

INFOWATCH

InfoWatch Vision 2.0.0. Installation Guide

23/05/2020

© JSC “InfoWatch”

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

http://www.infowatch.com

Table of Contents

1 Who Should Read this Guide 4

2 Set of Documents 5

3 Technical Support 6

4 System installation types. Hardware and software 7

5 Installing Vision 8

5.1 Installing plugin to InfoWatch Traffic Monitor 9

5.1.1 Plugin Archive Description 10

5.1.2 License file description 10

5.2 Configuring access network rules 11

5.3 Troubleshooting 12

6 Updating Vision 13

7 Uninstalling Vision 14

This guide contains information on installation, configuration, update and uninstallation of InfoWatch Vision 2.0.0 - the software intended to visualize the investigations of incidents based on data provided by InfoWatch Traffic Monitor.

1 Who Should Read this Guide

Information in this guide is intended for users who manage the System (perform the System configuration, analyze information objects, etc.).

This guide is intended for users familiar with the basics of Linux operating system.

2 Set of Documents

InfoWatch Vision 2.0.0 documentation package includes the following:

- "InfoWatch Vision. Installation Guide". The document describes how to install, configure, update and uninstall InfoWatch Vision.
- "InfoWatch Vision. Administration Guide". The document contains information on how to configure and prepare the System for proper operation.
- "InfoWatch Vision. User Guide". The document describes the working procedures and tasks facilitating by InfoWatch Vision.

Related documents on InfoWatch Traffic Monitor include as follows:

- "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.

3 Technical Support

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

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

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

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

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

4 System installation types. Hardware and software

There are two types of System installation and deployment concerning Infowatch Traffic Monitor server:

- on a separate server to operate with one or several Traffic Monitor servers (stand-alone)
- on one Traffic Monitor server

Software requirements are assessed in accordance with the volume and complexity of data being analyzed. The table below contains the minimum system requirements for random access memory in the hard disk drive.

<table>
<tr><th rowspan="3">Number of employees</th><th rowspan="3">Number of events</th><th rowspan="3">Events retention period</th><th colspan="4">Software</th></tr>
<tr><th colspan="2">Stand-alone installation</th><th colspan="2">Installing with Traffic Monitor</th><th rowspan="2">Processor</th></tr>
<tr><th>RAM</th><th>HDD</th><th>RAM</th><th>HDD</th></tr>
<tr><td>100</td><td>100 thousand</td><td rowspan="6">3 months</td><td>4 GB</td><td>330 MB</td><td>16 GB</td><td>50 GB</td><td rowspan="6">Number of cores - 6
Frequency - 3.1 GHz
Bitness - 64 bit
Support for SSE 4.2 instructions</td></tr>
<tr><td>500</td><td>500 thousand</td><td>4 GB</td><td>2 GB</td><td>24 GB</td><td>100 GB</td></tr>
<tr><td>1000</td><td>1 million</td><td>4 GB</td><td>5 GB</td><td colspan="2" rowspan="4">Joint Systems installation is not recommended due to high load to hardware resources</td></tr>
<tr><td>5 000</td><td>5 million</td><td>8 GB</td><td>20 GB</td></tr>
<tr><td>10 000</td><td>10 million</td><td>16 GB</td><td>35 GB</td></tr>
<tr><td>50 000</td><td>50 million</td><td>32 GB</td><td>160 GB</td></tr>
</table>

The System can be installed on the following operating systems:

- Astra Linux Special Edition 1.6 "Smolensk"
- Red Hat Enterprise Linux 7 and later
- CentOS Linux 7

PostgreSQL DBMS is to be used. The security officer can operate using Google Chrome and Yandex Browser.

Note:

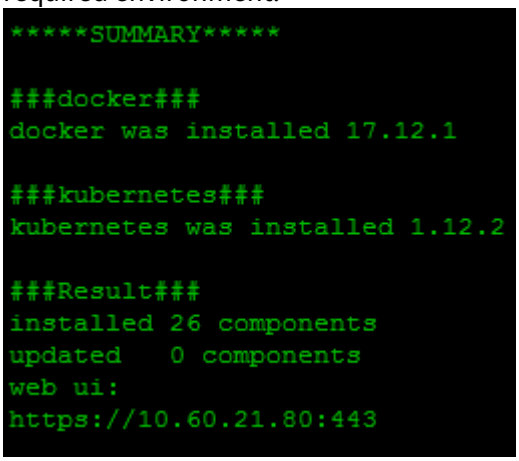
We recommend installing the System in companies with Active Directory, which shall not exceed 100000 users.

