql-15`

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**)

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.

ii. Create a backup copy of indexes. To do this:

1. Go to `/opt/iw/tm5/etc` directory and open to view **`indexer.conf`** file.
2. `"SphinxBaseDir"` parameter contains a path to directory with indexes. "`ArchiveDir`" parameter contains a path to indexes archive. Path to archives is specified according to `"NookDir"` parame

ter content.
Copy the directories with indexes and indexes archives to different section or to 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/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-15.conf` or `/etc/pgagent/pgagent-15.conf` depending on DBMS version
     - `/opt/iw/tm5/etc/postgresql/` – all files in the directory
     - `/opt/iw/tm5/etc/postgres.conf`

   > **Note:**
   >
   > Also the installer makes copies of environment configuration file in `/tmp/iwtm_db_configs_backup` directory. For user comport the installer recreates in directory the paths of original files which can be used to copy back to initial state. Copies created by installed are stored until successful upgrade is complete. Once completed these copies are to be removed.

Depending on the version installed, choose the instruction:

- Updating the System over the installed one;
- Updating the System via installation and restoring data from the backup copy (for PostgreSQL).

Updating the System over the installed one

> **Warning!**
>
> We strongly recommend backing up the System, cloning it, and updating on this particular testing machine.
>
> You should stop the services using the installer and run the update in the following order:
>
> 1. Interceptors
> 2. Indexer

3. Web console
4. Database

The updating order is as follows:

Step 1. Updating All Servers.

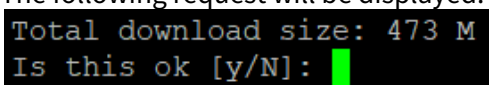
Step 2. Checking Consul Cluster.

Step 3. Performing Healthcheck of System Internal Services.

Step 4. Completing Servers Update.

STEP 1. UPDATING ALL SERVERS

To update servers, please take the following actions as per each server:

1. Copy files from InfoWatch Traffic Monitor distribution kit to /root directory. See the list of files for different OS and DBMS in *Distributed Installation of TM Enterprise*, step 5. The following instruction uses installer for Red Hat Enterprise Linux.
   This instruction is relevant for other supported OS: Oracle Linux, RED OS, AlmaLinux, Rocky Linux and Alt Server.
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-7.154.0.97-rhel7`
3. Connect external or local OS repositories.
   For example, you can find instructions on how to configure local Red Hat Enterprise Linux repository at the *official web page*.
4. To update all packages except `pgagent`, run the command:
   `yum upgrade --exclude="pgagent*"`
   The following request will be displayed:
   

   To continue, type **Y** and then press **Enter**.
5. Install the additional packages `python3-psycopg2` and `libzstd` by running the command:
   `yum install python3-psycopg2 libzstd`
   In case of error, download the packages from the EPEL repository and install them manually.
6. If you use a remote database:
   a. Make sure the DBMS version you use is supported by Traffic Monitor. See *Hardware and Software Requirements*.
   b. If DBMS version is actual, please skip this action.
   If DBMS needs to be upgraded:
      i. To stop Traffic Monitor services, run the command:
      `iwtm stop`
      ii. Stop the DBMS.
      iii. Upgrade the DBMS to supported version. To do this, use the official instructions.

      > **Note:**
      >
      > For PostgreSQL and PostgreSQL Pro you should also upgrade the service in use `pgagent`.

iv. After upgrade is complete, run the DBMS but do not start Traffic Monitor services.

7. If the Traffic Monitor server being updated interacts with Data Discovery 2.0 or later, then stop the `technologies` pod, which creates database connections to access the configuration.
   To stop the pod:
   a. Connect to the terminal of any node of the Investigation Centre cluster with installed Data Discovery, which connects to the Traffic Monitor database.
   b. The pod name contains the label of the node on which the pod is installed. To determine the pod name, run the command:
   `kubectl get pods -A -o wide | grep technolog`

   Example command line output after the command:

   ```
   root@lv-426:~# kubectl get pods -A -o wide | grep technolog
   infowatch      technologies-central-71cb89dd54-bgwn6      3/3     Running   0
   18h   10.244.0.86   lv-426   <none>           <none>
   ```

   Here, the node label is `central`.
   c. To stop the pod, run the following command on the node with the `central` label:
   `kubectl scale -n infowatch --replicas=0 deployment/technologies-central`
   d. Connect to the terminal of the server with Traffic Monitor again.
8. If Password Disclosure Adapter is installed and running in the System, then before updating Traffic Monitor, stop the adapter processes. For details, see the *InfoWatch Password Disclosure Adapter. Installation and Configuration Guide. Diagnostics and Removal of InfoWatch Password Disclosure Adapter* article.
9. In case you are using the Prometheus system, to stop the service, run the following command on the server installed with Database template:
   `systemctl stop iwtm-postgres_exporter` – for **PostgreSQL DBMS**
   `systemctl stop iwtm-oracledb_exporter` – for **Oracle DBMS**
10. On the server installed with Database template, before running the installer you are recommended to start database service in case it was stopped earlier. Depending on the DBMS you are using, enter one of the commands:
    - `systemctl start oracle` (for DBMS **Oracle**)
    - `systemctl start postgresql-15` (for DBMS **PostgreSQL**)
11. Enter the command to go to Traffic Monitor distribution kit directory:
    `cd /root`
12. 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_11.07.2024_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-7.15.0.97-2024-11-07_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.

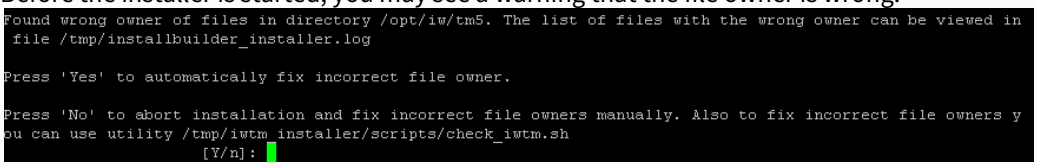
Run the installer using one of the modes:
Updating in text mode using server console

To update Traffic Monitor using server console:

a. Start the Traffic Monitor installer running the command:
`./iwtm-installer-x.x.x.xxx-rhel7`
Our example command:
`./iwtm-installer-7.15.0.97-rhel7`
The installer will prepare to run. At this step, files are not unpacked.

Note:

Before the installer is started, you may see a warning that the file owner is wrong.

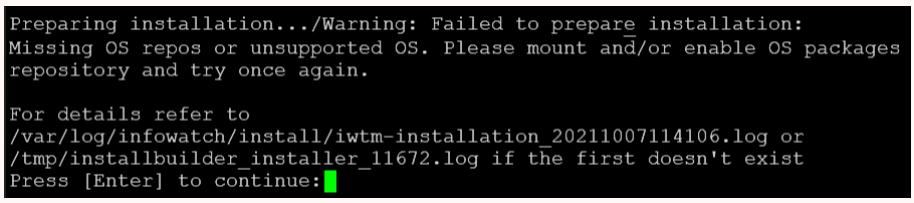


Type **Y** and press **Enter** for the installer to change the file owner and continue running.

Otherwise, you can enter **N** and press **Enter**, then edit the file owner manually or using the `/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 OS repository, EPEL repository and restart the installer.

