INFOWATCH

InfoWatch Data Discovery. Installation Guide

03/09/2026

© 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 This page has not yet been translated to English. products 8

4.2 Types of update 11

4.3 Exporting data to This page has not yet been translated to English. 12

4.4 Hardware and software requirements 12

4.4.1 Hardware requirements 12

4.4.2 Software requirements 14

5 Preparing the Server 16

5.1 The steps to prepare the server: 16

6 Configuring Network Access Rules 18

7 Installing Data Discovery 21

7.1 Options for starting the This page has not yet been translated to English. installation 22

7.2 Content Analysis Module 22

7.3 Installing Data Discovery Interactively 23

7.4 Installing Data Discovery with Parameters in the Command Line 28

7.5 Installing Content Analysis Module Interactively 33

7.6 Installing Content Analysis Module with Parameters on the Command Line 38

8 Installing the License and Plugin 44

8.1 Exporting data to Traffic Monitor 44

8.2 Importing data from Traffic Monitor 44

9 Troubleshooting 46

10 Updating Data Discovery 47

10.1 System settings and data 47
10.2 This page has not yet been translated to English. update options 47
10.3 Content Analysis Module 49
10.4 Features of updating the Investigation Centre cluster 49
10.5 Direct Update of Data Discovery 50
10.6 Updating Data Discovery by Resetting the Installation 54
10.7 Reinstalling Data Discovery to Another Cluster 58
10.8 Direct Update of Content Analysis Module 60
11 Uninstalling Data Discovery 62

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.

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.

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.

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

This page has not yet been translated to English.

products

This page has not yet been translated to English.

is a part of
This page has not yet been translated to English.

Investigation Centre.

This page has not yet been translated to English.

Investigation Centre is a single interface that enables operation and effective interaction between the following
This page has not yet been translated to English.

products:

- This page has not yet been translated to English.

  3.4
- This page has not yet been translated to English.

  2.4
- This page has not yet been translated to English.

  2.2
- This page has not yet been translated to English.

  3.4
- This page has not yet been translated to English.

  3.6

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 don't select any mode, the installer will use the default `central` value for both components.

This page has not yet been translated to English.

2.2 is based on Platform 2.4.1

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:

- All products in the cluster should be installed on the same Platform version, meaning that the first two numbers of the versions should be identical. The central Platform node should have the latest version in the cluster.
- If you install a product on a later Platform version, update all the other products in the cluster afterwards.
- In one cluster, you can deploy only one central node of the Platform and a single copy of each product in the `central` mode.
- For operation of
  This page has not yet been translated to English.

  in the `office` mode, there must be
  This page has not yet been translated to English.

  in the `central` mode in the cluster.
- 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.
- This page has not yet been translated to English.

  can be installed on any Platform node, but only in the `central` mode.

Products in the same cluster have:

- access to all functionality in one management console;
- common settings;
- common role model;
- shared access to data regardless of which product is integrated with the source, as well as access to all processed data.

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` mode on the Platform office node, you should still use the Platform central (`central`) node for work.

This page has not yet been translated to English.

2.2 is based on Platform 2.4.1, but supports **joint installation** and interaction with products and modules based on Platform 2.5. On {You can install Data Discovery 2.2 together with:

On Platform **2.4.1** you can install

This page has not yet been translated to English.

2.2 together with:

- This page has not yet been translated to English.

  3.4
- This page has not yet been translated to English.

2.4

- This page has not yet been translated to English.

3.4

- This page has not yet been translated to English.

3.6

On Platform **2.5** you can install

This page has not yet been translated to English.

2.2 together with:

- This page has not yet been translated to English.

3.5

- This page has not yet been translated to English.

2.4 (based on Platform 2.4.1)

- This page has not yet been translated to English.

3.5

- This page has not yet been translated to English.

3.7

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

This page has not yet been translated to English.

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

This page has not yet been translated to English.

supports:

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

Content Analysis Module supports direct update.

For more information about the update process, see *Updating Data Discovery*.

4.3 Exporting data to

This page has not yet been translated to English.

This page has not yet been translated to English.

can export data to
This page has not yet been translated to English.

.
This page has not yet been translated to English.

can work with
This page has not yet been translated to English.

7.1 and higher.

For more information about configuring export, see:

- *Installing the License and Plugin*
- This page has not yet been translated to English.

  . Administration Guide. *Zones and Servers*

4.4 Hardware and software requirements

4.4.1 Hardware requirements

Hardware requirements for

This page has not yet been translated to English.

depend on the network environment and expected load. Below is an example
This page has not yet been translated to English.

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 are using the functionality of This page has not yet been translated to English. or/and Content Analysis Module, This page has not yet been translated to English. will need additional disk space to store extracted text contents. We recommend increasing the available disk space by 40%. Please keep in mind that the required additional space depends on text data volume and company's document flow.

Component	Recommended requirements
RAM	16 GB
CPU	8 cores, 16 threads Intel Xeon or equivalent, with support for SSE 4.2 instructions
Network	1 Gbps LAN

Note:

ⓘ
When calculating hardware requirements for a joint installation, we recommend that for each component you should sum up requirements for

This page has not yet been translated to English.

and other products.

For example: if a product requires 24 GB of RAM, then for this product and

This page has not yet been translated to English.

to be able to work together, you will need 40 GB of RAM.

You can install the Content Analysis Module, which is used for detecting protected objects in text data, on the same server as

This page has not yet been translated to English.

or separately.
If you are going to use the **Content Analysis Module on the same server as**
This page has not yet been translated to English.

:

- To scan storages using one task and one scanner, hardware requirements for
  This page has not yet been translated to English.

  should be supplemented with **at least**:
  - 2 CPU cores;
  - 1 GB RAM;
  - 50 GB of disk space.
- To scan file storages with a large amount of data using two or more scanning tasks simultaneously with one scanner in each task, add **at least**:
  - 4 CPU cores;
  - 2 GB RAM;
  - 50 GB of disk space.

If the expected load increases, we recommend installing additional Content Analysis Modules on separate servers. The load will be distributed evenly between the servers.
If you are going to use **the Content Analysis Module on a separate server**, ensure **at least**:

- 4 CPU cores;
- 12 GB RAM;
- 100 GB of disk space.

If you use **recognition of text in images (OCR)**, **each running task** with this technology will require adding 8 CPU cores and 4 GB of RAM to the hardware requirements.

Important!

We recommend not installing

This page has not yet been translated to English.

and
This page has not yet been translated to English.

on the same server. Increased load from
This page has not yet been translated to English.

may lead to incorrect operation of
This page has not yet been translated to English.

.

4.4.2 Software requirements

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

Software type	Options
Operating system	• Astra Linux Special Edition, versions: • 1.7, "Voronezh" edition • 1.7.5, "Smolensk" and "Orel" editions • 1.8.0 "Smolensk" edition • Red Hat Enterprise Linux, versions: • 7.9 • 8.9 • 8.10 • Oracle Linux, versions: • 7.9 • 8.4 • RED OS, versions: • 7.3.3 • 8 • ALT Linux: • Server 10.2 • SP 10 **Warning!** It's required that **Netfilter** and **NAT** modules are loaded into the OS kernel.
Browser	• Google Chrome • Yandex Browser **Important**: the browser should have hardware support for WebGL/ WebGL2.