5 Installing Vision

Software distribution kit is an **iw_vision2.0_setup_2.0.0.xxxx.tar.xz** archive, where xxxx is an assembling number. This archive contains a full set of containers images with binary modules, required to deploy the System without internet access (offline installation). Besides, this archive contains the installation program. This installation program is written on Python 2.7 version that's why to install the System on OS running you should install the language interpreter first.

To install the System:

1. Create a `vision` directory on the drive:
   `mkdir vision`
2. Copy `iw_vision_setup_2.0.xxxx.tar.xz` archive to this directory.
3. Unpack the archive with distribution kit into this directory:
   `tar xf./iw_vision_setup_2.0.xxxx.tar.xz`
   To install the System on CentOS 7 operating system the package **xz-utils** is required, which is used to install the command line tools to operate with **xz** compression format. So you also need to:
   a. Unpack the archive and get the tar-file:
   `unxz iw_vision2.0_setup_2.0.0.xxxx.tar.xz`
   b. Unpack the received file into the current directory:
   `tar -xvf iw_vision2.0_setup_2.0.0.xxxx.tar`
4. Run the installation program:
   `./setup.py install`
5. Read the license agreement, which consists of a few pages. To go to the next page, press **Enter**.
6. Enter "y" to accept the license agreement and then press **Enter**.
7. Enter the IP address of IPv4 format: "`xxx.xxx.xxx.xxx`" and press **Enter**.
8. Specify the database type (the default one is `iw`) and press **Enter**.
9. Specify the path to place Clickhouse data (by default: `/mnt/chdata`) and press **Enter**.
10. Select the disk space in percent from the total amount of storage required for `/mnt/trdata` (by default: 45%) and press **Enter**.
11. Specify the path to place Tarantool data (by default: `/mnt/trdata`) and press **Enter**.
12. Select the disk space in percent from the total amount of storage required for `/mnt/trdata` (by default: 45%) and press **Enter**.
13. Specify the path to place PostgreSQL data (by default: `/mnt/pgdata`) and press **Enter**.
14. Select the disk space in percent from the total amount of storage required for `/mnt/pgdata` (by default: 10%) and press **Enter**.
15. Specify web interface connection port (by default: `443`) and press **Enter**.
16. Wait until the end of the installation. The program will install all the System components and required environment.



17. Configure POD network rules (for details, see "Firewalld and Kubernetes interaction conflicts", "Firewall complete shutdown").
18. Enter the IP address:port you've got (`https://10.60.21.80:443`) into your browser to start using the System.

In this section:

- Installing plugin to InfoWatch Traffic Monitor
- Configuring access network rules
- Troubleshooting

5.1 Installing plugin to InfoWatch Traffic Monitor

To install a license the following actions are to be taken:

1. Log into Traffic Monitor server management console as Security officer.
2. Go to **Administration** -> **Licenses**.
3. In **Licenses** section click .
4. In the opened window clock **Download**.
5. Add the license file **tm_license_yyyy_mm_dd.license**, which was provided by InfoWatch support services specialist using a file manager. After the license has been succesfully added you can see the related information in **Administration** -> **Licenses**.

> **Note:**
>
> InfoWatch Traffic Monitor licence should contain the name of the company issuing a license (**IW**) as well as the name of system receiving data (**Vision**).

To connect to Traffic Monitor server and provide data extraction from it you should install InfoWatch Vision plugin using Traffic Monitor management console. Zip archive is located as follows:

`iw_vision2.0_setup_2.0.0.x.tar/tmplugin/vision.zip`

To install the plugin:

1. Log into Traffic Monitor server management console as Security officer.
2. Go to **Administration** -> **Plugins**.
3. In **Plugins** section click .
4. In the opened window clock **Download**.
5. Add plugin file, using file manager.

After the plugin was successfully added, its information is available in **Administration** -> **Plugins**. For further data export from Traffic Monitor a token is required. This token is automatically created and is available in **Administration** section -> **Plugins** -> **Tokens**. Copy the token data and enter it to **Token** field in InfoWatch Vision managemen console, when setting up an integration.

License file description and plugin archive related information is available in "License file description" and "Plugin archive description". "Binding plugin and license" will tech you how to download a plugin and a license to InfoWatch Traffic Monitor via one archive.