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

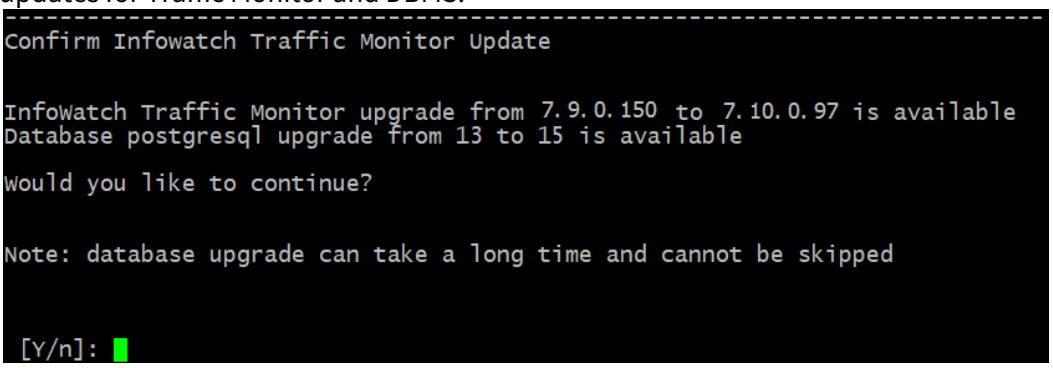
After this finished, a welcoming window will be displayed:



b. You must accept the terms of the License Agreement before continuing with the update. Select one of the following options. For this, type the figure specified next to it and press **Enter**:
   - **`Show the License Agreement`** – to view the License Agreement;
     If this option is selected:
     i. Select language to display the License Agreement:
        - **`English`**
        - **`Russian`**
     ii. Read the License Agreement. To go to the next page, press **Enter**.
     iii. Accept the License Agreement. For this, type **y** and press **Enter**.
   - **`I accept the License Agreement`** – to accept the License Agreement without preview;
   - **`I do not accept the License Agreement`** – to not accept the License Agreement and abort the update process.

> **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**.
>
> **Example:**
>
> If you do not input a value as per picture above and press Enter, the item `[1] Show the License Agreement` will be selected.

Then update confirmation window will be displayed. It will contain all available updates for Traffic Monitor and DBMS.



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

d. 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:**
>
> If components of Traffic Monitor are operating on several servers, then you should stop them one after another in the following order:
>
> i. Interceptors
> ii. Indexer
> iii. Web console
> iv. Database

e. 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.

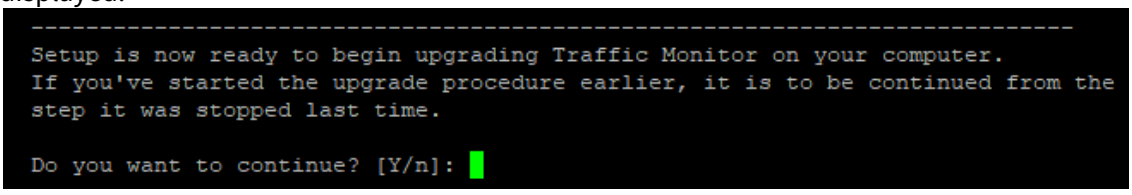
> **Warning!**
>
> If interception and analysis components `iw_cas`, `iw_pas` are used on separate servers, then stopping interceptors and cleaning up file queues may be pending.
>
> We recommend to select a different mode or to stop the components manually.

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.

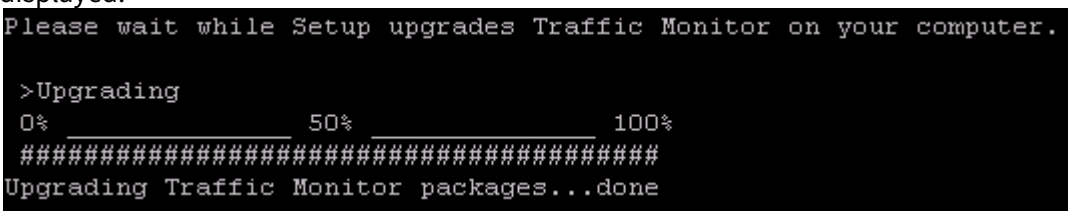
f. If you've selected `Quick stop` or `Waiting for stop`, events can be sent to error queue after Traffic Monitor resumes the work.
To continue type **Y** and press **Enter**.
While stopping an events processing progress will be displayed.

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



To continue 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.

h. Before completing 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. When updating is successfully completed 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 start services before you complete the update of the DBMS server and start it. You can wait and start the services after the update or continue without starting them in order to perform it later manually.
>
> The services should be started in the order depending on the templates activated on them.
>
> 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`

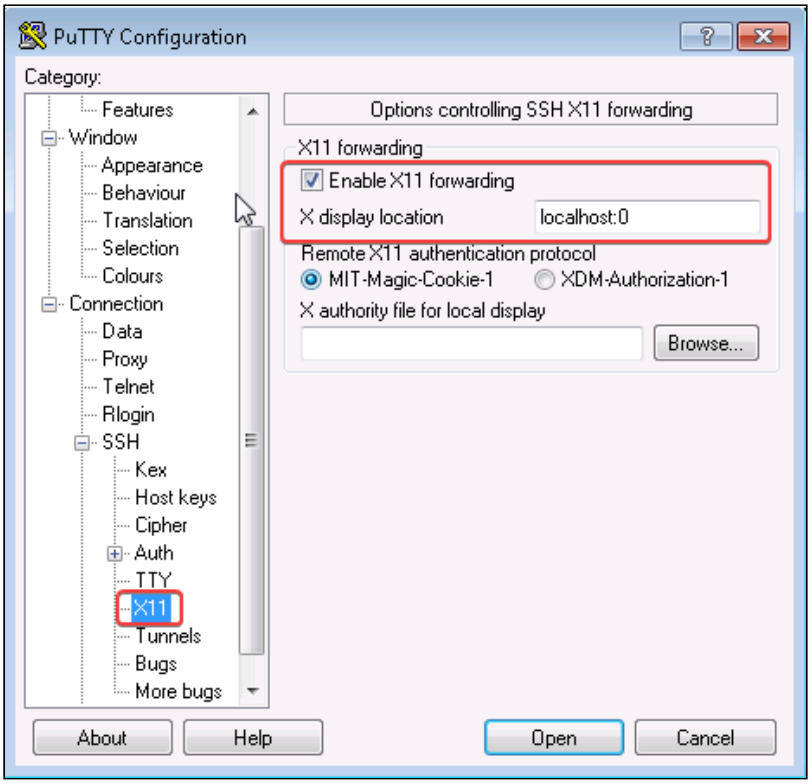
In case `luaengined.conf` configuration file contains `SmtpTmBccList` parameter, before starting services make sure there are no angle brackets (`<` and `>`) in the parameter's value. Otherwise, remove the brackets.

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.

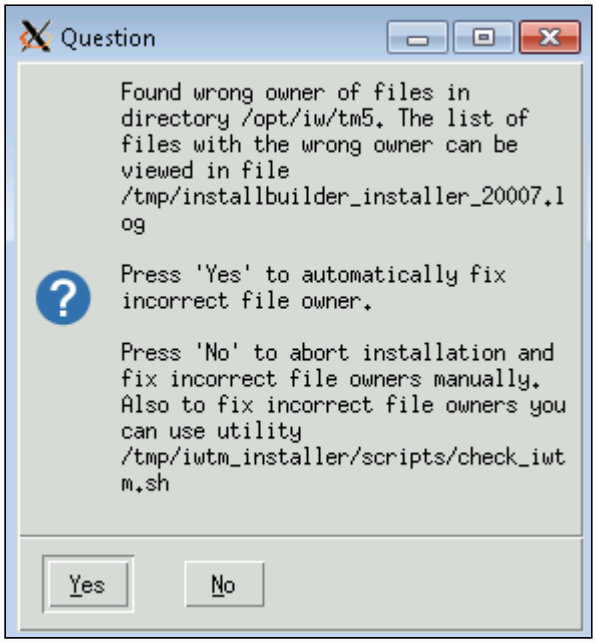
To update Traffic Monitor using graphical mode of installation, take the following steps:

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-7.15.0.97-rhel7`
Preparations will be made to start the installation. At this stage the unpacking of files is not being performed.

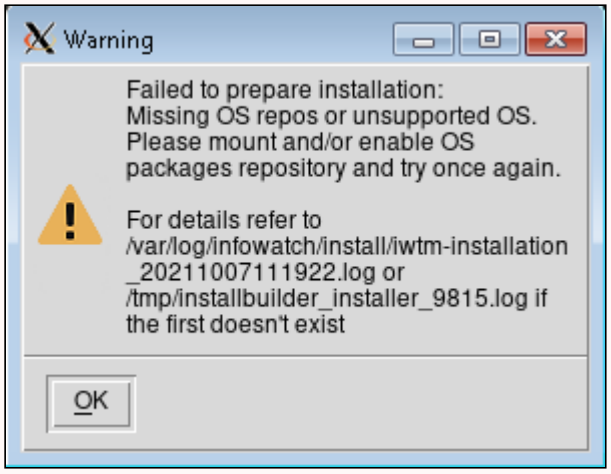
> **Note:**
>
> Before starting the installation a warning about wrong owner of files will be displayed.



