

INFOWATCH

InfoWatch Data Discovery. Installation Guide

25/10/2024

© JSC “InfoWatch”

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

http://www.infowatch.com

Table of Contents

1 Who should read this guide 5

2 Set of documents 6

3 Technical support 7

4 Installation/Update Types, Compatibility with Other Products, Hardware and Software Requirements 8

4.1 Installation types and compatibility with other InfoWatch products 8

4.2 Types of update 10

4.3 Exporting data to Traffic Monitor 10

4.4 Hardware and Software Requirements 10

4.4.1 Hardware requirements 10

4.4.2 Software Requirements 11

5 Preparing the Server 12

5.1 The steps to prepare the server: 12

6 Installing Data Discovery 13

6.1 Options for starting the Data Discovery installation 13

6.2 Installing Data Discovery Interactively 13

6.3 Installing Data Discovery with Parameters on the Command Line 18

7 Configuring Network Access Rules 22

8 Installing the License and Plugin 24

8.1 Exporting data to Traffic Monitor 24

8.2 Importing data from Traffic Monitor 24

9 Troubleshooting 26

10 Updating Data Discovery 27

10.1 System settings and data 27

10.2 Data Discovery update options 27

10.3 Direct Update of Data Discovery 28

10.4 Updating Data Discovery by Resetting the Installation 31

10.5 Reinstalling Data Discovery to Another Cluster 33

11 Uninstalling Data Discovery 35

This guide contains information on how to install, update, and remove InfoWatch Data Discovery (also referred to as the System or Data Discovery), software designed to search for confidential information on shared network resources, workstations, servers, and in document storages.

1 Who should read this guide

This guide is intended for deployment engineers and security officers who are going to work with the System and administrate it. This guide is intended for users familiar with the basics of the Linux operating system and PostgreSQL DBMS.

2 Set of documents

The documentation includes:

- "InfoWatch Data Discovery. Installation Guide". The document describes how to install, update, and uninstall the System.
- "InfoWatch Data Discovery. Administration Guide". The document contains information on how to configure the System.
- "InfoWatch Data Discovery. User Guide". The document describes how to work with scanning tasks.

Related documentation for InfoWatch Traffic Monitor (also referred to as Traffic Monitor) includes:

- "InfoWatch Traffic Monitor. Installation Guide". The guide describes how to install, configure, update, and uninstall InfoWatch Traffic Monitor.
- "InfoWatch Traffic Monitor. Administration Guide". The guide describes how to administrate InfoWatch Traffic Monitor (database, back end).
- "InfoWatch Traffic Monitor. User Guide". The guide describes how to work with InfoWatch Traffic Monitor (set up configuration, export/import data, prepare policies for processing objects).
- "InfoWatch Traffic Monitor. Configuration Files Guide". Provides explanations for frequently used configuration files.

3 Technical support

If you have any problems or questions related to the operation of the System, please contact our technical support service:

- If you purchased the product from InfoWatch partner, please contact the technical support service of the partner
- If you purchased the product from InfoWatch directly, please contact InfoWatch technical support 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 the Russian Federation. You can also visit technical support section on our website: http://infowatch.com/support.

4 Installation/Update Types, Compatibility with Other Products, Hardware and Software Requirements

4.1 Installation types and compatibility with other InfoWatch products

InfoWatch Data Discovery is a part of InfoWatch Investigation Centre.

InfoWatch Investigation Centre is a single interface that enable operation and effective interaction between the following InfoWatch products:

- Activity Monitor 3.1
- Data Access Tracker 2.1
- Data Discovery 1.10
- Prediction 3.1
- Vision 3.3

Each product can be installed and operated separately. However, using multiple products simultaneously provides more possibilities for the Security Officer to ensure the company's information security.

The main part for installation of each Investigation Centre product is the Platform. The installer of each product includes both the Platform and the product components. Installing both parts is required when you deploy the products.
Both product components and the Platform have two installation modes:

- `central`
- `office`

You can select the installation mode for the Platform and product when running the installer. If you do not select any mode, the installer will use the default `central` value for both components.

The Investigation Centre supports **distributed installation**: the central (`central`) and office (`office`) nodes of the Platform are combined into a cluster.
You can install components of products both on the central and on the office node of Platform. This allows you to create the Platform cluster with multiple products taking into account the infrastructure, security requirements and available capacity of the company.

> **Important!**
>
> When using a distributed installation, take into account the following key aspects:
>
> - For the products in a cluster to operate correctly, you must install them on the same Platform version. In case you install a product on a newer Platform version, update all the other products in the cluster.
> - In one cluster, you can deploy only one central node of the Platform and a single copy of each product in the central mode.
> - If the cluster already contains a product that was installed in the `central` mode, then another installation of this product in the `central` mode within the same cluster will fail with an error.
> - Data Access Tracler and Prediction can be installed only in the `central` mode. Both products support installation both on the central and on the office node of the Platform.

Product of the same cluster have:

- access to all functionality in one management console;

- common settings;
- common role model;
- access to data regardless of which product is integrated with the source, as well as access to all processed data.
  For example, for Prediction, data that was processed in Activity Monitor has higher priority than data that is received directly from the source - Device Monitor, which is a module of the Traffic Monitor product.

Important!

To connect to the Investigation Centre web interface, you should **always** use the address or name of the server on which the **Platform is installed in the `central` mode**.

If in the distributed installation you installed a product in the `central` node on the Platform office node, you should still use the Platform central node (`central`) for work.

Products of InfoWatch Investigation Centre support **joint installation** on one server.

