InfoWatch Data Access Tracker. Installation Guide

12/01/2026

© JSC “InfoWatch”

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

http://www.infowatch.com

Table of Contents

1 Who Should Read this Guide 4

2 Set of Documents 5

3 Technical support 6

4 Installation Types, Compatibility with Other Products, Hardware and Software Requirements 7

5 Preparing the Server 10

6 Installing Data Access Tracker 11

6.1 Installing DAT Interactively 12

6.2 Installing DAT with Command-Line Parameters 14

7 Troubleshooting 17

8 Configuring Network Access Rules 18

9 Updating Data Access Tracker 20

9.1 Updating DAT by Installation Reset 20

10 Uninstalling DAT 24

This guide contains information on how to install, update and remove InfoWatch Data Access Tracker (also referred to as DAT or the System). DAT software provides automatic audit results for directory service and mailbox access rights, as well as it enables you to track changes in access rights to filesystem objects.

1 Who Should Read this Guide

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

This guide is intended for users familiar with the basics of the Linux and Microsoft Windows operating systems.

2 Set of Documents

InfoWatch DAT documentation includes the following:

- "InfoWatch Data Access Tracker. Installation Guide". The document describes how to install, update and uninstall InfoWatch DAT.
- "InfoWatch Data Access Tracker. Administration Guide". The document contains information on how to configure and prepare InfoWatch DAT for operation.
- "InfoWatch Data Access Tracker. User Guide". The document describes how to work in InfoWatch DAT.

Related documentation for InfoWatch Traffic Monitor includes the following:

- "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, create policies for processing objects).
- "InfoWatch Traffic Monitor. Configuration Files Guide". Provides explanations for frequently used configuration files.

3 Technical support

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

- If you purchased the product from InfoWatch partner, please contact the technical support service of the partner
- If you purchased the product from InfoWatch directly, please contact InfoWatch technical support at support@infowatch.com.

Technical Support Service is available to assist you Mon-Fri, 7 AM – 9 PM (Moscow time, GMT+3), except weekends and public holidays in the Russian Federation. You can also visit technical support section on our website: http://infowatch.com/support.

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

InfoWatch DAT is a part of InfoWatch Investigation Centre.

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

- **Activity Monitor 3.2**
- **Data Access Tracker 2.2**
- **Data Discovery 2.0**
- **Prediction 3.2**
- **Vision 3.4**

Each product can be installed and work separately. However, using several products simultaneously provides the Security Officer with greater opportunities to ensure company information security.

The Investigation Centre products are installed on a base of Platform. The installer of each product contains both the Platform and product componets. You need to install both parts when deploying the products.

Both product components and the Platform support installation in the following two modes:

- `central`;
- `office`.

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

The Investigation Centre supports **distributed installation**: `central` and office `office` nodes of the Platform are combined into a cluster.

You can install components of the products both on the central and on the office node of the 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!

In case of distributed installation, please note that:

- All products in the cluster must be installed on the same Platform version. If you install a product on a newer Platform version, update all the other products in the cluster to ensure correct operation.
- In one cluster, you can deploy only one central node of the Platform.
- In one cluster, you can deploy a product in `central` mode only once. If the cluster already contains a product that has been installed in `central` mode, then another installation of this product in `central` mode within the same cluster will fail with an error.
- Data Access Tracker and Prediction can be installed on any Platform node but only in `central` mode.

Products installed in the same cluster have:

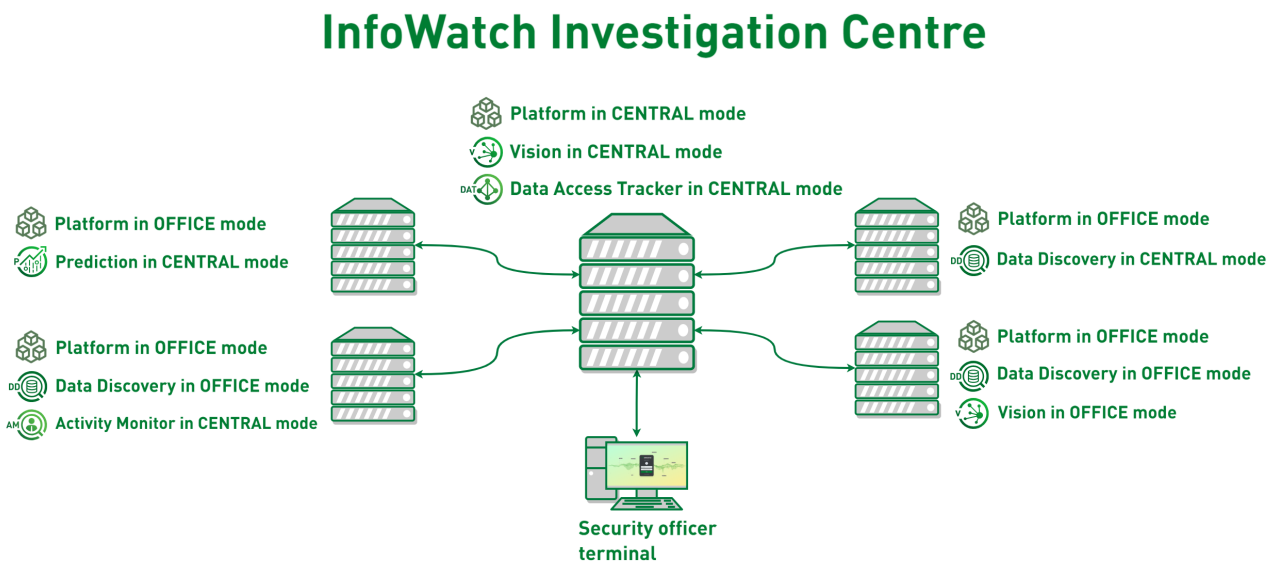
- Access to all functionality in the same management console;
- Common settings;
- A common role model;