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!

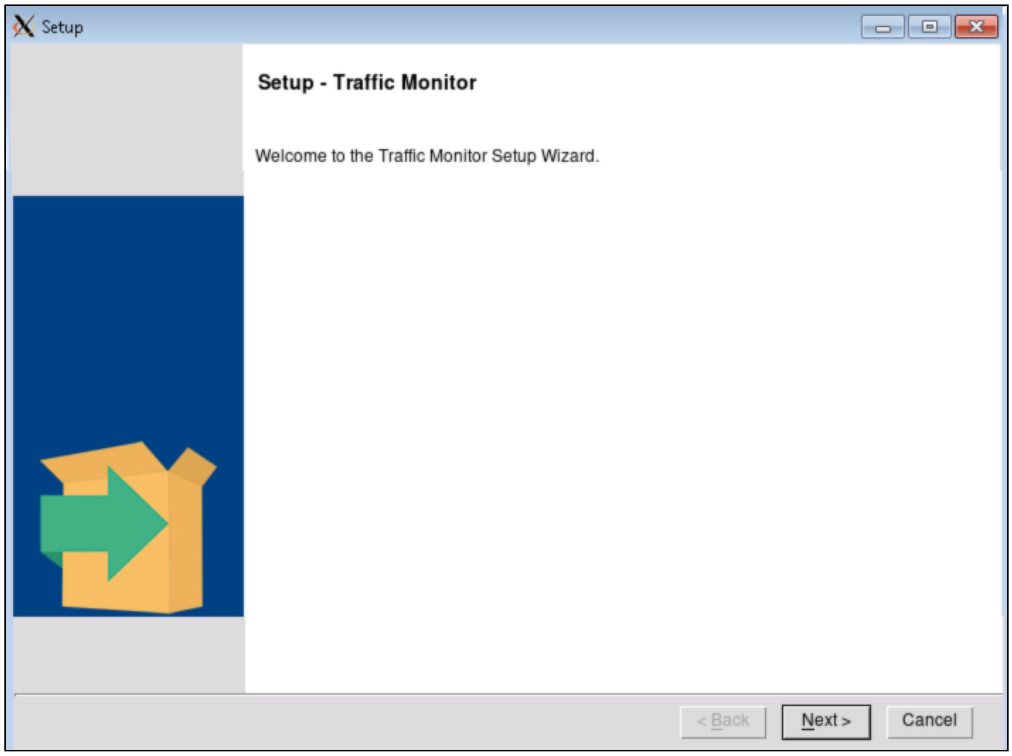
If available configured OS repositories are missing, the preparation process will stop with the following alert box:



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

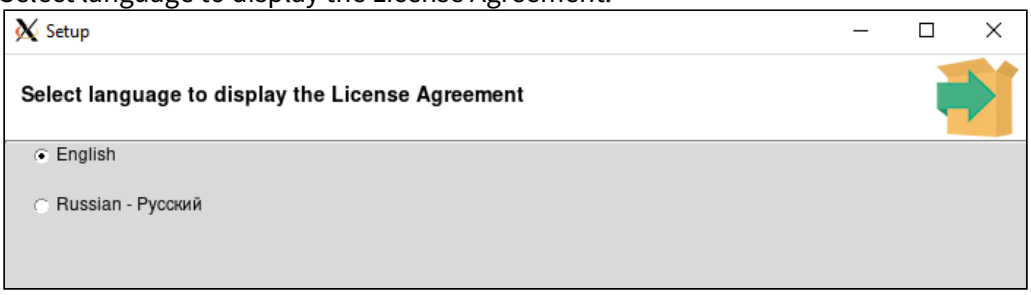
For more details on the error refer to the log files specified in the alert box.

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



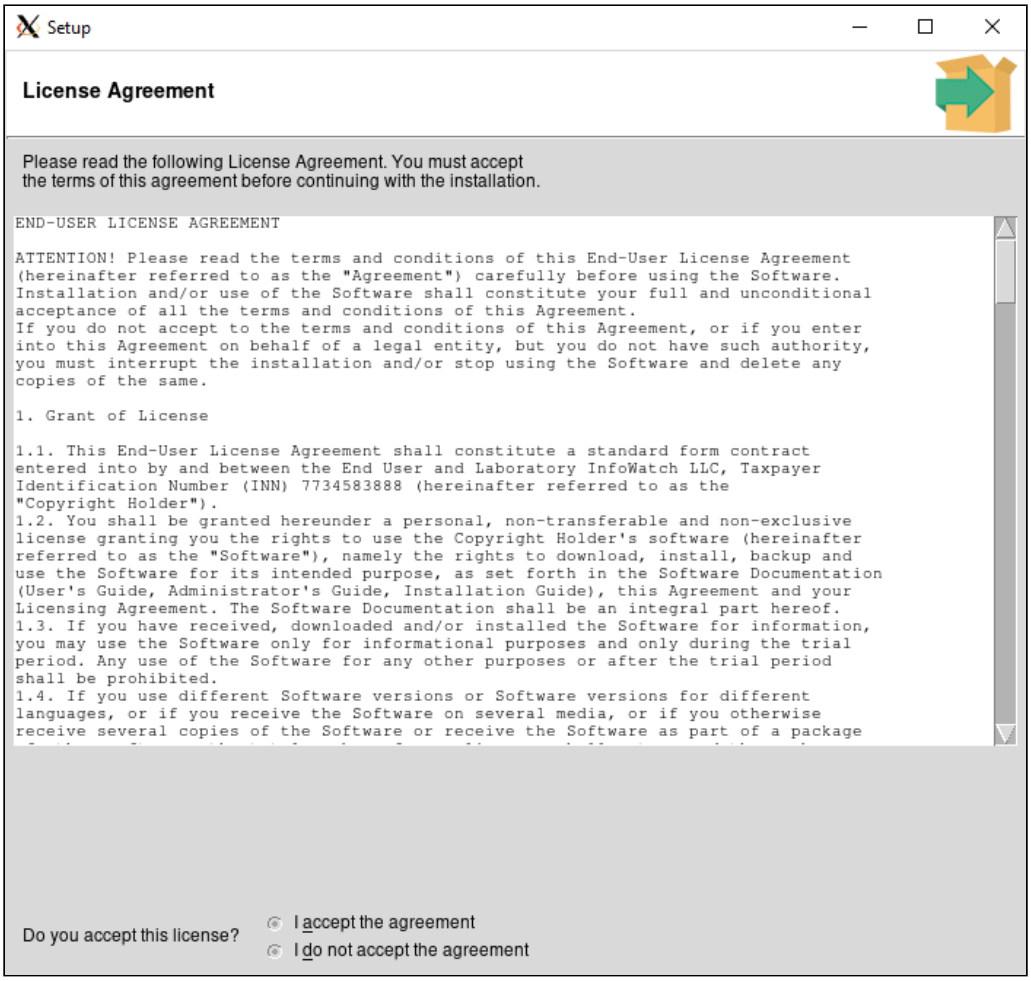
To go to the next parameter press **Next** button, to go back press – **Back**. To exit the installer press **Cancel** button.

f. You must accept the terms of the License Agreement before continuing with the update. For this:
   i. Select language to display the License Agreement:



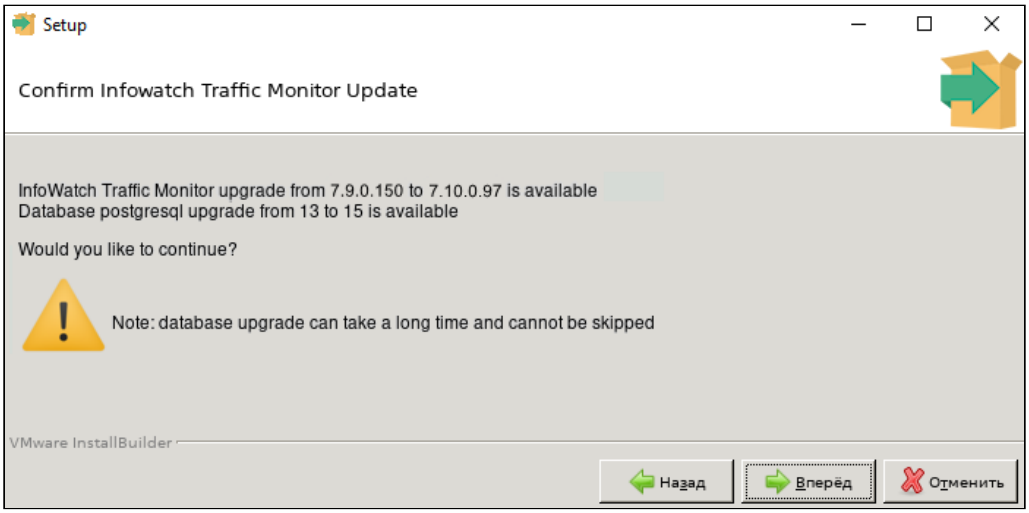
- `English`
- `Russian`

   ii. Select one of the following options. For this, click in the checkbox next to the required value and press the **Next** button:



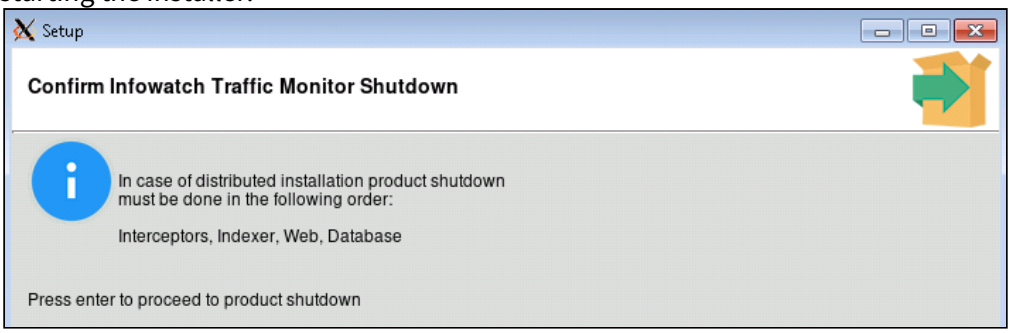
- **`I accept the agreement`** – to accept the License Agreement and continue the update process;
- **`I do not accept the agreement`** – to not accept the License Agreement and abort the update process.

g. The next window will contain data related to available upgrades for Traffic Monitor and DBMS.



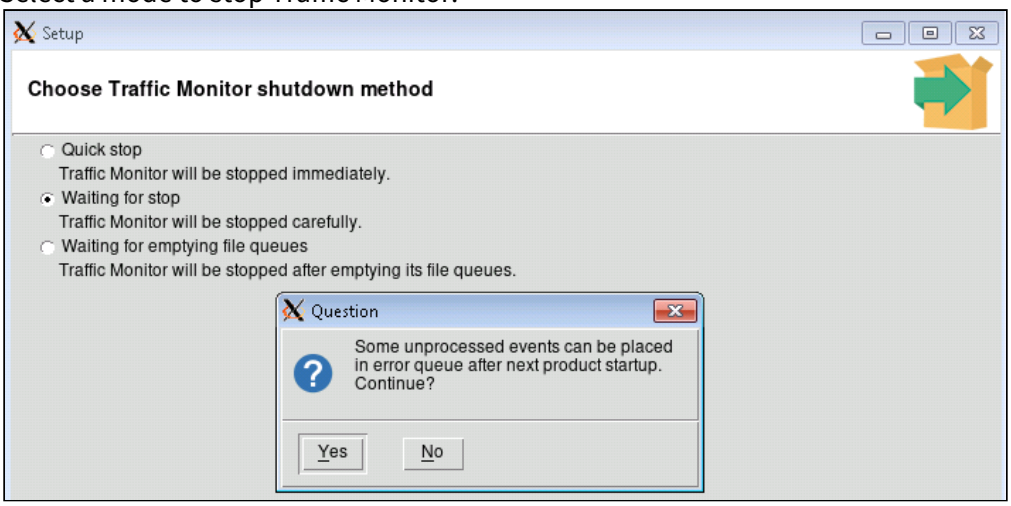
To continue press **Next**.

h. 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:**
>
> If components of Traffic Monitor are operating on several servers, then you should stop them one after another in the following order:
>
> i. Interceptors
> ii. Indexer
> iii. Web console
> iv. Database

i. 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 separate servers, then stopping interceptors and cleaning up file queues may be pending.

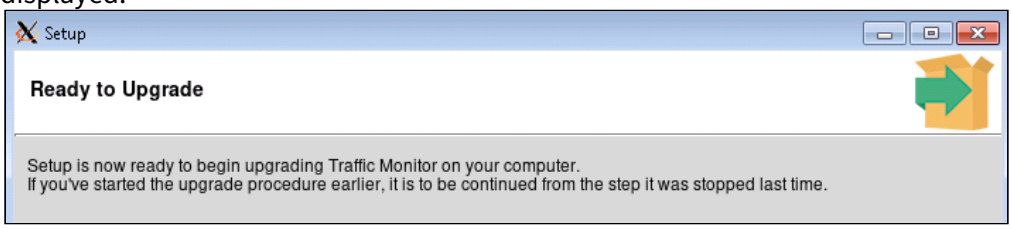
We recommend selecting a different mode or to stop the components manually.

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

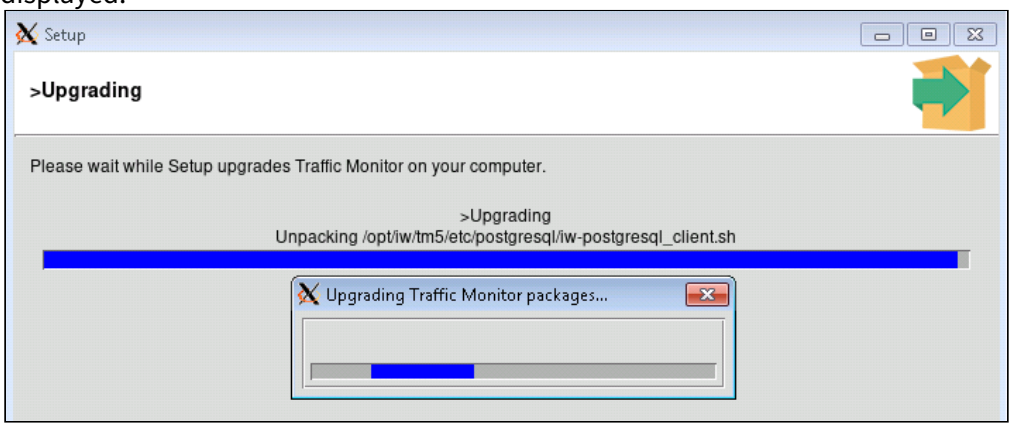
> **Note:**
>
> In case `Quick stop` is selected, the stopped services will have `failed` status before the update.

j. 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 processing progress will be displayed.