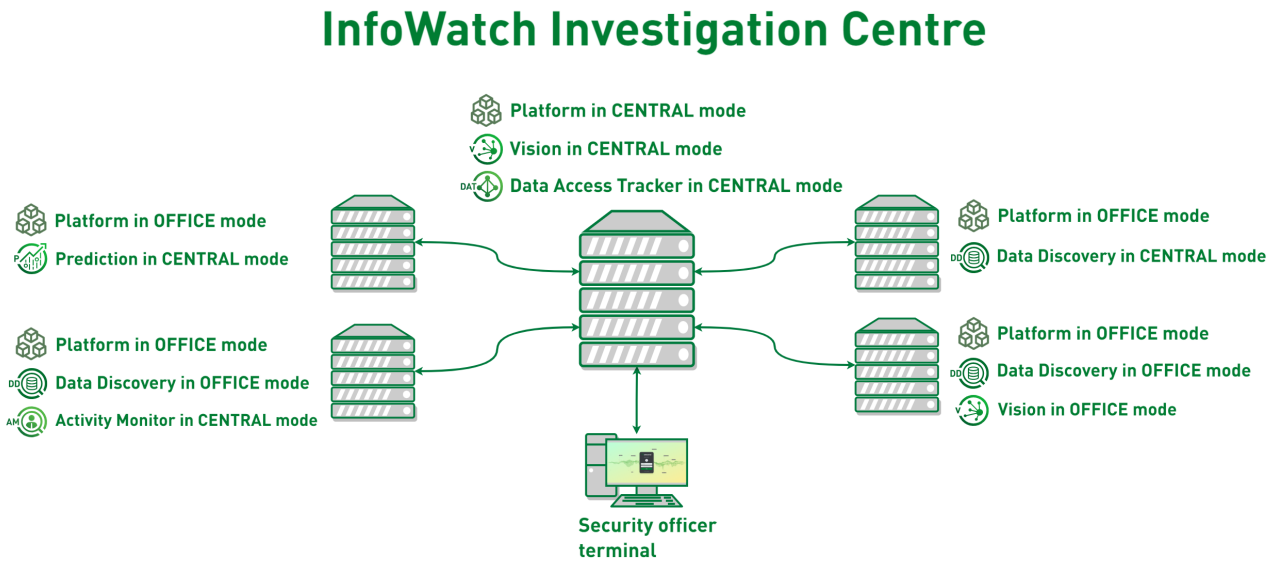
You can install **Data Discovery 1.10 together** with:

- **Activity Monitor 3.1**
- **Data Access Tracker 2.1**
- **Prediction 3.1**
- **Vision 3.3**

Note:

To calculate hardware requirements for joint installations, consider the requirements of each product. To accurately calculate the requirements for a specific project, contact InfoWatch technical support.

Below is an **example** of the Investigation Centre distributed cluster with joint installations of multiple products.



For more information about the installation process, see "Installing Data Discovery".

4.2 Types of update

Data Discovery supports:

- direct update;
- update by resetting and reinstalling over past data.

For more information about the update process and supported options, see "Updating Data Discovery".

4.3 Exporting data to Traffic Monitor

Data Discovery can export data to InfoWatch Traffic Monitor. Data Discovery can work with Traffic Monitor:

- version 6.10.x (6.10.15 and higher);
- version 7.x (7.1 and higher).

For more information about configuring export, see:

- Installing the License and Plugin
- "InfoWatch Data Discovery. Administration Guide", "Zones and servers".

4.4 Hardware and Software Requirements

4.4.1 Hardware requirements

Hardware requirements for Data Discovery depend on the network environment and expected load. Below is an example Data Discovery server configuration for processing 50 hosts within one scanning task:

Component	Recommended requirements
Disk	• Disk array: RAID 5 • Disks: 10K HDD • Disk array capacity: 400 GB **Note**: The required disk space depends on the number and size of files you are going to scan. **Warning!** In case you've used InfoWatch Data Analysis Service functionality, Data Discovery will take a sufficient amount of disk space to store the extracted text contents. Thus you are recommended to increase the disk volume up to 40 per cent, but please take into account that the required space volume depends on text data volume and company's docs flow specifics
RAM	16 GB
CPU	8 cores, 16 threads Intel Xeon or equivalent
Network	1 Gbps LAN

Note:

When calculating the hardware requirements for the joint installation, we recommend that for each component you should sum up requirements for Data Discovery and for other products.

For example: if a product requires 24 GB of RAM, then for this product and Data Discovery to be able to work together, you will need 40 GB of RAM.

Important!

We recommend not installing Data Discovery and Traffic Monitor on the same server. Increased load from Traffic Monitor may lead to incorrect operation of Data Discovery.

4.4.2 Software Requirements

To install and operate the System, you should use the following software:

Software type	Options
Operating system	• Red Hat Enterprise Linux: • versions 7.x (starting from 7.7); • versions 8.x (starting from 8.0); • Oracle Linux: • versions 7.x (starting from 7.9); • versions 8.x (starting from 8.4). **Important**: The **Netfilter** and **NAT** modules must be loaded into the OS kernel
Browser	• Google Chrome; • Yandex.Browser. **Important**: The browser must have hardware support for WebGL/WebGL2

Примечание:

Data Discovery uses DBMS PostgreSQL version 13.8. The DBMS is to be installed together with the product, you are not required to install it separately.

5 Preparing the Server

Before installing Data Discovery, follow the steps to prepare the server.