This page has not yet been translated to English.

uses DBMS PostgreSQL version 16.4. The DBMS is supplied with the product and does not require additional installation.

The Content Analysis Module supports installation on the same operating systems as

This page has not yet been translated to English.

.

For the correct operation, the versions of the Content Analysis Module and the configuration of Traffic Monitor that will be used should match.

This page has not yet been translated to English.

2.2 uses the Content Analysis Module versions **7.12.1**, **7.13**, or **7.14**.

Note:

ⓘ
The Content Analysis Module **7.14** is based on the Platform version 2.5.1, while

This page has not yet been translated to English.

2.2 is based on the Platform version 2.4.1 . If you want to use them on separate nodes in the same cluster, contact
This page has not yet been translated to English.

specialists to ensure that all nodes in the cluster use the same Platform version.

To search for similar files,

This page has not yet been translated to English.

2.2 uses
This page has not yet been translated to English.

1.5.0 or **1.6.0**.

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` (install this package even if `libnetfilter_conntrack` is already installed).
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:**

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

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

     ```
     dnf install container-selinux
     ```

   - 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
     ```

7. **If you are installing the product on a server running ALT OS:**

   Install the packages:
   - `python-modules-json`
   - `python-modules-distutils`
   - `python-modules-sqlite3`
8. **If you are installing the product on a server running Astra Linux Special Edition OS:**

Disable `astra-nochmodx-lock` setting.
For this, run the command:

```
astra-nochmodx-lock disable
```

9. Make sure that the date and time of your server are correct.

Note:

The distribution kit does not include the packages listed above.

These packages may be missing in the repositories. In this case, download and install the required packages manually.

6 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
Connection to scanning resources (protocols and storages are specified)		
Data Discovery server → SMB	TCP 139, 445	Port of a host with SMB connection. For scanning shared network resources and workstations running MS Windows OS
Data Discovery server → SSH	TCP 22	Port of a host with SSH connection. For scanning servers and workstations running Linux OS
Data Discovery server → SharePoint	TCP 443	Port of a host with SharePoint connection. For scanning document libraries in SharePoint Server 2016 via HTTPS
Data Discovery server → FTP	TCP 21	Port of a host with FTP connection. For scanning file resources via FTP
Data Discovery server → WebDAV (Nextcloud)	TCP 443	Port of a host with WebDAV connection. For scanning Nextcloud data storages via WebDAV
Data Discovery server → Alfresco	TCP 443	Port of a host with Alfresco system. For scanning server of the Alfresco Community Edition content management system via HTTP/HTTPS
This page has not yet been translated to English. server → Yandex Disk	TCP 443	Port of a host with Yandex Disk. For scanning Yandex Disk storages via REST API Disk. **Note**: For correct Yandex Disk scanning, the following domains should be available: • `https://downloader.disk.yandex.ru/` • `https://storage.yandex.net/` – including all of its first-level

Connection	Port	Description
		subdomains (`*.storage.yandex.net`)
Note: The ports specified for connection to scanning resources are default. If your network infrastructure uses other connection ports, take this into account when creating scanning tasks and adding hosts.		
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

7 Installing Data Discovery

The distribution kit is an archive named

`This page has not yet been translated to English.`

`_2.2.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
This page has not yet been translated to English.

components without access to the internet (offline installation), as well as the installer.

To install

This page has not yet been translated to English.

, use the command line.

You can install

This page has not yet been translated to English.

:

- on a separate server;
- in a cluster of
  This page has not yet been translated to English.

  servers;
- on a server together with other products;
- in a cluster with other products.

In case you are installing

This page has not yet been translated to English.

in the cluster together with other
This page has not yet been translated to English.

products, **make sure that the Platform version is the same in all the products on all nodes**. Otherwise, you need to update the products installed on the earlier version of the Platform.

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

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

   Example for version 2.2.0.191

   ```
   tar -xvf iw_discovery_setup_2.2.0.191.tar.xz
   ```

2. Run the command:

```
cat /ddiscovery/platform/setup.yaml | grep version
```

Note:

ⓘ
If the Platform will be updated to version 2.5 in the cluster with

This page has not yet been translated to English.

2.2, to reconnect the `contentbroker` service to the database, **restart** it.

To do this:

1. Run the restart command:

```
kubectl -n infowatch rollout restart deployment/contentbroker-central
```

2. Check the service status using the command:

```
kubectl -n infowatch rollout status deployment/contentbroker-central
```

Warning!

Make sure that all nodes in a cluster are available for each other in the network. To do this, open the required ports (see *Configuring Access Network Rules*).

Before installation, also make sure that:

- DNS resolution is set up for node names;
  or
- for each node, `/etc/hosts` file specifies accordance between node addresses and names.

To check if nodes are available, run the command between the cluster nodes:

```
ping <node_name>
```

7.1 Options for starting the

This page has not yet been translated to English.

installation

You can start the

This page has not yet been translated to English.

installation:

- **interactively** – the installer will sequentially request the installation parameters (see *Installing Data Discovery Interactively*);
- **by specifying installation parameters** in the installer launch command (see *Installing Data Discovery with Parameters in 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.

7.2 Content Analysis Module

To detect protected objects in scanned text files without sending data to

This page has not yet been translated to English.

for analysis,

This page has not yet been translated to English.

uses a separate Content Analysis Module.

The Content Analysis Module should be installed in the same cluster as

This page has not yet been translated to English.

. You can install it on a separate server or together with
This page has not yet been translated to English.

. For the correct operation, the versions of the Content Analysis Module and Traffic Monitor, the configuration of which will be used, must match. Data Discovery **2.2** uses the Content Analysis Module **7.12.1**, **7.13**, or **7.14**.

You can run the installation of the Content Analysis Module:

- **interactively** – the installer will sequentially ask for installation parameters (see *Installing Content Analysis Module Interactively*);
- **by specifying installation parameters** in the installer launch command (see *Installing Content Analysis Module with Parameters on the Command Line*).

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

7.3 Installing Data Discovery Interactively

Note:

ⓘ
If you are installing

This page has not yet been translated to English.

on a 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

This page has not yet been translated to English.

:

1. Make sure that your server meets the hardware and software requirements (see *Data Discovery Installation Types*).
2. Prepare the server for installing
   This page has not yet been translated to English.
   (see *Preparing the Server*).
3. Create a new directory on the server (for example, `distr_discovery`):

   ```
   mkdir distr_discovery
   ```

4. Copy the
   This page has not yet been translated to English.

   `_2.2.X.xxx.tar.xz` archive to the created directory.
   Here, we are using version `2.2.0.191`, so the archive name is
   This page has not yet been translated to English.