- Shared access to data no matter which product was 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 the product in the `central` mode on the `office` Platform node, you should still use the `central` Platform node for work.

InfoWatch Investigation Centre products support **joint installation** on one server. You can install DAT jointly with any of Investigation Centre products.

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



Hardware requirements

Minimum requirements for the System installation:

- Number of processor cores: 4 (frequency – 3.1 GHz, bit depth – 64 bit, with support for SSE 4.2 instructions);
- RAM: 16 GB;
- Hard drive: 100 GB.

Software requirements

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

Software type	Options
Operating system of DAT server	• Red Hat Enterprise Linux: • versions 7.x (starting from 7.7) • versions 8.x • Oracle Linux: • version 7.9 • versions 8.x (starting from 8.4) **Important:** Make sure the **Netfilter** and **NAT** modules are loaded into the OS kernel.
Operating system of controller domain server	Windows Server 2012 R2 and later
Browser	• Google Chrome • Yandex.Browser **Important:** For correct operation, we recommend using the latest versions of supported browsers.

Important!

You must configure a controller domain and an MS Active Directory account. For details, see:

- Setting Up Domain Controller in Active Directory
- Configuring Active Directory Account

Make sure that for all Active Directory accounts the following fields are filled: `PasswordNeverExpires`, `Enabled`, `PasswordExpired`, `LockedOut`.

Примечание:

DAT uses PostgreSQL 16.4. The DBMS is distributed together with the product and does not require additional installation.

5 Preparing the Server

Before installing the product, follow the steps below to prepare DAT server.

Step to prepare the server:

1. The istaller is written in Python 2.7. Install the Python 2.7 interpreter.
2. Configure POD network rules or disable the firewall (for details, see the following KB articles: "Firewalld and Kubernetes interaction conflicts" and "Firewall complete shutdown").
3. Data Access Tracker 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).
4. If you are using antivirus, configure it to work together with the System (see the KB article: "Antivirus configuration for Platform products").
5. If the OS uses SELinux, install the `container-selinux` package. This package is required for DAT to work correctly together with SELinux.

> **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 Installing Data Access Tracker

The distribution kit is an archive named **`iw_dat_setup_2.2.0.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 DAT components without access to the Internet (offline installation);
- The installer.

To install the product, use the command line.

You can install DAT:

- On a separate server;
- On a server together with other products;
- In a cluster together with other products.

Before running the DAT installer:

1. Prepare the server for DAT installation. For details, see "Preparing the Server".
2. Create a new directory, e.g., `dat`, and navigate to it:

   ```
   mkdir /dat
   cd /dat
   ```

3. Copy the **`iw_dat_setup_2.2.0.xxx.tar.xz`** archive to the created directory. Here, we are installing version `2.2.0.064`, so the archive name is `iw_dat_setup_2.2.0.064.tar.xz`.
4. Unpack the archive with the distribution kit:

   ```
   tar -xvf iw_dat_setup_2.2.0.064.tar.xz
   ```

You can **run DAT installation**:

- **In interactive mode**, during which the installer will sequentially request installation parameters (for details, see "Installing DAT Interactively");
- **In silent mode**, where you can specify the installation parameters in the installer launch command (for details, see "Installing DAT with Command-Line Parameters").

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

Important!

When installing Data Access Tracker into a distributed Investigation Centre cluster, make sure that the Platform version is the same on each node. For the list of compatible versions, see "Installation Types, Compatibility with Other Products, Hardware and Software Requirements".

Important!