5.1.1 Plugin Archive Description

Plugin is a **.zip** archive which includes the **manifest.json** file, containg the following plugin data:

Code	Description
`{`	
`"PLUGIN_ID": "2C1D7336267741DF9FC226297503CAFF",`	Unique 128 bits plugin identifier (UUID)
`"DISPLAY_NAME": "InfoWatch Vision",`	Unique plugin name
`"DESCRIPTION": "InfoWatch Vision",`	Plugin description
`"VERSION": "2.0.0",`	Plugin version
`"IS_SYSTEM": false,`	"Preset" sign meaning the plugin is installed by default
`"VENDOR": "IW",`	Software company identifier related to company's name, specified in the license
`"PATTERN_SEARCH_LICENSE": "{\"operator\": \"or\",\"conditions\":[{\"importer_name\": \"Vision\"}]}",`	Pattern used to search previously loaded licenses for binding them with plugin
`"DATA_RECEIVER": ["Vision"],`	Events receiving system

`"LICENSE": [ ]`	License files paths section
	Example:
	`"LICENSE": [`
	`{"PATH":"licenses/license file 1.license"},`
	`{"PATH":"licenses/license file 2.license"},`
	`],`

`}`	

5.1.2 License file description

The license file **tm_license_yyyy_mm_dd.license** contains the following parameters:

Code	Description
`{`	
`"License": {`	License description

`"ActiveDays": 60,`	Period of validity: • for demonstartion - by default 30 days, maximum 60 days; • for commercial - 365 days
`"Features": [`	Licensed channels
`{`	
`"common_name": "IW",`	Company, issuing a license
`"importer_name": "Vision"`	System receiving TM data
`}`	
`],`	
`"Signature": "304502206a59cc72611dffe2a4a73e4e08e2b5386edf8d8fc336fd2f40ae643e",`	Digital signature which was generated based on digital fingerprint
`"Licensee": "",`	License purchaser (licensee)
`"Meta": {`	License parameters
`"restrictions": "demo",`	Kind of license: demonstartion or commercial
`"type": "standard",`	License type: standard or corporate
`"users": "10000",`	Maximum number of users
`"context": "3eeaa674ef003f48762287379980888ce1a9b6dc5b65435be66dd3eb258e7b5afb"`	
`},`	
`"Fingerprint": "002704ff708441611350b7f0368ef082201f7e509f953b618db63fcb4e9abbe7",`	Digital fingerprint
`"IssueDate": "2019-08-06",`	Issue date
`"Issuer": "InfoWatch"`	License issuer
`}`	
`}`	

5.2 Configuring access network rules

The following connections should be enabled for proper System operation:

Connection	Port	Description
Administrator's workstation → Vision 2.0 server	TCP 22	Used to manage Vision 2.0 server via ssh console
Security officer's workstation → Vision 2.0 server	TCP 443	Used to access Vision 2.0 web console
Vision 2.0 server → Traffic Monitor web server	TCP 443	Used to load data from Traffic Monitor to Vision 2.0
Vision 2.0 server → LDAP servers	TCP 3268 TCP 389	Used to synchronize Vision 2.0 with LDAP catalogues
Vision 2.0 server → NTP servers	UDP 123	Used to synchronize time
Vision 2.0 server → DNS servers	UDP 53	Used to enable DNS queries

5.3 Troubleshooting

When installing the System a failure may occur: breaking installation process, blackouts, etc. In this case the System will be installed incorrectly. To solve a problem described above you should run reset operations. After reseting, repeat all the steps of installation.

To reset the System installation:

1. Go to the directory, where the System is installed to.
2. Run the command:
   ```
   ./setup.py reset
   ```

6 Updating Vision

Note:

Vision 1.0 cannot be updated to the current version. You should initiate the installation process in accordance with "

How to install Vision 2.0".

To update the System take the following actions:

1. Copy **iw_vision_2.0.xxxx.tar.xz** archive with the new version and paste to installation folder.
2. Unpack the archive containing software distribution kit to:
   `tar xfJ ./iw_vision_2.0.xxxx.tar.xz`
3. Run the updating program:
   `./setup.py update`

When updating the System all user configurations and data stored in the System will be saved.

7 Uninstalling Vision

To uninstall the System the following actions are to be taken:

1. Go to the folder containing the latest software version.
2. Run the command:
   `./setup.py remove`
3. Wait until the end of removal process. The program will remove the System components. The System data will not be removed. If required, these data can be manually removed from the folders you've specified during the installation.