5.1 The steps to prepare the server:

1. Data Discovery installation program is written in Python 2.7. Install the Python 2.7 interpreter. The distribution kit does not include the interpreter package.
2. Configure POD network rules or disable the firewall (for details, see "Firewalld and Kubernetes Interaction Conflicts" and "Firewall Complete Shutdown").
3. Configure network access rules for the correct operation of the product (for details, see "Configuring Network Access Rules").
4. Data Discovery uses Kubernetes. To enable correct operation of Kubernetes, install the following packages:
   - **socat**;
   - **conntrack** or **conntrack-tools** (you should install this package even if **libnetfilter_conntrack** is already installed).

   > **Note:**
   >
   > The distribution kit does not include these packages.
   >
   > Packages may not be available in the repositories of some operating systems. In this case, you download and install the required packages manually.

5. If you use an antivirus, configure it to operate together with the System (see the Knowledge Base article: "Antivirus Configuration for Platform Products").
6. If the OS uses SELinux, install the **container-selinux** package. This package is required for Data Discovery to operate correctly together with SELinux.

   > **Note:**
   >
   > The distribution kit does not include the package.
   >
   > Package may not be available in the repositories of some operating systems. In this case, download and install the required package manually.

6 Installing Data Discovery

The distribution kit is an archive whose name is **`iw_discovery_setup_1.10.X.xxx.tar.xz`**, where `xxx` is the build number. The archive contains a set of binary modules of container images required for deploying the Platform and Data Discovery components without access to the Internet (offline installation) as well as the installer.

To install Data Discovery, use command line.

You can install Data Discovery:

- on a separate server;
- in a cluster of Data Discovery servers;
- on a server together with other products;
- in a cluster with other products.

6.1 Options for starting the Data Discovery installation

You can start the Data Discovery installation:

- interactively - the installer will sequentially request the installation parameters (see "Installing Data Discovery Interactively"),
- specifying installation parameters in the installer launch command (see "Installing Data Discovery with Parameters on the Command Line").

In both cases, the installer supports joint installation on the same server with other Investigation Centre products as well as distributed installation in a cluster.

Warning!

In case you are installing Data Discovery in the cluster together with other InfoWatch products, then make sure that the Platform version is the same in all the products on all nodes. Otherwise, it is required to update the products installed on the earlier version of Platform.

To view the Platform version of the product you are installing:

1. Unpack the archive with product distributive. In our example, into the `/ddiscovery` directory. To do this go to the directory and run the following command:

   Example for version 1.10.0.192:

   ```
   tar -xvf iw_discovery_setup_1.10.0.192.tar.xz
   ```

2. Run the command:
   `cat /ddiscovery/platform/setup.yaml | grep version`

6.2 Installing Data Discovery Interactively

Note:

If you are installing Data Discovery on the server where other Investigation Centre products are already installed, the installer will not ask for some of the parameters. This happens because these directories and settings were already specified during the initial installation of the Platform.

To install Data Discovery:

1. Make sure that your server meets the hardware and software requirements (see "Data Discovery Installation Types").
2. Follow the steps to prepare the server for installing Data Discovery (see "Preparing the Server").
3. Create a new directory on the server (for example, `distr_discovery`):

```
mkdir distr_discovery
```

4. Copy the **`iw_discovery_setup_1.10.X.xxx.tar.xz`** archive to the created directory. Here, we are using version `1.10.0.171`, so the archive name is `iw_discovery_setup_1.10.0.171.tar.xz`.
5. Open the directory to which you have copied the archive.
6. Unpack the archive with the distribution kit to this directory:

```
tar -xvf iw_discovery_setup_1.10.0.171.tar.xz
```

7. Run the installer using the command like:

```
./setup.py install --nodemode=<Platform_installation_mode> --
productmode=<product_installation_mode>
```

Note:

To install:

- **the product in the central mode on the Platform central node:**

```
./setup.py install --nodemode=central --productmode=central
```

- **the product in the office mode on the Platform central node:**

```
./setup.py install --nodemode=central --productmode=office
```

- **the product in the central mode on the Platform office node:**

```
./setup.py install --nodemode=office --productmode=central
```

- **the product in the office mode on the Platform office node:**

```
./setup.py install --nodemode=office --productmode=office
```

If you do not specify the installation modes for the Platform and the product, the istaller will use the default `central` mode.

If Data Discovery is the first component you are installing on the server and you specify only the `--nodemode` parameter, then the installer will use the same value for the `--productmode` parameter.

Important!

During the installation, the Platform products that are already installed on the server may be unavailable.

8. Read the license agreement. It contains several pages. To go to the next page, press **Enter**.
9. To accept the license agreement, type "**y**" and press **Enter**.

Note:

If you reject the license agreement, the installer will abort the process and exit.

10. If you are intalling the **Platform central node** (`--nodemode=central`), 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" (by default, `0.0.0.0`).
If you specify `0.0.0.0` , all available network interfaces will be used.

Note:

Here and below, to use the default values, press **Enter** without entering any values.

11. If you are installing the **Platform office node** (`--nodemode=office`):
    a. Enter the address of the Platform central node in IP address or domain name format (e.g., `192.0.2.0` or `host.example.com`).
    b. Specify the token to connect to the Platform central node.
    To get a token to connect to the Platform central node:
        i. Connect to the Platform central node console via SSH.
        ii. Run the command in the terminal to get the token:

```
kubeadm token list
```

The token will be displayed on the screen:

```
TOKEN

7tit5e.48g51shamcnn7uq5
```

Here, the token is `7tit5e.48g51shamcnn7uq5`.

iii. Specify the node label (by default, `office`) and press **Enter**.
The label may consist of letters of the Latin alphabet and/or numbers. The length of the label must not exceed 32 characters.