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



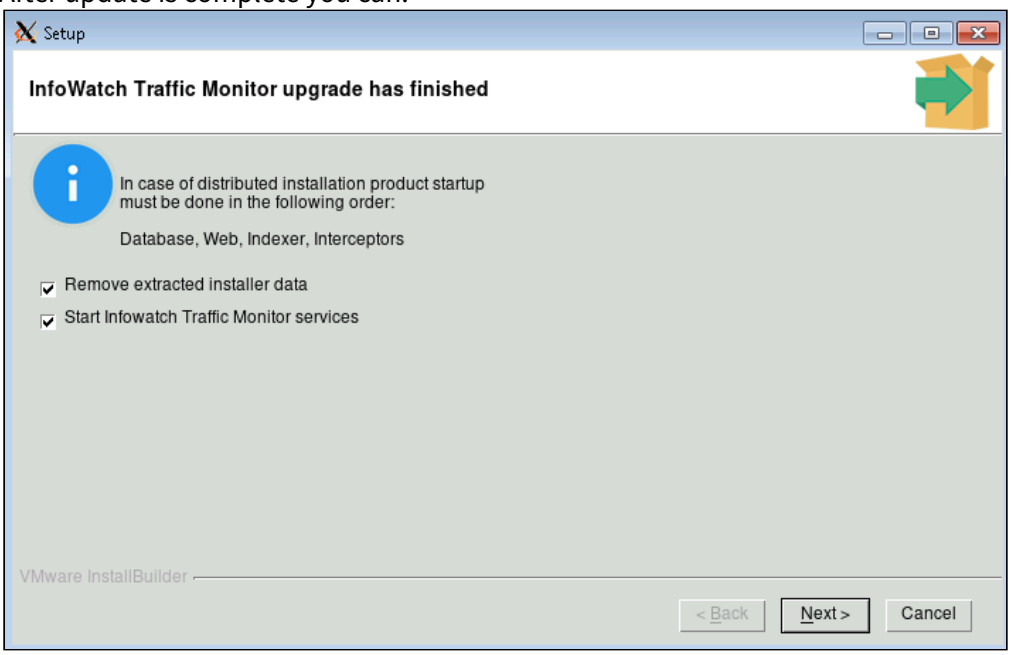
To start the updating press **Yes** button.
The unpacking of Traffic Monitor updating files will start. Implementation progress will be displayed.



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.

l. After update is complete you can:



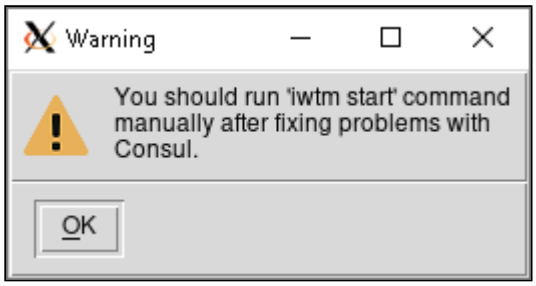
After updating is complete you can:

- **`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;
- **`Start Infowatch Traffic Monitor services`** – start the services which were stopped.

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 **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 start services before updating and starting DBMS server. You can either wait and start the services after you update the DBMS server or continue without starting and do it later manually.

You are required to start the services in the order that depends on the templates activated on these services.

Do not start Traffic Monitor services before the server installed with Database template is updated and started.

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
```

In case `luaengined.conf` configuration file contains `SmtpTmBccList` parameter, before starting services make sure there are no angle brackets (`<` and `>`) in the parameter's value. Otherwise, remove the brackets.

m. 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.

4.5.1 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-7.15.0.97-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.

4.5.2 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:

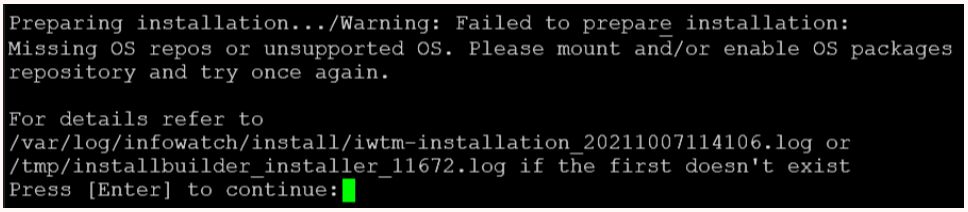
- `none` – no information displayed while updating and no interaction is required;
- `minimal` – status of implementation is displayed while updating, no interaction is required;
- `minimalWithDialogs` – status of implementation is displayed while updating, pop-up windows can be displayed and interaction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

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

```
./iwtm-installer-7.15.0.97-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 alert box:



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

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

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.

4.5.3 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);	If Traffic Monitor components are operating on several servers, then they should be stopped one after another in the following order:

Name	Default value	Valid values	Description	Note
			• `wait_stop` (wait until current events processing is complete); • `clean_fq` – (before stopping wait until all events are processed and the queues are cleared)	a. Interceptors b. Indexer c. Web console d. Data base 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`) If components of interception and components of analysis (`iw_cas` , `iw_pas`) are operating on different servers, then stopping interceptors cleaning file queues might hung. It is recommended to use other modes or to stop them manually.
`start_services_after_upgrade`	`1`	`0,1`	The parameter defines if the installer should run the services after update	Do not start services before updating DBMS server. 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. To manage the monitoring system after the update use iwtm-nagios service.

Name	Default value	Valid values	Description	Note
				For example, to check Nagios status use the command: `systemctl status iwtm-nagios` If `luaengined.conf` configuration file contains `SmtpTmBccList` parameter, and there are angle brackets (`<` and `>`) in the parameter's value, remove the brackets before starting services. In this case, you should not set `start_services_after_upgrade` to `1`. If Traffic Monitor components are operating on several servers, then they should be stopped one after another in the following order: a. Data base b. Web console c. Indexer d. Interceptors
`eula`		`show`, `accept`	Display the License Agreement text, Accept the License Agreement without preview	If you run the installation not in the unattended mode and do not specify the parameter, then the License Agreement text will be displayed. You will be asked to accept the agreement. If you run the installation in the unattended mode, this parameter value is ignored and the License Agreement is accepted by default.

13. Enter the command to find files with **`.rpmnew`** extension, except backups of configuration files:
`find / -name "*rpmnew*" -not -path "/opt/iw/tm5/etc_conf_backup*" -print`
If the files have been found, they are displayed at the console. In this case, you should correctly merge them with configuration files (please see *Merging Configuration Files*).

> **Note:**
>
> To merge successfully the configuration files please see the following articles:
>
> - rpmnew and rpmsave files;
> - Processing rpmnew and rpmsave after the System is updated Red Hat Enterpries Linux.

> **Важно!**
>
> When updating, do not change files **`database.conf`**, **`consul.json`**.
>
> On the server installed with the Web console template, after merging in **`web.conf`** configuration file, in `search_meta` block, `hostname` parameter, specify the IP address of the server with the Indexer template.

14. On servers installed with Interceptors template, in `/opt/iw/tm5/etc/scripts/` directory there should be a file **`iwssid.lua`**, it should be left with no changes in case it was not edited before the update. Otherwise it should be correctly merged with the file **`iwssid.lua.rpmnew`** (please see *Merging Configuration Files*).

> **Note:**
>
> All configuration to work In line was moved to `luaengined.conf`.

15. Check Consul cluster – see the description below.

STEP 2. CHECKING CONSUL CLUSTER

To check Consul cluster take the following steps:

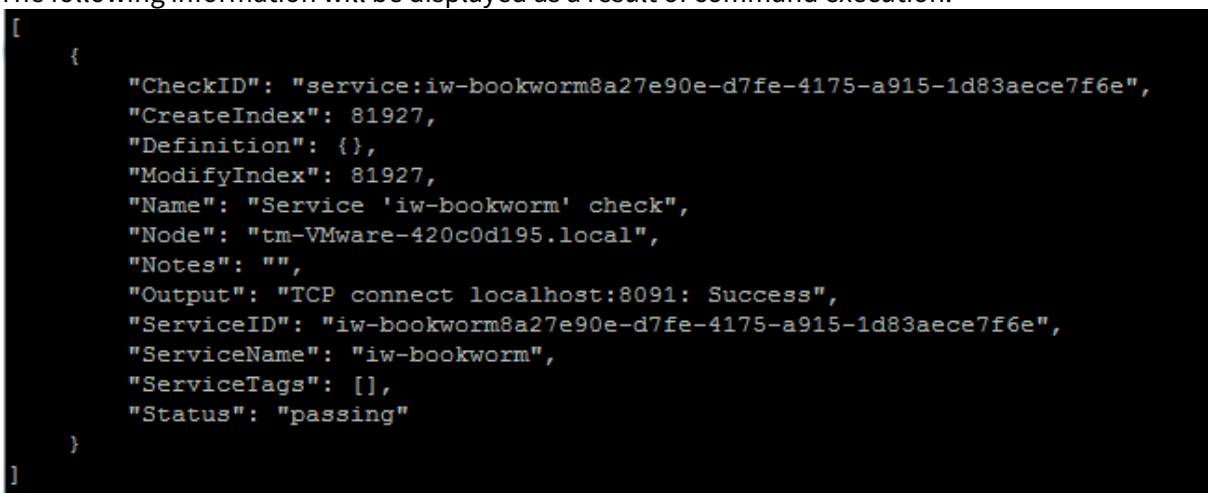
1. Start Consul on all servers to be updated by running the command:
   `service iwtm-consul start`
   Enter the command to check status:
   `service iwtm-consul status`
2. To check Consul on DBMS server (TME DB Server), enter the command:
   a. To get the IP-address of the primary server in the cluster (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 3. 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.