   `_2.2.0.191.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_2.2.0.191.tar.xz
```

7. **To install the product on OS Alt SP 10:**

   Use Kubernetes from the OS repositories.
   To do this:

   a. Follow the steps for OS Alt SP 10 from the article *Preparing the Server*.
   If you have already completed the preparation, skip this step.
   b. Run the command:

   ```
   kubectl taint nodes <node_name> node-role.kubernetes.io/control-plane:NoSchedule-
   ```

   In our example:

   ```
   kubectl taint nodes ddnode node-role.kubernetes.io/control-plane:NoSchedule-
   ```

   c. In the next step, when running the installer, additionally specify the option **`--externalK8S=True`**

8. Run the installer using the command like:

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

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
  ```

Note:

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

If

This page has not yet been translated to English.

is the first component you are installing on the server and you specify only the `--nodemode` parameter, 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.

9. Read the license agreement. It contains several pages. To go to the next page, press **Enter**.
10. 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.

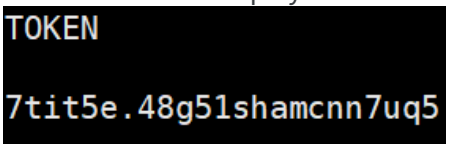
11. If you are installing the **Platform central node** (`--nodemode=central`), enter the IP address of the network interface to communicate with the cluster and press **Enter**. The IP address should be in the IPv4 format: `xxx.xxx.xxx.xxx` (by default, `0.0.0.0`).
If you specify `0.0.0.0` , all available network interfaces will be used.
Note:

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

12. 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 (such as `192.0.2.0` or `host.example.com`).
    b. Specify the token to connect to the Platform central node.
    To get the token:
        i. Connect to the Platform central node management console via SSH.
        ii. In the terminal, run the command to get the token:

```
kubeadm token list
```

The token will be displayed on the screen:

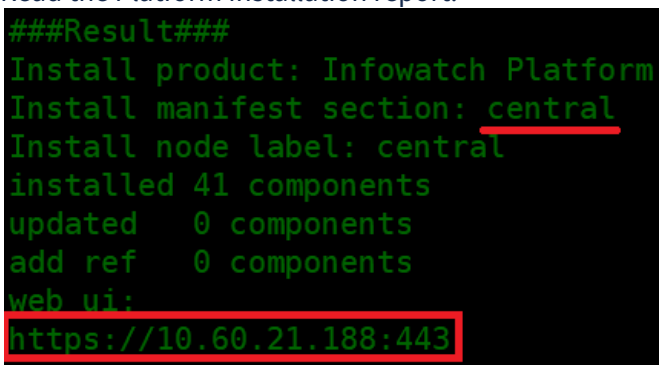


Here, the token is `7tit5e.48g51shamcnn7uq5`

        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.
13. Allocate RAM to host ClickHouse data (by default, `80%`) and press **Enter**.
14. Specify the path to place ClickHouse data (by default, `/opt/chdata`) and press **Enter**.

15. Specify the path to place PostgreSQL data (by default, `/opt/pgdata`) and press **Enter**.
16. Specify the path to place NATS data (by default, `/opt/natsdata`) and press **Enter**.
17. Specify the path to place binary data (by default, `/opt/dsdata`) and press **Enter**.
18. Specify the path to temporarily place
    This page has not yet been translated to English.

    events before uploading them to the Platform (by default, `/opt/factsldrtmdata`) and press **Enter**.
19. If you are installing the **Platform central node**, specify the port for connecting to the web interface (by default, `443`) and press **Enter**.
20. Wait for the installation of the Platform to complete.
21. Read the Platform installation report.

    If you install the Platform central node, the **`web ui`** column contains the address and port for connecting to the web interface (here, `https://10.60.21.188:443`)
22. Specify the path for storing scanned files (by default, `/opt/disctps`) and press **Enter**. This path will be used on all servers of the
    This page has not yet been translated to English.
    cluster.
    Important!

    The storage directory should be empty.

    After installation, the storage should contain only files and directories that were added by

    This page has not yet been translated to English.

    . If you add other files or directories to the storage,
    This page has not yet been translated to English.

    may not work correctly.

    Note:

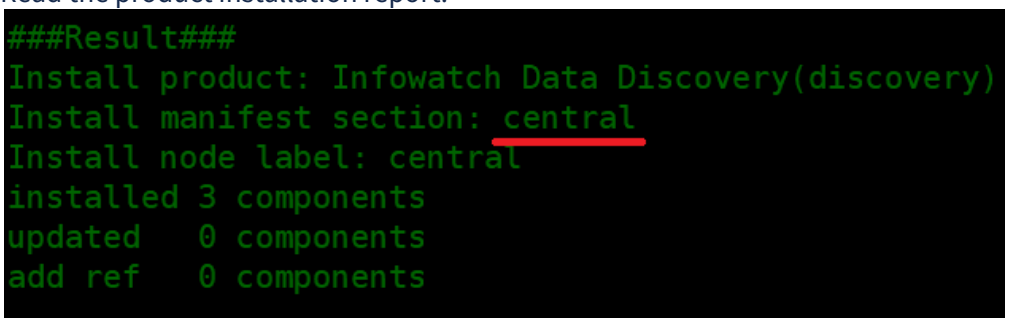
    We recommend placing the server storage on a separate partition or disk. For more information about configuring the server storage, see

    This page has not yet been translated to English.

    . Administration Guide. Zones and Servers.
23. Wait for the
    This page has not yet been translated to English.

    installation to complete.

24. Read the product installation report:



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

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

26. For
This page has not yet been translated to English.
to work, you need to update the settings of the inotify subsystem in the OS.
To do this:
    a. Check if the `/ etc/sysctl.d/discovery.conf` configuration file with the following content is available:

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

    If the configuration file is available, skip the next two steps in the instructions.
    b. If the file was not created by the installer scripts earlier, create it and add the content from the previous step.
    c. To apply the new subsystem settings, run the following command:

    ```
    sysctl --load=/etc/sysctl.d/discovery.conf
    ```

27. 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 status `Running`.
Note:

ⓘ
After installing

This page has not yet been translated to English.

, the installer scripts **enable the rotation and deletion of log files** (see
This page has not yet been translated to English.

. Administration Guide. Log File Rotation).

28. 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:

ⓘ
If in the cluster with the

This page has not yet been translated to English.

2.2 installed the **Platform is updated to version 2.5**, restart the `contentbroker` service to reconnect it to the database.

To do this:

1. On any
   This page has not yet been translated to English.
   node, run the restart command:

   ```
   kubectl -n infowatch rollout restart deployment/contentbroker-central
   ```

2. Check the service status using the command:

   ```
   kubectl -n infowatch rollout status deployment/contentbroker-central
   ```

7.4 Installing Data Discovery with Parameters in the Command Line

With the

This page has not yet been translated to English.

installer, you can install the product with minimal user interaction. To do this, run the installation program specifying all the required parameters in the command line.

Before running the

This page has not yet been translated to English.

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
   This page has not yet been translated to English.
   server for installation (see *Preparing the Server*).
3. Create a new directory on the disk (such as `distr_discovery`):

   ```
   mkdir distr_discovery
   ```

4. Copy the
   This page has not yet been translated to English.
   `_2.2.X.xxx.tar.xz` archive to the created directory.
   Here, we are using version `2.2.0.191`, so the archive name is
   This page has not yet been translated to English.
   `_2.2.0.191.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_2.2.0.191.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. The specified default values are the values offered by the installer in interactive mode.