12. Allocate RAM to host Clickhouse data (by default, `80%`) and press **Enter**.
13. Specify the path to place Clickhouse data (by default, `/mnt/chdata`) and press **Enter**.
14. Specify the path to place PostgreSQL data (by default, `/mnt/pgdata`) and press **Enter**.
15. Specify the path to place NATS data (by default, `/mnt/natsdata`) and press **Enter**.
16. Specify the path to place binary data (by default, `/mnt/dsdata`) and press **Enter**.
17. If you are installing the **Platform central node**, specify the port for connecting to the web interface (by default, `443`) and press **Enter**.
18. Wait for the installation of the Platform to finish.
19. Read the Platform installation report.

```
###Result###
Install product: Infowatch Platform
Install manifest section: central
Install node label: central
installed 41 components
updated   0 components
add ref   0 components
web ui:
https://10.60.21.188:443
```

If you install the Platform, the **`web ui`** column contains the address and port for connecting to the web interface (here, `https://10.60.21.188:443`)

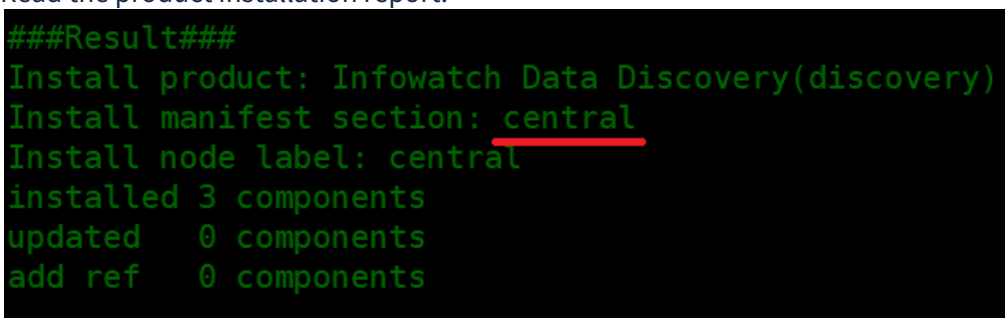
20. Specify the path for storing scanned files (by default, `/mnt/disctps`) and press **Enter**. This path will be used on all servers of the Data Discovery cluster.

> **Important!**
>
> The storage directory must be empty.
>
> After installation, the storage should contain only files and directories that were added by Data Discovery. If you add other files or directories to the storage, Data Discovery may not work correctly.

> **Note:**
>
> We recommend locating the storage on a separate partition or disk. On configuring the server storage, see "*InfoWatch Data Discovery. Administration Guide*", "Zones and servers".

21. Wait for the installation of Data Discovery to finish.

22. Read the product installation report:



23. To display information about the Platform and products in the cluster, run the command:

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

24. Make sure that all services are running. For this, use the following command:

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

The command will display a list of services. Each service should have the `Running` status.

> **Note:**
>
> To increase the speed of scanning resources, you can add Inotify subsystem settings in the OS.
>
> For this:
>
> a. `Open the /etc/sysctl.conf` configuration file for editing.
> b. Add the following lines at the end of the file:
>
> ```
> fs.inotify.max_user_instances = 32768
> fs.inotify.max_user_watches = 32768
> fs.inotify.max_queued_events = 262144
> ```
>
> c. Save the changes and close the configuration file.
> d. To apply the new subsystem settings, run the command:
>
> ```
> sysctl -p
> ```

25. To start using the product, connect to the Investigation Centre web interface. To do this, enter the address and port of the Platform central node in your browser.

> **Note:**
>
> After you install Data Discovery, we recommend configuring rotation of log files. For details, see "InfoWatch Data Discovery. Administration Guide", "Log File Rotation"

6.3 Installing Data Discovery with Parameters on the Command Line

The Data Discovery installer allows you to install the product with minimal user interaction. To do this, run the installation program specifying all the required parameters on the command line.

Before running the Data Discovery installer:

1. Make sure that your server meets the hardware and software requirements (see "Data Discovery Installation Types").
2. Follow the steps to prepare the Data Discovery server for installation ("Preparing the Server").
3. Create a new directory on the disk (e.g., `distr_discovery`):

```
mkdir distr_discovery
```

4. Copy the **`iw_discovery_setup_1.10.X.xxx.tar.xz`** archive to the created directory. Here, we are using version `1.10.0.171`, so the archive name is `iw_discovery_setup_1.10.0.171.tar.xz`.
5. Open the directory to which you have copied the archive.
6. Unpack the archive with the distribution kit to this directory:

```
tar -xvf iw_discovery_setup_1.10.0.171.tar.xz
```

Check out the list of keys in the table below. You can use these keys to specify the product installation parameters for the installer. By default, the values that the installer offers interactively are specified.

> **Note:**
>
> If you do not specify the installation mode for the Platform and product, the installer will use the `central` value.