Important!

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.com/support

Log files for checking:

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

To exclude errors, we recommend checking log files even if the services have been started successfully.

Recommended logging level – not lower than INFO. A log file can be missing if no errors registered.

STEP 4. COMPLETING SERVERS UPDATE

To complete servers update, the following action are to be taken as per each of the servers:

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`

   Warning!

   Components of Traffic Monitor should be started in the following order:

   a. Database
   b. Web console
   c. Indexer
   d. Intercepters

   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

```
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**

Error record

```
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.

2. In Traffic Monitor, we have extended the list of default tasks that automatically delete obsolete tasks.
   Tasks for the `cron` scheduler are now specified in the `/etc/cron.d/iwtm_cleanup` file (file contents are described in the *Automatic deletion of unnecessary files in Traffic Monitor* article).
   For new tasks to work correctly:
   a. Delete obsolete tasks by editing the `cron` configuration file:
      `sudo crontab -e`
   b. Save changes and exit the configuration file editor.
   c. Restart the service:
      `systemctl reload crond`

3. If you haven't edited the previous `/etc/cron.d/iwtm_error_queue` file with tasks before the update, then skip this step.
   Otherwise, the `/etc/cron.d/iwtm_error_queue` file will be deleted and its contents will be saved in the `/etc/cron.d/iwtm_error_queue.rpmsave` file.
   For earlier added tasks to start working again, create a file for your tasks in the `/etc/cron.d/` directory and copy required tasks from `/etc/cron.d/iwtm_error_queue.rpmsave` to this file.

   > **Note:**
   >
   > You can add your tasks to the `/etc/cron.d/iwtm_cleanup` file. On the next update, this file will be renamed to `/etc/cron.d/iwtm_cleanup.rpmnew` and replaced with a file with default content. After the next update, you will need to move added tasks from the `/etc/cron.d/iwtm_cleanup.rpmnew` file to a new `/etc/cron.d/iwtm_cleanup` file.
   > To avoid moving tasks every time, you can create a separate file with your tasks in the `/etc/cron.d/` directory.

4. If you are using the Prometheus system and in case the server installed with Database template has not been rebooted to stop the service, you should run the following command:
   `systemctl start iwtm-postgres_exporter` – for **PostgreSQL DBMS**
   `systemctl start iwtm-oracledb_exporter` – for **Oracle DBMS**
5. If the Traffic Monitor server being updated interacts with Data Discovery 2.0 or later, then earlier you stopped the `technologies` pod. Run the pod again. For this:
   a. Connect to the node of the Intestigation Centre cluster.
   b. To start the pod, on the node with the `central` label, run the command:
      `kubectl scale -n infowatch --replicas=1 deployment/technologies-central`
   c. Connect to the terminal of the server with Traffic Monitor again.
6. If you previously stopped the processes of Password Disclosure Adapter, start these processes. For details, see the *InfoWatch Password Disclosure Adapter. Installation and Configuration Guide. Diagnostics and Removal of InfoWatch Password Disclosure Adapter* article.
7. Enter the command to clear cache:
   `yum clean all`
8. Enter the command to test processes' start:
   `iwtm status`
   A list of processes and their statuses will be displayed.

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.

> **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.

Updating the System via installation and restoring data from the backup copy (for PostgreSQL)

Warning!

We strongly recommend backing up the System, cloning it, and updating on this particular testing machine.
If you do not want to copy the data because you will mount the disk or the section containing your data, we recommend to backup them anyway.
After clear installation of the System you will need to set the configuration files of Traffic Monitor again. We recommend to store them so you can configure settings after the update.

In case `luaengined.conf` configuration file contains `SmtpTmBccList` parameter, and there are angle brackets (`<` and `>`) in the parameter's value, remove the brackets before starting services.

1. To stop Traffic Monitor services, run the command:
   `iwtm stop`
2. On the server installed with Database template, check the number of events DB contains. For this, run the command:
   `psql postgres iwtm -c "select count(1) from object;"`
3. Complete *database and indexes backup*.
4. Install a new version of Traffic Monitor.

   Note:

   Unless you plan to change servers with Indexer, Web console and Interceptors templates (e.g. install a new OS or transfer templates to different servers), you can update them *over the installed ones*. In this case, skip steps 8-10 of this instruction.

   Warning!

   If the backup copies of your DB are stored on external devices, do not connect them during the update. You need to do it before restoring and updating the DB.

   When the update is complete, do not remove the packages created by the installer during the process of update (the point **Remove extracted installer data**).

   Perform the following steps on the servers with the new version of Traffic Monitor.
5. To stop services on all servers, run the commands:
   `iwtm stop`
6. On the server installed with Database template:
   a. Enter the command to stop the DB:
      `systemctl stop postgresql-15`

> **Note:**
>
> To restore the initial state of clean installation, you can copy the directories `u01` and `u02`.

b. To change the access rights to the directory, enter the command:
`chmod 777 /var/log/infowatch/update`
c. Copy reserve DB copy so that it was located the same way it was placed initially.
d. Change the owner of the directories by running the commands:
```
chown -R postgres:postgres /u01/
chown -R postgres:postgres /u02/
```
e. Enter the command to go to the directory that contains scripts:
`cd /tmp/iwtm_installer/scripts`
f. From the directory run the script to update the DBMS by using the command:
`./install_postgres.sh --distrib_path=<directory_with_DBMS_distributive> --tm_version=<new_version_of_Traffic_Monitor> --update`
As per our example:
`./install_postgres.sh --distrib_path=/root --tm_version=7.15.0.97 --update`

> **Note:**
>
> In the example the distributive `iwtm-postgresql-15.14-x.x.x.xxx-rhel7.tar.gz` is located in the `/root` directory.
> To view the version of Traffic Monitor you have installed, enter the command:
> `cat /opt/iw/tm5/version`

g. After the successfull update complete the command to check the status of DBMS service:
`systemctl status postgresql-15`
h. Run the script to update the data scheme by using the command:
`./install_dbschema.sh --tm_version=<new_version_of_Traffic_Monitor> --db_type=postgres --update`
As per our example:
`./install_dbschema.sh --tm_version=7.15.0.97 --db_type=postgres --update`
i. Complete the step 2 of the instruction to compare the number of events in the DB before and after the update.

7. On the server with Indexer template:
   a. Copy the backup copies of indexes so that the location and the rights were the same as they were initially.
   If the initial location of indexes is not the default one, then you will have to specify it in the corresponding sections of the configuration files (see *backup instructions*).
   b. Change the owner of the directory by running the command:
   `chown -R iwtm:iwtm /var/lib/sphinx/`
   Command above contains the default location.
8. On the server with Web console template:
   a. Copy the backup copy of `iw_adlibitum` service configuration so that the location and the rights were the same as they were initially.
   If the initial location of `iw_adlibitum` service configuration is not the default one, then

you will have to specify it in the corresponding sections of the configuration files (see *backup instructions*).

b. Change the owner of the directory by running the command:
`chown -R iwtm:iwtm /opt/iw/tm5/etc/adlibitum/`
Command above contains the default location.

c. Run the commands:
`sudo -u iwtm touch /opt/iw/tm5/www/backend/protected/runtime/first_run`
`iwtm restart kicker`

9. Reboot all servers by running the following command on each of them:
`reboot`

> **Warning!**
>
> You should start components of Traffic Monitor one after another in the following order:
>
> a. Database
> b. Web console
> c. Indexer
> d. Interceptors

10. Run the command to check statuses of the processes:
`iwtm status`
The list of processes and their statuses will be displayed.