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.
`--externalK8S`		`True`	Using Kubernetes from the Alt SP OS repositories.
`--loc`	`ru`	`ru, en`	Product localization, the language that is used for pre-installed entities. The parameter is **optional** to run the installer.
`--licagree`	`no`	`yes,no`	Accepting the license agreement.
`--disable-check-free-disk`	-	-	Whether to disable free disk space check: • 20 GB to store images; • 100 GB to store data in specified directories. **Note:** if directories for storing data are located on different disks, the installer checks if 100 GB of free space is available on each of them.
`--disable-check-total-ram`	-	-	Whether to disable check for 8 GB of RAM.
`--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.

Key	Default value	Available values	Description
`--chdbpath`	`/opt/chdata`		Path for storing ClickHouse data.
`--natspath`	`/opt/natsdata`		Path for storing NATS data.
`--pgdbpath`	`/opt/pgdata`		Path for storing PostgreSQL data.
`--dsdatapath`	`/opt/dsdata`		Path for storing binary data.
`--factsldrtmdatapath`	`/opt/factsldrtmdata`		Path to temporarily place This page has not yet been translated to English. events before uploading them to the Platform.
`--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`	`/opt/disctps`		Specify the path for storing scanned files. This path will be used on all servers of the This page has not yet been translated to English. cluster. Specify the value when installing the This page has not yet been translated to English. central node.

To install

This page has not yet been translated to English.

:

1. **To install the product on OS Alt SP 10:**

   Use Kubernetes from the OS repositories.
   For this:

   a. Follow the steps for OS Alt SP 10 in the article *Preparing the Server*.
   If you have already completed the preparation, skip this step.
   b. Run the command:

   ```
   kubectl taint nodes <node_name> node-role.kubernetes.io/control-plane:NoSchedule-
   ```

   In our example:

   ```
   kubectl taint nodes ddnode node-role.kubernetes.io/control-plane:NoSchedule-
   ```

   c. In the next step, when running the installer, specify the option `--externalK8S=True`
2. Run the
   This page has not yet been translated to English.
   installer specifying these parameters.

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

```
./setup.py install --nodemode=central --productmode=central --licagree=yes --advertise=0.0.0
.0 --chmemsize=80% --chdbpath=/opt/chdata --pgdbpath=/opt/pgdata --dsdatapath=/opt/dsdata
```

```
--factsldrtmdatapath=/opt/factsldrtmdata --guiport=443 --natspath=/opt/natsdata --tpspath=/
opt/disctps
```

Example command to install the Platform office node 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=/opt/chdata --
chmemsize=80% --natspath=/opt/natsdata --pgdbpath=/opt/pgdata --dsdatapath=/opt/dsdata --
factsldrtmdatapath=/opt/factsldrtmdata
```

3. 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.
4. Wait for the
   This page has not yet been translated to English.

   installation to complete.
   To display information about the Platform and products in the cluster, run the command:

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

5. For
   This page has not yet been translated to English.
   to work, you need to update the settings of the inotify subsystem in the OS.
   To do this:
   a. Check if the `/ etc/sysctl.d/discovery.conf` configuration file with the following content is available:

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

      If the configuration file is available, skip the next two steps in the instructions.
   b. If the file was not created by the installer scripts earlier, create it and add the content from the previous step.
   c. To apply the new subsystem settings, run the following command:

      ```
      sysctl --load=/etc/sysctl.d/discovery.conf
      ```

6. Make sure that all services are running. To do this, run the command:

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

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

ⓘ
After installing

This page has not yet been translated to English.

, the installer scripts **enable rotation and deletion of log files** (see
This page has not yet been translated to English.

. *Administration Guide. Log File Rotation*).

7. 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:

ⓘ
If in the cluster with

This page has not yet been translated to English.

2.2 installed the **Platform is updated to version 2.5**, restart the `contentbroker` service to reconnect it to the database.

To do this:

1. On any
   This page has not yet been translated to English.
   node, run the restart command:

```
kubectl -n infowatch rollout restart deployment/contentbroker-central
```

2. Check the service status with the command:

```
kubectl -n infowatch rollout status deployment/contentbroker-central
```

7.5 Installing Content Analysis Module Interactively

Note:

ⓘ
The Content Analysis Module should be installed in the same cluster as

This page has not yet been translated to English.

.

If you are installing the Content Analysis Module on a server where other Investigation Centre products are already installed, the installer will not ask for some of the parameters, as those directories and settings were already specified during the initial installation of the Platform.

The instruction applies to versions 7.12, 7.13, and 7.14.

To install the Content Analysis Module:

1. Make sure that your server meets the hardware and software requirements (see *Installation/ Update Types, Compatibility with Other Products, Hardware and Software Requirements*).

2. Follow the steps to prepare the server for installing the Content Analysis Module (see *Preparing the Server*).
3. Create a new directory on the server (for example, `distr_tech`):

```
mkdir distr_tech
```

4. Copy the
This page has not yet been translated to English.

`_7.13.0.xxx.tar.xz` archive to the created directory.
Here, we are using version `7.13.0.167`, so the archive name is
This page has not yet been translated to English.

`_7.13.0.167.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_tm_setup_7.13.0.167.tar.xz
```

7. **To install the module on OS Alt SP 10:**

   Use Kubernetes from the OS repositories.
   For this:

   a. Follow the steps for OS Alt SP 10 from the article *Preparing the Server*.
   If you have already completed the preparation, skip this step.
   b. Run the command:

```
kubectl taint nodes <node_name> node-role.kubernetes.io/control-plane:NoSchedule-
```

   In our example:

```
kubectl taint nodes technode node-role.kubernetes.io/control-plane:NoSchedule-
```

   c. In the next step, when you run the installer, specify the option **`--externalK8S=True`**
8. Run the installer using the command like:

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

   To install:

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

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

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

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

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

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

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

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

If you do not specify the Platform and module installation modes, the installer will select the `central` mode by default.
Important!

During installation, Platform products installed on the server may not be available.

9. Read the license agreement. It contains several pages. To go to the next page, press **Enter**.
10. 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.

11. If you are installing 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 the 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.

12. 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 (for example, `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 should not exceed 32 characters.

13. Allocate RAM to host ClickHouse data (by default, `80%`) and press **Enter**.
14. Specify the path to place ClickHouse data (by default, `/opt/chdata`) and press **Enter**.
15. Specify the path to place PostgreSQL data (by default, `/opt/pgdata`) and press **Enter**.
16. Specify the path to place NATS data (by default, `/opt/natsdata`) and press **Enter**.
17. Specify the path to place binary data (by default, `/opt/dsdata`) and press **Enter**.
18. Specify the path to temporarily place
This page has not yet been translated to English.

events before uploading them into the Platform (by default, `/opt/factsldrtmdata`) and press **Enter**.
19. If you are installing the **Platform central node**, specify the port for connecting to the web interface (by default, `443`) and press **Enter**.
20. Wait for the installation of the Platform to complete.
21. Read the Platform installation report.
22. The Content Analysis Module uses the
This page has not yet been translated to English.
configuration. To upload the configuration, specify the address of the server with the
This page has not yet been translated to English.
database and press **Enter**.
Warning!