Key	Default value	Available values	Description
`--nodemode`	`central`	`central, office`	The Platform installation mode
`--productmode`	`central`	`central, office`	The product installation mode
`--loc`	`ru`	`ru, en`	Product localization, the language that is used for pre-installed entities. The parameter is **optional** to run the installer
`--licagree`	`n`	`y, yes, n, no`	Accepting the license agreement

Key	Default value	Available values	Description
`--chmemsize`	`80%`	1-100% or a numeric value If you do not specify %, then the specified value will be treated as the volume in GB	Amount of RAM used for Clickhouse data
`--chdbpath`	`/mnt/chdata`		Path for placing ClickHouse data
`--natspath`	`/mnt/natsdata`		Path for placing NATS data
`--pgdbpath`	`/mnt/pgdata`		Path for placing PostgreSQL data
`--dsdatapath`	`/mnt/dsdata`		Path for placing binary data
`--advertise`	`0.0.0.0`		IP address of the network interface on which the `kubelet` service is running. Specify the value when installing the Platform central node
`--guiport`	`443`		Web interface connection port. Specify the value when installing the Platform central node
`--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` Specify the value when installing the Platform office node

Key	Default value	Available values	Description
`--nodelabel`	`office`		The node label. Specify the value when installing the Platform office node
`--tpspath`	`/mnt/disctps`		Specify the path for storing scanned files. This path will be used on all servers of the Data Discovery cluster. Specify the value when installing the Platform central node

To install Data Discovery:

1. Run the Data Discovery installer with specifying parameters.

   Example command to install the cental Platform and Data Discovery in the central mode:

   ```
   ./setup.py install --nodemode=central --productmode=central --licagree=yes --advertise=0.0.0.0 --chmemsize=80% --chdbpath=/mnt/chdata --pgdbpath=/mnt/pgdata --dsdatapath=/mnt/dsdata --guiport=443 --natspath=/mnt/natsdata --tpspath=/mnt/disctps
   ```

   Example command to install the branch Platform and Data Discovery in the office mode:

   ```
   ./setup.py install --nodemode=office --productmode=office --licagree=yes --nodelabel=lv-426 --cluster=10.60.21.188 --clustertoken=bvp2e1.e9zilgwg7v2urtsr --chdbpath=/mnt/chdata --chmemsize=80% --natspath=/mnt/natsdata --pgdbpath=/mnt/pgdata --dsdatapath=/mnt/dsdata
   ```

2. If you have specified all required parameters, the installer will start the installation.
   If you have not specified some of the parameters, the installer will start the interactive mode and ask you to specify the values.
3. Wait for the Data Discovery installation to complete.
4. To display information about the Platform and products in the cluster, run the command:

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

5. Make sure that all services are running. For this, run the command:

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

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

Note:

To increase the speed of scanning resources, you can add Inotify subsystem settings in the OS.

For this:

a. Open the `/etc/sysctl.conf` configuration file for editing.
b. Add the following lines at the end of the file:

```
fs.inotify.max_user_instances = 32768
fs.inotify.max_user_watches = 32768
fs.inotify.max_queued_events = 262144
```

c. Save the changes and close the configuration file.
d. To apply the new subsystem settings, run the command:

```
sysctl -p
```

6. To start using the product, connect to the Investigation Centre web interface. To do this, enter the central Platform address and port in your browser.

Note:

After you install Data Discovery, we recommend configuring rotation of log files. For details, see "InfoWatch Data Discovery. Administration Guide", "Log File Rotation"

7 Configuring Network Access Rules

For correct operation, the following connections must be allowed:

Connection	Port	Description
Access to the web interface and SSH console		
Administrator workstation → Data Discovery server	TCP 22	Data Discovery server port. Used for managing Data Discovery Server via the SSH protocol
Security Officer workstation → Investigation centre	TCP 443	Port for connection to the Investigation centre web interface (central node of Platform). Default value: **443**. You specify the value during the Platform installation. To change the port number: 1. Reset the System installation (see "Troubleshooting"). 2. Reinstall the System with the new value.
Connections to external systems		
Data Discovery server → Traffic Monitor server	TCP 9100	Traffic Monitor server port. Used for sending data from Data Discovery to Traffic Monitor via XAPI
Data Discovery server → LDAP server	TCP 3268 TCP 389	LDAP server ports. Used for integrating Data Discovery with LDAP directories
Data Discovery server → LDAPS server	TCP 3269 TCP 636	LDAPS server ports. Used for integrating Data Discovery with LDAPS directories
Data Discovery server → DNS server	UDP 53	DNS server port. Used for resolving DNS queries
Data Discovery server → NTP server	UDP 123	NTP server port. Used for time synchronization
Data Discovery server → Mail server	For the protocol: • TLS - 465	The mail server ports. The default values are specified.

Connection	Port	Description
	• STARTTLS - 587	Used to send mail notifications from Prediction and Activity Monitor. Data Discovery uses mail server only for regular report sending
System operation in a cluster		
Platform server in the `office` mode → Platform server in the `central` mode	TCP 6443 TCP 2379, 2380 TCP 10251, 10252, 10255	Platform server ports in the `central` mode. Used for communication between Platform in the `office` mode and Platform in the `central` mode
Platform server in the `central` mode → Platform server in the `office` mode	TCP 10251, 10255 TCP 30000–32767	Platform server ports in the `office` mode. Used for communication between the Platform in the `central` mode and the Platform in the `office` mode
Platform server in the `central` mode ← → Platform server in the `office` mode	UDP 8472 TCP 10250	Used to tunnel traffic between the cluster nodes
Platform server in the `central` mode ← → Platform server in the `office` mode	TCP 10256	The port must be available on all nodes of the cluster. Used to check the status of the `kube-proxy` component

8 Installing the License and Plugin

8.1 Exporting data to Traffic Monitor

Data Discovery allows you to export file copies to Traffic Monitor for analysis. For this, you need **the plugin and the license for interception module** in Traffic Monitor.