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

> **Note:**
>
> Clear cache of your browser before starting the works, so the Console is displayed correctly. You can do it by using the standard tools of your browser.

If you updated Traffic Monitor components on Oracle Linux 8, AlmaLinux 8 or Rocky Linux 8 OS, recover the original OS release file.

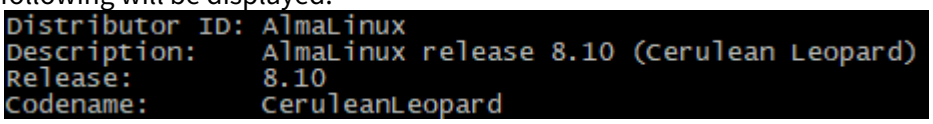
For this:

1. Run the command depending on OS:
   - in Oracle Linux 8:
     `mv /etc/release.bak /etc/oracle-release`
   - in AlmaLinux 8 or Rocky Linux 8:
     `mv /etc/release.bak /etc/redhat-release`
2. Confirm overwriting of the file. For this, enter "`yes`" and press **Enter**.

3. Check that the original release file is successfully recovered. For this, run the command:

```
lsb_release -a
```

As a result, the information on your OS should be displayed. For example, for AlmaLinux 8 OS, the following will be displayed:



Important!

In Traffic Monitor 7.14, we have updated the supplied certificates and the public key that are used for connecting to the XAPI service via SSL. By default, the certificates and the key are stored in the folder `/opt/iw/tm5/etc/cert`.

If you are updating Traffic Monitor from version 7.13 or earlier, and Data Discovery, Device Monitor, adapters, or other third-party services within your perimeter interact with Traffic Monitor using the XAPI service, make sure you factor in such a replacing of certificates and the public key.

If you previously:

- **Used your own** certificates and the key with **names other** than the default file names, the update **will not affect** the interaction of the services, because the files you added will not be deleted.
- **Deleted the files supplied** with the product and used **your own** certificates and the key **with similar names**, after updating, **replace the certificates in Traffic Monitor** with those you generated.
- **Copied** the certificates and the key **supplied** with Traffic Monitor to the folders of other products, adapters, or services, after updating, **copy them again** from the `/opt/iw/tm5/etc/cert` folder.

To learn about installing or changing certificates:

- In **Device Monitor Windows**, see *InfoWatch Device Monitor. Installation, Configuration and Administration Guide. Configuring validation of the remote server certificates*
- In **Device Monitor Linux**, see *InfoWatch Device Monitor for Linux. Installation guide*
- In **Data Discovery**, see *InfoWatch Data Discovery. Administration Guide. Zones and Servers*

Important!

In case before updating Traffic Monitor to version 7.15 service encryption was enabled, make sure your settings correspond to the actual instruction. See *InfoWatch Traffic Monitor. Administration Guide. SSL Thrift Encryption*.

4.6 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.

4.6.1 Merging configuration files in Midnight Commander

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

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

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

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

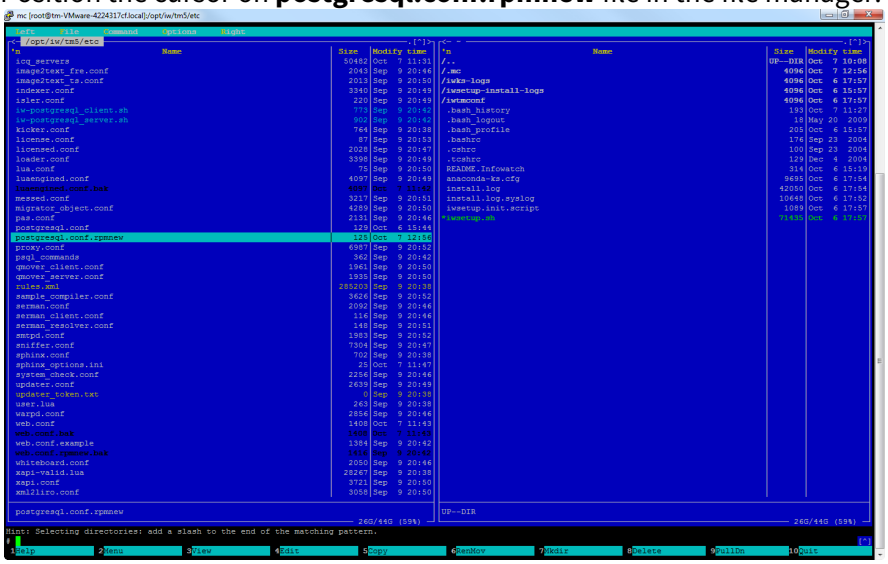
The **postgresql.conf.rpmnew** file looks like:

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

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

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

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



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

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

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

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

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

4.6.2 Merging configuration files by means of vimdiff

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

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

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

4.7 Updating Data Storage

External storage of binary data - Data Storage - is a part of Platform. To update Data Storage, update Platform. You can do it in one of the following ways:

- Update a Platform product if it is installed on the Data Storage server. In this case Platform will be updated automatically.
  You can find update description in this product documentation.
- Update Platform installed without products. This type of update is described below.

Updating Platform

The Traffic Monitor 7.15.0 kit includes Data Storage based on Platform 2.5.0.

Platform 2.5.0 supports:

- standard direct update from versions 2.3.X and 2.4.X;
- update by resetting the current installation and reinstalling over old data.

The distribution kit is an archive whose name is **`iw_platform.tar.xz`**. The archive contains a set of binary modules of container images required for deploying Platform without access to the Internet (offline installation). The archive also contains the updater.

To update Platform, use command line.

> **Note:**
>
> To view the version of Platform you are installing:
>
> 1. Unpack the archive with Platform distributive (see *Updating Platform by Resetting the Installation*, step 5). In our example, into the `platform` directory.
> 2. Run the command:
>
> ```
> cat platform/setup.yaml | grep version
> ```

4.7.1 Direct Update of Platform

To update Platform:

1. Prepare the server for the update (see *Preparing the Server*).

   > **Note:**
   >
   > During the update, the installer checks for:
   >
   > - At least 100 GB of disk space for ClickHouse, PostgreSQL, NATS, and binary data storage directories. If data storage directories are located on different disks, then the installer checks for 100 GB of free space on each of them.
   > - At least 20 GB on a disk for image directories.
   > - At least 8 GB RAM.
   > - At least 2 CPU cores.
   > - Support of SSE 4.2 instructions.
   > - Installed `conntrack` package.

2. Create a new directory for the distribution kit of the new Platform version and go to it:

   ```
   mkdir new_platform
   cd new_platform
   ```

3. Copy the archive to the created directory.
4. Unpack the archive using the command:

   ```
   tar -xvf iw_platform.tar.xz
   ```

5. Make sure that the section with the `/var/lib/containerd` directory has at least 50 GB of free space.
   To view available space, run the command:

   ```
   df -h /var/lib/containerd
   ```

   Note:

   To free up disk space, you can delete images of unused containers from previous versions. **Do not delete the containers of the current installed version.**

   To delete all versions of containers except the specified one:

   a. Add the following strings to the `/etc/crictl.yaml` file (create the file, if needed):

   ```
   runtime-endpoint: unix:///run/containerd/containerd.sock
   image-endpoint: unix:///run/containerd/containerd.sock
   timeout: 2
   pull-image-on-create: false
   disable-pull-on-run: false
   ```

   b. Run the commands:

      i. To delete the Platform containers (where `x.x.x.x` is the **current installed** version of the Platform):

      ```
      crictl rmi $(crictl image | awk '($2 !~ /x.x.x.x|latest/ && $1 ~ /
      docker.infowatch.ru\/platform-core-release/ && $1 !~ /flannel/) {print
      $3}')
      ```

      ii. To delete Docker containers:

      ```
      rm -rf /var/lib/docker
      ```

6. Run Platform update:

   ```
   /setup.py update
   ```

7. Specify the path to temporarily place Traffic Monitor events before uploading them into the Platform (by default, `/opt/factsldrtmdata`) and press **Enter**.
8. Wait until Platform update is complete.
9. Make sure that all services are running. For this, run the command:

   ```
   kubectl get pods -n infowatch
   ```

   The command displays the list of services. Each service should have the status `Running`.
10. If, after the update, you need to free up disk space, you can delete the unused containers the same way as described in step 5.