Only interaction with **PostgreSQL DBMS** is supported.

In case you are using

This page has not yet been translated to English.

7.10 or earlier versions, protected objects should not contain elements of the Autolinguist technology. In order for content analysis module to work with configurations of these
This page has not yet been translated to English.

versions, remove the elements of the Autolinguist technology from protected objects.

Note:

If
This page has not yet been translated to English.

is installed on several servers or uses a remote database, specify the server where the DBMS is deployed.

If a cluster has several servers with the Content Analysis Module, they all must have the same configuration.

23. Specify the port for connecting to the
This page has not yet been translated to English.

database (by default, `5433`) and press **Enter**.
24. To access the database, specify the password of the **`iwtm_linux`** user.
Note:

If you did not change the user name and password during the

This page has not yet been translated to English.

installation, specify the default values (see
This page has not yet been translated to English.

. *Installation Guide. Pre-installed Server Parameters*).

25. Wait for the installation of the Content Analysis Module to complete.
26. To display information about the Platform and products in the cluster, run the command:

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

27. 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 status `Running`.

28. For
This page has not yet been translated to English.

to work with the Content Analysis Module the protected objects are required. To add them to the Investigation Centre, create an integration with
This page has not yet been translated to English.

and run it (for details, see
This page has not yet been translated to English.

. *Administration Guide. Integration with InfoWatch Traffic Monitor*). We recommend adding protected objects from the
This page has not yet been translated to English.

configuration that was used during installation of the Content Analysis Module.
In case no products in the cluster use
This page has not yet been translated to English.

events, you can select "Data exchange protocol 2.0" in integration settings. With this protocol, the System will receive only the configuration, without events, thereby reducing the load, as well as the time for adding configuration to the product.

After the installation, **Settings** in the **Zones and servers** section of the Investigation Centre will be supplemented:

- a server with the **Content analysis** role will be added, if the Content Analysis Module is installed separately from
This page has not yet been translated to English.

;
- the **Content analysis** role will be added for the existing server, if the Content Analysis Module is installed on the same server as
This page has not yet been translated to English.

.

Note:

ⓘ
You can remove the Content Analysis Module the same way as other products on the Platform:

1. Open the directory with the unpacked distribution kit.
2. Run the command:

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

7.6 Installing Content Analysis Module with Parameters on the Command Line

Note:

ⓘ
The Content Analysis Module should be installed in the same cluster as

This page has not yet been translated to English.

.

If you are installing the Content Analysis Module on a server where other Investigation Centre products are already installed, the installer will not ask for some of the parameters, as those directories and settings were already specified during the initial installation of the Platform.

The instruction applies to versions 7.12.1, 7.13, and 7.14.

The Content Analysis Module installer allows you to install the product with minimal user interaction. To do this, run the installation program specifying all the required parameters in the command line.

Before running the Content Analysis Module installer:

1. Make sure that your server meets the hardware and software requirements (see *Installation/ Update Types, Compatibility with Other Products, Hardware and Software Requirements*).
2. Follow the steps to prepare the server for installing the Content Analysis Module (see *Preparing the Server*).
3. Create a new directory on the server (such as, `distr_cas`):

```
mkdir distr_cas
```

4. Copy the
   This page has not yet been translated to English.

   `_7.13.0.xxx.tar.xz` archive to the created directory.
   Here, we are using version `7.13.0.167`, so the archive name is
   This page has not yet been translated to English.

   `_7.13.0.167.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_tm_setup_7.13.0.167.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 used.

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`	Platform installation mode.
`--productmode`	`central`	`central`, `office`	Module installation mode.
`--externalK8S`		`True`	Using Kubernetes from the OS Alt SP repositories.
`--loc`	`ru`	`ru`, `en`	Product localization, language for pre-installed entities. This parameter is **optional** for running the installer.
`--licagree`	`no`	`yes`, `no`	Acceptance of the license agreement.
`--disable-check-free-disk`	-	-	Whether to disable free disk space check: • 20 GB to store images; • 100 GB to store data in specified directories. **Note:** if directories for storing data are located on different disks, the installer checks if 100 GB of free space is available on each of them.
`--disable-check-total-ram`	-	-	Whether to disable check for 8 GB of RAM.
`--chmemsize`	`80%`	1–100% or a numeric value. If you do not specify %, then the specified value will be treated	Amount of RAM used for ClickHouse data.

Key	Default value	Availabl e values	Description
		as the volume in GB.	
`--chdbpath`	`/opt/chdata`		Path for storing ClickHouse data.
`--natspath`	`/opt/ natsdata`		Path for storing NATS data.
`--pgdbpath`	`/opt/pgdata`		The path to store PostgreSQL database files.
`--dsdatapath`	`/opt/dsdata`		Path for storing binary data.
`-- factsldrtmda tapath`	`/opt/ factsldrtmdat a`		Path to temporarily place This page has not yet been translated to English. events before uploading them to the Platform.
`--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 when installing the Platform office node.
`--nodelabel`	`office`		Node label. Specify when installing the Platform office node.
`--tm-db-host`			Address of the server with the This page has not yet been translated to English. database.

Key	Default value	Availabl e values	Description
			Only interaction with PostgreSQL DBMS is supported. If there are several servers with the Content Analysis Module in the cluster, they should have the same configuration. In case you are using **This page has not yet been translated to English.** **7.10 or earlier** versions, protected objects should not contain elements of the Autolinguist technology. In order for the Content Analysis Module to work with configurations of these This page has not yet been translated to English. versions, remove elements of the Autolinguist technology from protected objects.
`--tm-db-port`	`5443`		Port for connecting to the This page has not yet been translated to English. database.
`--tm-db-pass-iwtm-linux`			The `iwtm_linux` user password to access the database.

To install the Content Analysis Module:

1. **To install the module on OS Alt SP 10:**

   You need to use Kubernetes from the OS repositories.
   For this:

   a. Follow the steps for OS Alt SP 10 from the article *Preparing the Server*.
   If you have already completed the preparation, skip this step.
   b. Run the command:

   ```
   kubectl taint nodes <node_name> node-role.kubernetes.io/control-plane:NoSchedule-
   ```

   In our example:

   ```
   kubectl taint nodes technode node-role.kubernetes.io/control-plane:NoSchedule-
   ```

   c. In the next step, when you run the installer, specify the option `--externalK8S=True`
2. Run the installer specifying these parameters.