To add the license:

1. Log into Traffic Monitor server management console as Security officer.
2. Go to **Administration** -> **Licenses**.
3. In the **Licenses** area, click .
4. Using a file manager, add the **tm_license_yyyy_mm_dd.license** license file you received from InfoWatch technical support service.

After the license has been successfully added, information about it is available in **Administration** -> **Licenses**.

To export data, use the preinstalled plugin in the Traffic Monitor Management Console:

- "InfoWatch Crawler" for Traffic Monitor version 7.3 and higher
- "InfoWatch Data Discovery" for Traffic Monitor whose version is lower than 7.3

The plugin is displayed only if a valid license is installed in Traffic Monitor.

Information about the plugin is displayed in the **Administration** -> **Plugins** section in the Traffic Monitor Management Console. To send data to Traffic Monitor, a token is required. The token is created automatically and available in the **Administration** -> **Plugins** -> **Tokens** section.

For more information about configuring data export, see "*InfoWatch Data Discovery. Administration Guide*", "Zones and servers".

8.2 Importing data from Traffic Monitor

To enable exporting data from Traffic Monitor, you need to configure an integration in the Investigation Centre web interface (for details, see "*InfoWatch Data Discovery. Administration Guide*", the "Integration with InfoWatch Traffic Monitor" article). For this, **the Investigation Centre plugin and license for data export** must be added in Traffic Monitor. A token for integration is automatically created after the plugin is installed. The token is available in the **Administration** > **Plugins** section of the Traffic Monitor Management Console, on the **Tokens** tab of the **InfoWatch Investigation Centre** plugin.

In **Traffic Monitor version 7.10 and later**, the unlimited license for data export to Investigation Centre and the **InfoWatch Investigation Centre** plugin are preinstalled.

In **Traffic Monitor version 7.9 and earlier**, add the license and the plugin manually as decribed below.

To add the license manually:

1. Log into Traffic Monitor server management console as Security officer.
2. Go to **Administration** > **Licenses**.
3. In the **Licenses** area, click .
4. Using a file manager, add the **tm_license_yyyy_mm_dd.license** license file you received from InfoWatch technical support service.

After the license has been successfully added, information about it is available in **Administration** > **Licenses**.

Important!

To export data to Investigation centre, the Traffic Monitor licence must contain the following information:

- company issuing a license - **IW**;
- system receiving data - **Platform**.

To add the plugin manually:

1. Log into Traffic Monitor server management console as Security officer.
2. Go to **Administration** > **Plugins**.
3. In the **Plugins** section, click .
4. In the opened window, click **Select file**.
5. Add plugin file using a file manager.
   The plugin is a zip archive `platform/tmplugin/platform.zip`. Folder with the plugin is located in the directory with the unpacked distributive.

After the plugin has been successfully added, information about it is available in **Administration** > **Plugins**.

The "Binding plugin and license" knowledge base article describes how to download a plugin and a license to InfoWatch Traffic Monitor via one archive.

9 Troubleshooting

The installation may be interrupted by the installer crash, power outage, etc. In this case, the System is installed incorrectly. If this happens, we recommend resetting the installation.

To reset the installation:

1. Stop all scanning tasks in the Data Discovery web interface.
2. Open the directory to which you unpacked the distribution archive during the installation.
3. Run the command:
   `./setup.py reset`

Resetting the installation does not delete results of the System operation. You can use them after reinstalling the System.

Warning!

Resetting the System installation automatically resets all other Platform products installed on the server.

If you reset the installation on the Platform central node, components of all products in the cluster will become unavailable. In this case, reset the installation on each office node.

After installing Data Discovery, reinstall other products in the cluster.

10 Updating Data Discovery

Data Discovery update is supported from the following versions:

- **1.8.0**;
- **1.9.0**;
- **1.9.1**;
- **1.10.0**.

> **Note:**
>
> To update Data Discovery from earlier version, you should first update it to version **1.8** or **1.9.x**.

The distribution kit is an archive whose name is `iw_discovery_setup_1.10.X.xxx.tar.xz`, where `xxx` is the build number. The archive contains a set of binary modules of container images required for deploying the Platform and Data Discovery components without access to the Internet. The archive also contains the updater.

To update Data Discovery, use command line.

10.1 System settings and data

- **Scanning tasks**:
  - Resource processing within the scanning tasks continues from where it ended before the System update.

    > **Warning!**
    >
    > Before updating, stop all the scanning tasks in the Data Discovery interface. Start the tasks manually when the update is completed on all the cluster servers.

- **Configuration files**:
  - If you update Data Discovery by resetting the current installation, some configuration files may be set to the default values. If you have edited the System configuration files, check values in the files after the update.

10.2 Data Discovery update options

All update options support joint work with other Platform products.

> **Important!**
>
> In case of joint installation of Data Discovery and Prediction, stop Prediction data calculation for the duration of Data Discovery update. See the "Required Steps to Update Products that are Installed on Platform together with Prediction" article in the knowledge base for details.

Data Discovery supports:

- Direct standard update

- Update by resetting the current installation and reinstalling over old data

> **Note:**
>
> If you are updating Data Discovery and switching to another server or another OS, use the mode with resetting the current installation.
>
> If Data Discovery works properly, we recommend using the standard update.

To **update a distributed cluster** of Investigation Centre:

1. **Update the central node** of the cluster and all products that are installed on this node.
2. **Update office nodes** and all products that are installed on them.

