

INFOWATCH

InfoWatch Vision 2.0. Installation Guide

06/07/2019

© 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 2.0 8

5.1 Setting up a firewall 9

5.2 Troubleshooting 9

6 Updating Vision 2.0 10

7 Uninstalling Vision 2.0 11

This guide contains information on installation, configuration, update and uninstallation of InfoWatch Vision 2.0 - 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 documentation package includes the following:

- "InfoWatch Vision 2.0. Installation Guide". The document describes how to install, configure, update and uninstall InfoWatch Vision 2.0.
- "InfoWatch Vision 2.0. Administration Guide". The document contains information on how to configure and prepare the System for proper operation.
- "InfoWatch Vision 2.0. User Guide". The document describes the working procedures and tasks facilitating by InfoWatch Vision 2.0.

Related documents on InfoWatch Traffic Monitor includes as follloows:

- "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 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 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 thousands</td><td rowspan="7">3 months</td><td>4 GB</td><td>330 MB</td><td>16 GB</td><td>50 GB</td><td rowspan="7">Number of cores - 6
Frequency - 3.1 GHz
Bitness - 64 bit</td></tr>
<tr><td>500</td><td>500 thousands</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="5">Joint Systems installation is not recommended due to high load to hardware resources</td></tr>
<tr><td>5 000</td><td>5 millions</td><td>8 GB</td><td>20 GB</td></tr>
<tr><td>10 000</td><td>10 millions</td><td>16 GB</td><td>35 GB</td></tr>
<tr><td>50 000</td><td>50 millions</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. Security officer can operate using Google Chrome browser.

Note:

System is recommended to be installed in the companies with Active Directory, which shall not exceed 100000 users.

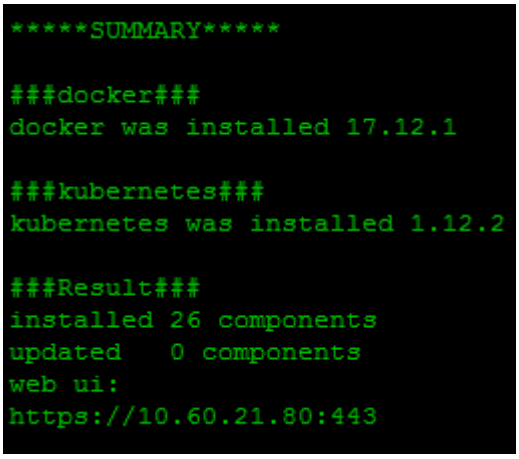
5 Installing Vision 2.0

Software distribution kit is an **iw_vision_2.0.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 directory on vision drive as follows:
   `mkdir vision`
2. Copy `iw_vision_setup_2.0.xxxx.tar.xz` archive to a newly created directory.
3. Unpack the archive with distribution kit into the folder:
   `tar xfJ ./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. Thus the following actions are to be additionally taken:
   a. Unpack the archive and get the tar-file:
   `unxz iw_vision_setup_2.0.xxxx..tar.xz`
   b. Unpack the file you've got into the current directory:
   `tar –xvf iw_vision_setup_2.0.xxxx.tar`
4. Run the installation program:
   `./setup.py install`
5. Read the license agreement consisting of few pages. To go to the next page use **Enter** key.
6. Enter "`y`" to accept the license agreement and then press **Enter**.
7. Enter 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 per cent 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 per cent 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 per cent 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 installation. The program will install all the System components and required environment.



17. Enter the IP address:port you've got (`https://10.60.21.80:443`) into your browser to start using the System.

System installation reset in case of failure

If there is any failure occured during the System installation: installing program interruption, power outage, etc., the System will be installed incorrectly. In this case you should initiate the System reset. After you have reset the System it should be installed again.

To reset the system installation:

1. Go to System installation directory
2. Run the command:
   `./setup.py reset`

5.1 Setting up a firewall

To connect to Traffic Monitor server you should disable firewall (brandmauer). To do this the following actions are to be taken:

1. Log into server using root account.
2. Make sure the brandmauer **firewalld** was started:
   `systemctl status firewalld`
3. If **firewalld** is running, stop it using the command:
   `systemctl stop firewalld`
4. Then the brandmauer will be stopped till the end of current session and to be started again when the new session is started. To change this scenario, remove brandmauer from autorun:
   `systemctl disable firewalld`

5.2 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 you have 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 2.0

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 2.0

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.