Example command to install the cental Platform node and the module in the central mode:

```
./setup.py install --nodemode=central --productmode=central --licagree=yes --advertise=0.0.0.0 --chmemsize=80% --chdbpath=/opt/chdata --pgdbpath=/opt/pgdata --dsdatapath=/opt/dsdata --factsldrtmdatapath=/opt/factsldrtmdata --guiport=443 --natspath=/opt/natsdata --tm-db-host=10.60.22.33 --tm-db-port=5443 --tm-db-pass-iwtm-linux=xxXX1234
```

Example command to install the Platform office node and the module 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=/opt/chdata --chmemsize=80% --natspath=/opt/natsdata --pgdbpath=/opt/pgdata --dsdatapath=/opt/dsdata --factsldrtmdatapath=/opt/factsldrtmdata --tm-db-host=10.60.22.33 --tm-db-port=5443 --tm-db-pass-iwtm-linux=xxXX1234
```

3. 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.
4. Wait for the Content Analysis Module installation to complete.
5. To display information about the Platform and products in the cluster, run the command:

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

6. 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 status `Running`.
7. For
   This page has not yet been translated to English.

   to work with the Content Analysis Module, the protected objects are required. To add them to the Investigation Centre, create an integration with
   This page has not yet been translated to English.

   and run it (for details, see
   This page has not yet been translated to English.

   . *Administration Guide*. *Integration with InfoWatch Traffic Monitor*). We recommend adding protected objects from the
   This page has not yet been translated to English.

   configuration that was used during installation of the Content Analysis Module.
   In case no products in the cluster use
   This page has not yet been translated to English.

   events, you can select "Data exchange protocol 2.0" in integration settings. With this protocol, the System will receive only the configuration, without events, thereby reducing the load, as well as the time for adding configuration to the product.

After the installation, **Settings** in the **Zones and servers** section of the Investigation Centre will be supplemented:

- a server with the **Content analysis** role will be added, if the Content Analysis Module is installed separately from
  This page has not yet been translated to English.

  ;
- the **Content analysis** role will be added for the existing server, if the Content Analysis Module is installed on the same server as
  This page has not yet been translated to English.

  .

Note:

ⓘ
You can remove the Content Analysis Module the same way as other products on the Platform:

1. Open the directory with the unpacked distribution kit.
2. Run the command:

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

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 System settings and then repeat the installation steps. After the reset, all data is saved in the System. So, when you are prompted to delete the existing data during re-installation, select **No**.

To reset the System installation:

1. In case of joint installation of Data Discovery and Prediction, stop Prediction data calculation. For details, see the *Required steps to update products that are installed on Platform together with Prediction* article in the knowledge base.
2. Memorize or save the paths to the current data storing directories. To get a list of the directories, run the command:

   ```
   cat /var/lib/iwplatform/data/volumes.txt
   ```

3. Memorize or save node labels. 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}"
   ```

4. Go to the directory with the unpacked distribution kit of the product.
5. Run the reset command:

   ```
   /setup.py reset
   ```

6. After the reset, assign the same labels to the cluster nodes as they had before the update.

Important!

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, you should reinstall other products in the cluster.

10 Updating Data Discovery

This page has not yet been translated to English.

can be updated from the following versions:

- **2.0**
- **2.1**

Note:



To update

This page has not yet been translated to English.

from earlier versions, first update it to one of the versions listed above.

The distribution kit is an archive named

This page has not yet been translated to English.

`_2.2.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
This page has not yet been translated to English.

components without access to the internet. The archive also contains the updater.

To update

This page has not yet been translated to English.

, use the 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

    This page has not yet been translated to English.

    interface. Start the tasks manually when the update is completed on all the cluster servers.
- **Configuration files**:
  - If you update 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 This page has not yet been translated to English. update options

Important!



In case of joint installation of

This page has not yet been translated to English.

and
This page has not yet been translated to English.

, stop
This page has not yet been translated to English.

data calculation for the duration of
This page has not yet been translated to English.

update. For details, see
This page has not yet been translated to English.

. *Installation Guide. Direct Update of*
This page has not yet been translated to English.

or *Updating*
This page has not yet been translated to English.

by Resetting the Installation.

This page has not yet been translated to English.

2.2 supports:

- direct update
- update by resetting the current installation and reinstalling over old data

If

This page has not yet been translated to English.

and other products are installed in different clusters, you can update the products in the other cluster and then install the new
This page has not yet been translated to English.

version to that cluster (for details, see *Reinstalling Data Discovery to Another Cluster*).

Warning!

In case you are updating

This page has not yet been translated to English.

in the cluster together with other
This page has not yet been translated to English.

products, make sure that the Platform version is the same for 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 the product distributive. In our example, to the `/ddiscovery` directory. To do this, go to the directory and run the following command:

   Example for version 2.2.0.191:

   ```
   tar -xvf iw_discovery_setup_2.2.0.191.tar.xz
   ```

2. Run the command:

```
cat /ddiscovery/platform/setup.yaml | grep version
```

10.3 Content Analysis Module

This page has not yet been translated to English.

can operate with the Content Analysis Module versions 7.12.1, 7.13, and 7.14. The Content Analysis Module supports direct update from 7.11 and 7.12.

10.4 Features of updating the Investigation Centre cluster

If you have multiple products installed in a cluster, make sure to consider the update requirements for each product before updating.

1. If
   This page has not yet been translated to English.

   is installed in the cluster, **stop** its **data calculation** during any update (for more information, see
   This page has not yet been translated to English.

   . Installation Guide. Direct Update of
   This page has not yet been translated to English.

   or *Updating*
   This page has not yet been translated to English.

   by Resetting the Installation).
2. If
   This page has not yet been translated to English.
   is installed on the updated node, **update** it **first**.
3. If you update the products by resetting the installation (`reset`):
   - To save zone and server settings in the new
     This page has not yet been translated to English.
     version, before resetting the installation, connect to the node where
     This page has not yet been translated to English.
     is installed in the `central` mode and **stop the Discoperator service** by running this command:

     ```
     kubectl scale --replicas=0 deployment discoperator-<node_label> -n infowatch
     ```

     Example for Data Discovery in central mode on the office node with the label lv426:

     ```
     kubectl scale --replicas=0 deployment discoperator-lv426 -n infowatchkubectl scale
     --replicas=0 deployment discoperator-lv426 -n infowatch
     ```

   - **This page has not yet been translated to English.**
     should be the first to be **reinstalled**.

- This page has not yet been translated to English.

  3.4 should be the **last** to be reinstalled.

Before updating the cluster, we also recommend that you read the instructions for all installed products.

10.5 Direct Update of Data Discovery

Warning!

After updating to version 2.2, only the data from the last completed scans will remain, and the **data from previous scans will be deleted**.

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

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.

If you are using a remote connection via SSH protocol, we recommend using the Screen utility to avoid problems if the connection to the server is lost. If you disconnect from the utility, the processes running in it will not be interrupted, which will allow you to continue the update safely.

To update

This page has not yet been translated to English.

:

1. **Stop all scanning tasks** in the
   This page has not yet been translated to English.

   web interface.
2. Prepare the server for the update (see *Preparing the Server*).
3. Create a new directory on the disk (for example, `distr_discovery`):

   ```
   mkdir distr_discovery
   ```

4. Copy the
   This page has not yet been translated to English.

   `_2.2.X.xxx.tar.xz` archive to the created directory.
   Here, we are using version `2.2.0.191`, so the archive name is
   This page has not yet been translated to English.

   `_2.2.0.191.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_2.2.0.191.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. 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 the Platform containers (where `x.x.x.x` is a version of a **currently installed** 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
This page has not yet been translated to English.
containers (where `x.x.x.x` is a version of a **currently installed**
This page has not yet been translated to English.