> **Note:**
>
> If Data Discovery and other products are installed in different clusters, you can update the products in the other cluster and then install the new Data Discovery version to that cluster (for details, see 'Reinstalling Data Discovery to Another Cluster").

> **Warning!**
>
> In case you are updating Data Discovery in the cluster together with other InfoWatch products, then make sure that the Platform version is the same in all the products on all nodes. Otherwise, it is required to update the products installed on the earlier version of Platform.
>
> To view the Platform version of the product you are updating:
>
> 1. Unpack the archive with product distributive. In our example, into the `/ddiscovery` directory. To do this go to the directory and run the following command:
>
>   **Example for version 1.10.0.192:**
>
>    ```
>    tar -xvf iw_discovery_setup_1.10.0.192.tar.xz
>    ```
>
> 2. Run the command:
>   `cat /ddiscovery/platform/setup.yaml | grep version`

10.3 Direct Update of Data Discovery

> **Warning!**
>
> To **update a distributed cluster** of Investigation Centre:
>
> 1. **Update the central node** of the cluster and all products that are installed on this node.
> 2. **Update office nodes** and all products that are installed on them.

To update Data Discovery:

1. **Stop all scanning tasks** in the Data Discovery web interface.
2. Follow the steps to prepare the server for the update ("Preparing the Server").
3. Create a new directory on the disk (e.g., `distr_discovery`):

```
mkdir distr_discovery
```

4. Copy the **`iw_discovery_setup_1.10.X.xxx.tar.xz`** archive to the created directory. Here, we are using version `1.10.0.171`, so the archive name is `iw_discovery_setup_1.10.0.171.tar.xz`.
5. Open the directory, to which you have copied the archive.
6. Unpack the archive with the distribution kit to this directory:

```
tar -xvf iw_discovery_setup_1.10.0.171.tar.xz
```

7. Make sure that the section with the `/var/lib/containerd` directory contains 50 GB or more of disk space.
   To check the volume of available disk space, use the command:

```
df -h /var/lib/containerd
```

> **Note:**
>
> To free up disk space, you can delete unused container images of the previous versions. **Do not remove containers of the currently installed version**. Please note that the commands below will remove all versions of containers except the one specified. To do this complete the following steps:
>
> a. Create a file **`/etc/crictl.yaml`** or add the following content to it:
>
> ```
> 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. Complete the commands:
>
> i. To delete Platform containers (where x.x.x.x - is a **currently installed** version of 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 Data Discovery containers (where x.x.x.x – is a **currently installed** version of Data Discovery):

```
crictl rmi $(crictl image | awk '($2 !~ /x.x.x.x|latest/ && $1 ~ /
docker.infowatch.ru\/discovery/) {print $3}')
```

iii. To delete Docker containers:

```
rm -rf /var/lib/docker
```

8. Run the updater:

```
./setup.py update
```

Warning!

Files metadata left within the storage after scanning tasks deletion will be also deleted **when upgrading to version 1.10**.

During the update, products that are already installed on the server may be unavailable.

9. Wait for the Data Discovery update to complete.
10. Make sure that all services are running. For this, use the following command:

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

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

Note:

To increase the speed of scanning resources, you can add Inotify subsystem settings in the OS.

For this:

a. Open the `/etc/sysctl.conf` configuration file for editing.
b. Add the following lines at the end of the file:

```
fs.inotify.max_user_instances = 32768
fs.inotify.max_user_watches = 32768
fs.inotify.max_queued_events = 262144
```

c. Save the changes and close the configuration file.
d. To apply the new subsystem settings, run the command:

```
sysctl -p
```

11. To display information about the Platform and products in the cluster, run the command:

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

The command will output information about all servers of the cluster.

12. If there are other products installed on the server, update them to versions that are compatible with Data Discovery 1.10 (see "Installation/Update Types, Compatibility with Other Products, Hardware and Software Requirements").
13. If Data Discovery is installed in a distributed cluster, update the Platform and products on other servers to versions that are compatible with Data Discovery 1.10.
14. If you need to free up disk space after updating, you can delete unused `docker` or `containerd` containers. For details, see "How to delete unused Docker and Containerd containers".
15. Clear the cache of the browser you were using before updating the product.
    The Investigation Centre web interface is available at the Platform central node address.

10.4 Updating Data Discovery by Resetting the Installation

> **Warning!**
>
> To **update a distributed cluster** of Investigation Centre:
>
> 1. **Update the central node** of the cluster and all products that are installed on this node.
> 2. **Update office nodes** and all products that are installed on them.

Updating be resetting the installation consists of the following steps:

1. Resetting the installation. Resetting the installation does not delete the System data.
2. Installing new versions of the Platform and product and specifying already existing folders with data.

To update Data Discovery:

1. **Stop all scanning tasks** in the Data Discovery web interface.
2. Follow the steps to prepare the server for the update (see "Preparing the Server").
3. Create a new directory on the disk (e.g., `distr_discovery`):

```
mkdir distr_discovery
```

4. Copy the **`iw_discovery_setup_1.9.X.xxx.tar.xz`** archive to the created directory.
   Here, we are using version `1.10.0.171`, so the archive name is `iw_discovery_setup_1.10.0.171.tar.xz`.
5. Open the directory, to which you have copied the archive.
6. Unpack the archive with the distribution kit to this directory:

```
tar -xvf iw_discovery_setup_1.10.0.171.tar.xz
```

7. When updating, you can assign the same labels to the nodes as they had before the update.
   To view the list of labels in the cluster, run the command:

```
kubectl get node -n infowatch -o jsonpath="{range .items[*]}
{.metadata.annotations.flannel\.alpha\.coreos\.com/public\-ip}
{.metadata.labels.kubernetes\.io/hostname} {.metadata.labels.iwnode}{'\n'}{end}"
```

8. Reset the current installation:

```
./setup.py reset
```

> **Warning!**
>
> If there are other Platform-based products installed on the server, installations of these products will be reset. Branches connected to the central offices will stop working.
>
> After installing the new version of Data Discovery, reinstall the Platform products and specify directories with existing data.