4.7.2 Updating Platform by Resetting the Installation

Updating using reset consists of the following steps:

1. Resetting the installation **using the new installer**. Resetting the installation does not delete the System data.
2. Installing new version of Platform and specifying already existing folders with data.

> **Note:**
>
> If you connect remotely via SSH, we recommend using the Screen utility to avoid problems in case of a lost connection with the server. When disconnecting from the utility, all the processes started are not to be interrupted and you may safely continue the update.

To update Platform:

1. Follow the steps to prepare the server for the update (see *Preparing the Server*).

   > **Note:**
   >
   > During the update, the installer checks for:
   >
   > - At least 100 GB of disk space for ClickHouse, PostgreSQL, NATS, and binary data storage directories. If data storage directories are located on different disks, then the installer checks for 100 GB of free space on each of them.
   > - At least 20 GB on a disk for image directories.
   > - At least 8 GB RAM.
   > - At least 2 CPU cores.
   > - Support of SSE 4.2 instructions.
   > - Installed `conntrack` package.

2. Create a new directory on the disk (e.g. `platform`):

   ```
   mkdir platform
   ```

3. Copy the **`iw_platform.tar.xz`** archive to the created directory.
4. Open the directory to which you have copied the archive.
5. Unpack the archive with the distribution kit to this directory:

   ```
   tar -xvf iw_platform.tar.xz
   ```

6. Before reseting the installation, remember the current directories where your data are stored. You can get the list of these directories with the command:

   ```
   cat /var/lib/iwplatform/data/volumes.txt
   ```

7. Reset the current installation **using the new installer**:

```
./setup.py reset
```

8. Wait until the Platform reset is complete.
9. Reboot the server using the command:

```
reboot
```

10. If you update and switch to a new server or a new OS, copy directories with the data that were specified during installation and paste them to another partition or to a new server.
By default, the directories are located in **`/opt`**. Be sure to preserve rights and owners when copying the directories. For copying, use standard tools, such as the **`rsync`** utility.
11. To free up some space on your disk, you can delete the `/var/lib/` **`containerd`** directory with container images of previous versions. For this, use the command:

```
rm -rf /var/lib/containerd
```

12. Install the new version of Platform (see *Installing Platform*).

> **Important!**
>
> During the installation, specify existing directories to place the data. When the System asks you if you want to clear up folders before the installation, select "**n**".
>
> By default, the installer creates directories in `/opt`. If, before the update, you used another path, then it is recommended to specify the old directories when installing a new version. On how to view the list of them, see step 6.

13. If after the update you need to free up some space on your disk, then you can delete unused containers, docker or containerd. For details, see the article *How to Delete Unused Docker and Containerd containers?*.

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 Data Storage removal in *Uninstalling Data Storage*.
- See details on DB schema removal in *Deleting the Database Scheme*.
- 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).
- See details on Device Monitor removal (Server and Clients) in *InfoWatch Device Monitor. Installation, Configuration and Administration Guide*.

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 Uninstalling Data Storage

You can uninstall Data Storage via the command line.

To uninstall Data Storage:

1. Break the connection between Traffic Monitor and Data Storage. For this, on the Traffic Monitor server, run the command:
   `platform_conf_ctl --ds-remove`
2. On the Data Storage server, go to the folder to which the installer with the latest Platform version was unpacked.
3. Uninstall Platform by running the command:
   `./setup.py remove`
4. Wait for the uninstallation process to complete.

> **Note:**
>
> The installer will remove components of Platform. After removal, results of the Platform operation will remain on the server. The data will remain in the directories that were specified during installation of Platform.

5.2 Deleting the Database Scheme

> **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 which was installed with Database template, including cases when remote database is used.

In case you're using 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`).

To delete a database scheme, follow the steps:

1. **Stopping Traffic Monitor**
   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.
2. **Starting the scheme removing**
   a. Go to directory
      `/opt/iw/tm5/csw/oracle` or `/opt/iw/tm5/csw/postgres`
   b. Run script:
      `./uninstall.sh`
3. **Removing old versions of configuration**
   a. Remove all content of the directory:
      `rm -rf /opt/iw/tm5/etc/configerator/*`

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. Preset Policies* article);
- Queries and reports (see *InfoWatch Traffic Monitor. User Guide. Reports Section*);
- 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).

Note:

If required, you may delete the database content and indexes as well. Delete it only if you're sure the data cannot be further required.

To do this:

1. Delete the directories `u01` and `u02` using the command:
   `rm -Rvf /u01 /u02`
2. Delete indexes using the command:
   `rm -Rvf /var/lib/sphinx`

5.3 Uninstalling Traffic Monitor

Warning!

If the database is located on the same server, where the uninstallation process is to be started, first, remove the DBMS.

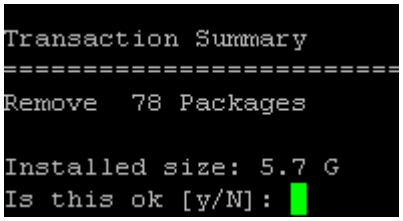
The uninstalling process affects **only** the server where you execute the remove command.If you need to restore events when reinstalling Traffic Monitor, we recommend creating a backup copy of the database before you start the removal (for details, see *InfoWatch Traffic Monitor. Administration Guide. Creating Database Backup* article in *PostgreSQL* or *Oracle* section.We also recommend creating backup copies of the configuration and settings.

Traffic Monitor uninstallation process runs in the server console using OS tools.

To uninstall Traffic Monitor:

1. Enter the login and password to log into the operating system (log in as **root** user using the password created during the installation).
2. Stop Traffic Monitor processes using the command:
   `iwtm stop`
3. To remove Traffic Monitor packages, enter the commad :
   - On servers running Red Hat Enterprise Linux, RED OS, Oracle Linux, AlmaLinux and Rocky Linux:
     `yum remove \`rpm -qa | grep iwtm\``
   - On servers running Alt Server:
     `apt-get remove \`rpm -qa | grep iwtm\``
     Preparing for removal will start.

4. Preparation finished, the list of packages to be removed will be displayed in the confirmation window:



   To continue, enter "**Y**" and press **Enter**.
   Removal of Traffic Monitor packages 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 have been changed (changed files will get the suffix **.rpmsave**, for example, **web.conf.rpmsave**; unchanged files will be removed);
- Object 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. 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 `/opt/iw` directory and all of its content by using OS tools.

> **Warning!**
>
> Before removal, make sure that directories do not contain important information.

To remove the directory, you can use the command:

```
rm -Rvf /opt/iw
```

To be able to reinstall correctly:

1. Delete the file containing information about repository, which was created for product. Use the following command:
   `rm -f /etc/yum.repos.d/tm-x.x.x.xxx-release.repo`
   As per our example:
   ```
   rm -f /etc/yum.repos.d/tm-7.15.0.97-release.repo
   ```
2. If PostgreSQL was used, run the following command to delete the rest components:
   - On servers running Red Hat Enterprise Linux, RED OS, Oracle Linux, AlmaLinux and Rocky Linux:
     ```
     yum remove phantomjs pgagent_15 redis postgresql15 postgresql15-libs postgresql15-server postgresql15-contrib
     ```

- On servers running Alt Server:
  `apt-get remove pgagent redis postgresql15 postgresql15-server postgresql15-contrib`

> **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 «'».
- The user password cannot have «**%**<other_symbols>**%**» format, i.e. it cannot both begin and end with «%» symbol.

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/*
  - libcole.so – *arturo@directmail.org*; *andy.scriven@research.natpower.co.uk*
  - libhtmltree.so – *pauljlucas@mac.com*