):

```
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. **During the update**, ClickHouse data migration will require **disk space in addition** to the space allocated for the installer operation and for the transition to the new version. Once the update is complete, the additional space will be freed.
To determine the amount of additional space:

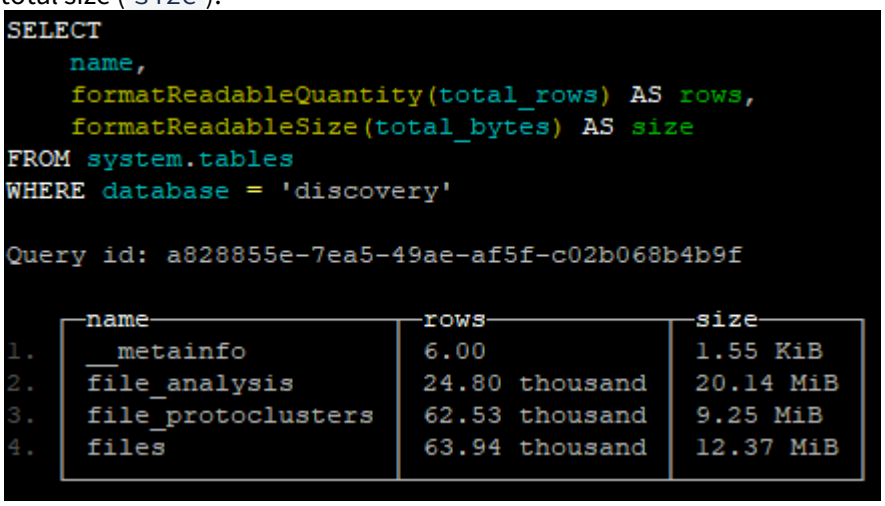
a. On the node with
This page has not yet been translated to English.
in the `central` mode, run the following command to connect to ClickHouse:

```
kubectl exec --stdin --tty -n infowatch deploy/clickhouse-central -- clickhouse-client -d discovery --user discovery --password $(kubectl get secret discoperator-discovery-central-db-secret -n infowatch -o jsonpath='{.data.service_ch_password}' | base64 --decode)
```

b. To get the size of the data tables, run the following request:

```
SELECT
    name,
    formatReadableQuantity(total_rows) AS rows,
    formatReadableSize(total_bytes) AS size
FROM system.tables
WHERE database = 'discovery'
```

The request will display the table names (`name`) with the number of rows (`rows`) and the total size (`size`).



c. To determine the required additional space, select the highest value from the following:
   - size of table **`files` x 3**
   - size of table **`file_analysis` x 2**
   - size of table **`file_protoclusters` x 2**

   Example:

   Table sizes: `files` = 29 GB, `file_analysis` = 42 GB, `file_protoclusters` = 30 GB.

   In this example, additional 87 GB are required, because 29 * 3 = 87 is the highest value.

Note:

ⓘ
Note that data migration will require additional time during the update process. The more data in the tables, the longer the migration will take. For example, migrating 100 million records will take approximately 12 minutes of additional time.

9. 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 2.0**.

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

10. Specify the path to temporarily place
This page has not yet been translated to English.

    events before uploading them to the Platform (by default, `/opt/factsldrtmdata`) and press **Enter**.
11. Wait for the
This page has not yet been translated to English.
update to complete. After the update, the installer will automatically delete image containers of previous versions.
12. Make sure that all services are running. To do this, run the command:

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

    The command will display the list of services. Each service should have the status `Running`.
13. For
This page has not yet been translated to English.
to work, you need to update the settings of the inotify subsystem in the OS.
To do this:
    a. Check if the `/ etc/sysctl.d/discovery.conf` configuration file with the following content is available:

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

    If the configuration file is available, skip the next two steps in the instructions.
    b. If the file was not created by the installer scripts earlier, create it and add the content from the previous step.
    c. To apply the new subsystem settings, run the following command:

    ```
    sysctl --load=/etc/sysctl.d/discovery.conf
    ```

14. 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.
15. If there are other products installed on the server, update them to versions that are compatible with
This page has not yet been translated to English.

    2.2 (see *Installation/Update Types, Compatibility with Other Products, Hardware and Software Requirements*).

16. If
    This page has not yet been translated to English.
    is installed in a distributed cluster, update the Platform and products on other servers to versions that are compatible with
    This page has not yet been translated to English.
    2.2.
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.

Note:

ⓘ
If in the cluster with

This page has not yet been translated to English.

2.2 installed the **Platform was updated to version 2.5**, then **restart** the `contentbroker` service to reconnect it to the database.

To do this:

1. On any
   This page has not yet been translated to English.
   node, run the restart command:

   ```
   kubectl -n infowatch rollout restart deployment/contentbroker-central
   ```

2. Check the service status with the command:

   ```
   kubectl -n infowatch rollout status deployment/contentbroker-central
   ```

10.6 Updating Data Discovery by Resetting the Installation

Important!

❗
To update a whole distributed Investigation Centre cluster by resetting the current installation, follow the steps:

1. **Reset** installation on **office nodes** with products in `office` mode.
2. **Reset** installation on **office nodes** with products in `central` mode.
3. **Reset** installation on the **central node**.
4. **Install** the **central** node.
5. **Install office** nodes with products in `central` mode.
6. **Install office** nodes with products in `office` mode.

When updating a cluster, reset installation only once for each node.

Updating by resetting the installation consists of the following steps:

1. Resetting the installation **with the new installer**. 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.

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 System update.

To update

This page has not yet been translated to English.

:

1. **Stop all scanning tasks** in the
   This page has not yet been translated to English.

   web interface.
2. Prepare the server for the update (see *Preparing the Server*).
3. Create a new directory on the disk (for example, `distr_discovery`):

   ```
   mkdir distr_discovery
   ```
4. Copy the
   This page has not yet been translated to English.

   `_2.2.X.xxx.tar.xz` archive to the created directory.
   Here, we are using version `2.2.0.191`, so the archive name is
   This page has not yet been translated to English.

   `_2.2.0.191.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_2.2.0.191.tar.xz
   ```
7. In case
   This page has not yet been translated to English.

   and
   This page has not yet been translated to English.

   are installed jointly or you are planning to use them jointly, stop
   This page has not yet been translated to English.

   data calculation for the time of
   This page has not yet been translated to English.

   update. For details, see Required Steps to Update Products that are Installed on Platform together with Prediction.
8. When you install the new version after the reset, assign the same labels to the cluster 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}"
```

9. In order to save settings for zones and servers in the new version, before resetting the installation, connect to the node where
This page has not yet been translated to English.
is installed in the `central` mode and stop the **Discoperator service** using the command:

```
kubectl scale --replicas=0 deployment discoperator-<node_label> -n infowatch
```

Example for Data Discovery in the central mode on the office node with the lv426 label:

```
kubectl scale --replicas=0 deployment discoperator-lv426 -n infowatch
```

10. Before resetting the installation, remember or save the paths to the current data storage directories. To get the list of directories, use the command:

```
cat /var/lib/iwplatform/data/volumes.txt
```

11. **Reset** the current installation using **the installer of the new version**:

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

Important!

If other Platform products are installed on the server, these products will be reset. When resetting the installation on the central node, products installed on office nodes will stop working.

After installing the new version of

This page has not yet been translated to English.

, reinstall the Platform products by specifying the directories with the existing data.

In case you have **already updated another product** on this server to a compatible version, **do not reset the Platform installation again** when updating

This page has not yet been translated to English.

, because the Platform is already of the required version.

If the product is installed **on the office node in the `central` mode**, **access to products will be reset** for the added user roles after resetting the installation.

12. Wait for the Platform and product reset process to complete.
13. If you are also upgrading to a different server or a new OS, copy the directories with the data that were specified during installation to another partition or to a new server.
Note:

In

This page has not yet been translated to English.

2.0 and later, the directories are located along the `/opt` path by default.
Make sure to preserve rights and owners when copying the directories. For copying, use standard tools, such as the `rsync` utility.

14. Make sure that the section with the `/var/lib/containerd` directory contains 40 GB or more of disk space.
    To check the volume of available disk space, use the command:

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

15. To free up disk space, you can delete the directory with container images of previous versions `/var/lib/containerd.`
    For this, run the command:

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

16. Reboot the server using the command:

    ```
    reboot
    ```

17. Install the new
    This page has not yet been translated to English.
    version (see *Installing Data Discovery*).
    Important!

    During the installation, specify the directories with the data of the previous version to store the data. When the System asks you if you want to clear up folders before the installation, select "`n`".

    If you are updating **from version 1.10 and earlier**, note that starting with version 2.0 the default installation paths are different. If you previously used the default paths, then during the installation of

    This page has not yet been translated to English.

    2.2 or later versions, the installer will not be able to find data from the previous version and will create directories along the `/opt` path. To avoid this, move the data to the `/opt` directory or specify the old directories when installing the new version.

    All nodes of the cluster with

    This page has not yet been translated to English.

    should contain the same path to the storage of scanned files (`/opt/disctps` by default).

18. If other products were installed on the server before the reset, install the product versions that are compatible with
    This page has not yet been translated to English.

    2.2 (see Installation/Update Types, Compatibility with Other Products, Hardware and Software Requirements).

19. If
    This page has not yet been translated to English.

is installed in a distributed cluster, update the Platform and products on the other servers to versions that are compatible with
This page has not yet been translated to English.

.

20. 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.
21. 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.

Important!

If

This page has not yet been translated to English.

is installed **on the office node in the `central` mode**, **access to products will be reset** for the added user roles as a result of the previous installation reset. After updating, go to **Settings** and reconfigure access to products for these roles (see
This page has not yet been translated to English.

. Administration Guide. Roles).

Note:

If in the cluster with

This page has not yet been translated to English.

2.2 installed the **Platform was updated to version 2.5**, then **restart** the `contentbroker` service to reconnect it to the database.

To do this:

1. On any
This page has not yet been translated to English.
node, run the restart command:

```
kubectl -n infowatch rollout restart deployment/contentbroker-central
```

2. Check the service status with the command:

```
kubectl -n infowatch rollout status deployment/contentbroker-central
```

10.7 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 integrations 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 2.1 (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_2.1.X.xxx.tar.xz`** to the created directory.
   Here, we are using version `2.1.0.152`, so the archive name is `iw_discovery_setup_2.1.0.152.tar.xz`.
5. Go to the directory, to which you copied the archive.
6. Unpack the archive with the distribution kit to this directory:

   ```
   tar -xvf iw_discovery_setup_2.1.0.152.tar.xz
   ```

7. Reset the current installation using the installer of the new version:

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

8. The Platform and product installation will be reset. Wait for the process to complete.
9. Make sure that the section with the `/var/lib/containerd` directory contains 40 GB or more of disk space.
   To check the volume of available disk space, use the command:

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

10. 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
    ```

11. Reboot the server using the command:

```
reboot
```

12. 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**».

    If you are updating **from version 1.10 and earlier**, please note that starting with version 2.0, default installation paths are different. If you previously used the default paths, then during the installation of Data Discovery 2.1 or later versions, the installer will not be able to find data from the previous version and will create directories along the `/opt` path. To avoid this, move the data to the `/opt` directory or specify the old directories when installing a new version.

    All nodes of the cluster with Data Discovery should contain the same path to the storage of scanned files (`/opt/disctps` by default).

13. 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?".
14. 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.

10.8 Direct Update of Content Analysis Module

In order to update Content Analysis Module:

1. **Stop all scanning tasks** in 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_tech`):

    ```
    mkdir distr_tech
    ```

4. Copy the `iw_tm_setup_7.12.0.xxx.tar.xz` archive to the created directory.
    Here, we are using version `7.12.0.94`, so the archive name is `iw_tm_setup_7.12.0.94.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_tm_setup_7.12.0.94.tar.xz
    ```

7. Run the updater:

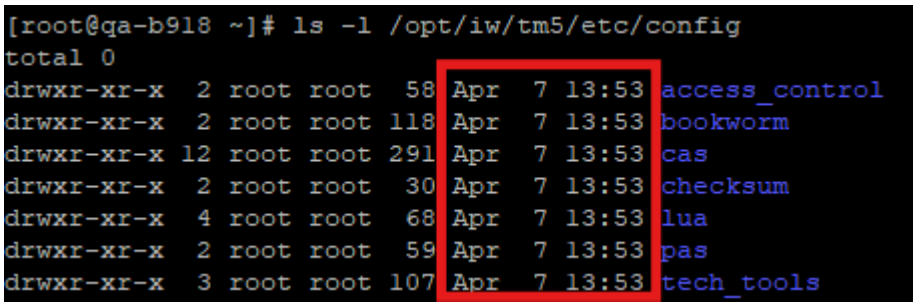
```
./setup.py update
```

8. Specify the path to temporarily place Traffic Monitor events before uploading them into the Platform (by default, `/opt/factsldrtmdata`) and press **Enter**.
9. Wait for the Data Discovery update to complete.
10. To ensure that `updater` service loads the latest version of Traffic Monitor configuration, we recommend removing the previous version with the command below:

```
rm -rf /opt/iw/tm5/tmp
rm -rf /opt/iw/tm5/etc/config
```

11. Some time later after the removal, `updater` service will load the latest Traffic Monitor configuration.
    To check the dates of creating or editing a configuration, run the command:

```
ls -l /opt/iw/tm5/etc/config
```



12. Once the module has been updated, you can restart previously stopped scanning tasks in Data Discovery web interface.

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, including internal passwords and related data. The Data Discovery data will be preserved. If necessary, you can delete the data manually from directories that were specified during the installation.

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 will not operate and will not be removed automatically. You need to remove them manually.

Note:

In case of distributed installation, if the product is installed on an office node and, no other products are installed on this node then, after the product removal on the node it is recommended to remove the platform elements too. For this, after running the command `./setup.py remove` run the command `./setup.py reset.`

In case the product is installed on a central node or there are other products on the office node, then is it strongly recommended not to run the command `./setup.py reset` after the product removal.