9. Wait for the reset installation process for the Platform and product to complete.
10. If you are also upgrading to a different server or a new OS:
    a. Copy directories with the data that were specified during installation to another partition or to a new server.
    By default, the directories are located along the `/mnt` path. Be sure to preserve rights and owners when copying the directories. For copying, use standard tools, such as the **`rsync`** utility.
    b. After resetting the current installation, copy the `/var/lib/iwplatform/` **`dbadmin.yaml`** file with the database passwords from the old server to the new one.
11. To free up some disk space, you can delete the directory with container images of previous versions `/var/lib/` **`containerd.`** For this, complete the command:

```
rm -rf /var/lib/containerd
```

12. Reboot the server using the command:

```
reboot
```

13. Install the new version of Data Discovery (see "Installing Data Discovery").

> **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**".

14. If other products were installed on the server before the reset, install the product versions that are compatible with Data Discovery 1.9 (see "Installation/Update Types, Compatibility with Other Products, Hardware and Software Requirements").
15. If Data Discovery is installed in a distributed cluster, update the Platform and products on the other servers to versions that are compatible with Data Discovery 1.10.

16. If you need to free up disk space after updating, you can delete unused `docker` or `containerd` containers. For details, see "How to delete unused Docker and Containerd containers".
17. Clear the cache of the browser you were using before updating the product.
    The Investigation Centre web interface is available at the Platform central node address.

10.5 Reinstalling Data Discovery to Another Cluster

If Data Discovery and other products are installed in different clusters, you can install the new version of Data Discovery to the cluster where another product is already installed. As a result, you will be able to work with Data Discovery and the other products in the single web interface of the Investigation Centre. Besides, the products will have common intergrations and the ability to exchange their data.

Important!

Please note that when reinstalling Data Discovery to another cluster, the following entities **will not be transferred**:

- users,
- roles,
- integrations,
- scanning task launch schedules.

As a result, the new cluster of the Investigation Centre will contain only users, roles and integrations that were there before adding Data Discovery.

After reinstallation, **reconfigure the schedules** for launching the scanning tasks.

To reinstall Data Discovery to another cluster:

1. Choose a cluster where you want to install the new version of Data Discovery. In this cluster, update the products to versions that are compatible with Data Discovery 1.10 (see "Installation/Update Types, Compatibility with Other Products, Hardware and Software Requirements").
2. On the Data Discovery server, follow the steps to prepare the server for the update ("Preparing the Server").
3. Create a new directory on the disk (e.g., `distr_discovery`):

   ```
   mkdir distr_discovery
   ```

4. Copy the **`iw_discovery_setup_1.10.X.xxx.tar.xz`** to the created directory.
   Here, we are using version `1.10.0.171`, so the archive name is `iw_discovery_setup_1.10.0.171.tar.xz`.
5. Go to the directory, to which you copied the archive.
6. Unpack the archive with the distibution kit to this directory:

   ```
   tar -xvf iw_discovery_setup_1.10.0.171.tar.xz
   ```

7. Reset the current installation:

   ```
   ./setup.py reset
   ```

8. The Platform and product installation will be reset. Wait for the process to complete.
9. To free up some disk space, you can delete the directory with container images of previous versions `/var/lib/containerd`. For this, use the command:

```
rm -rf /var/lib/containerd
```

10. Reboot the server using the command:

```
reboot
```

11. Install the **Platform office node with the new Data Discovery version** (see "Installing Data Discovery").

> **Important!**
>
> To install Data Discovery on the Platform office node, user the following command:
>
> ```
> ./setup.py install --nodemode=office --productmode=central
> ```
>
> When prompted by the installer, provide the address and token of the new cluster central Platform.
>
> When the installer asks you to specify directories for storing data, specify the directories with the data of the previous version. When asked 'Should I empty folders before installation?', choose «**n**».

12. If you need to free up disk space after updating, you can delete unused Docker and Containerd containers. For details, see the article: "How to delete unused Docker and Containerd containers?".
13. Clear the cache of the browser you were using before updating the product.
The Investigation Centre web interface is available at the address of the Platform central node.

11 Uninstalling Data Discovery

To uninstall Data Discovery:

1. **Stop all tasks** in the Data Discovery web interface.
2. Open the directory on the server, to which you unpacked the distribution archive during Data Discovery installation.
3. Run the command:

   ```
   ./setup.py remove
   ```

4. Wait for the removal to complete. The program will remove the System components. The Data Discovery data will be preserved. If necessary, you can delete the data manually from directories that were specified during the installation.
5. Delete the product internal passwords and related data that remained on the server. For this, use the following commands:

   ```
   kubectl delete daemonsets -l product=discovery -n infowatch
   kubectl delete deployments -l product=discovery -n infowatch
   kubectl delete configmaps -l product=discovery -n infowatch
   kubectl delete secrets -l product=discovery -n infowatch
   ```

Note:

If you remove Data Discovery that was installed in the `central` mode, then the Data Discovery components that were installed in the `office` mode on other nodes are not removed automatically. You need to remove them manually.