It is necessary that all nodes in a cluster are available for each other in the network. For that, 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>
```

6.1 Installing DAT Interactively

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

To install DAT:

1. Run the interactive installer:
   - **to install the product on the central Platform node:**

     ```
     ./setup.py install
     ```

   - **to install the product on the office Platform node:**

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

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

   > **Note:**
   >
   > If you reject the license agreement, the installer will abort the installation and exit.

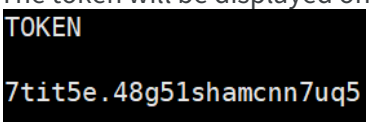
4. If you are installing the **central Platform node** (`--nodemode=central`), specify the IP address of the network interface and press **Enter**. The IP address should be in IPv4 format:
   " `xxx.xxx.xxx.xxx` " (by default, `0.0.0.0`).
   If you specify `0.0.0.0` , all available network interfaces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

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

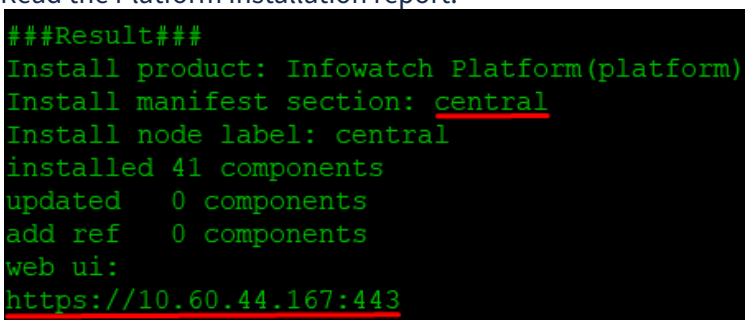
5. If you are installing **the office Platform node** (`--nodemode=office`):
   a. Enter the address of the central Platform node in IP address or domain name format (e.g., `192.0.2.0` or `host.example.com`).
   b. Specify the token to connect to the central Platform node.
   To get the token:
     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

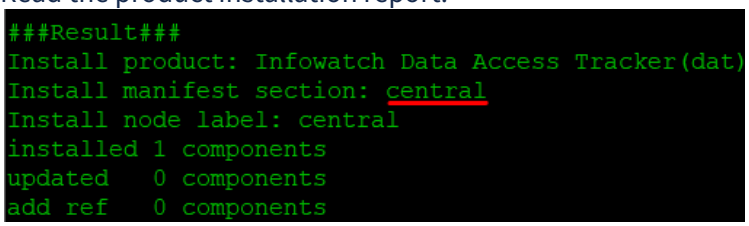
      

      Here the token is `7tit5e.48g51shamcnn7uq5` .
   c. Specify the node label (by default, `office`) and press **Enter**.
   The label may consist of letters of the Latin alphabet and/or numbers. The length of the label must not exceed 32 characters.
6. Allocate RAM (in gigabytes or percentage) to host ClickHouse data (by default, `80%`) and press **Enter**.
7. Specify the path to place ClickHouse data (by default, `/opt/chdata`) and press **Enter**.
8. Specify the path to place PostgreSQL data (by default, `/opt/pgdata`) and press **Enter**.
9. Specify the path to place NATS data (by default, `/opt/natsdata`) and press **Enter**.
10. Specify the path to store data (by default, `/opt/dsdata`) and press **Enter**.
11. If you are installing the **central Platform node**, specify the port for connecting to the web interface (by default, `443`) and press **Enter**.
12. Wait for the installation of the Platform to finish.
13. Read the Platform installation report:

    If you install the Platform, the **`web ui`** row contains the address and port for connecting to the web interface (here, `https://10.60.44.167:443`)
14. Wait for the installation of DAT to finish.

15. Read the product installation report:



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

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

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

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

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

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

6.2 Installing DAT with Command-Line Parameters

The DAT installer allows you to install the product with minimal user interaction. To do this, run the installation program and specify all the required parameters in the command line.

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 suggests interactively are specified.

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

Key	Default value	Available values	Description
`--nodemode`	`central`	`central`, `office`	The Platform installation mode
`--productmode`	`central`	`central`, `office`	The product installation mode **Note:** For DAT, only `central` mode is available.
`--loc`	`ru`	`ru`, `en`	Product localization, the language that is used for pre-installed entities. The parameter is **optional** to run the installer

Key	Default value	Available values	Description
`--licagree`	`n`	`yes`, `no`	Accepting the license agreement
`--chmemsize`	`80%`	1-100% or a numeric value If you do not specify %, then the specified value will be treated as the volume in GB	Amount of RAM used for ClickHouse data
`--chdbpath`	`/opt/chdata`		Path for placing ClickHouse data
`--natspath`	`/opt/natsdata`		Path for placing NATS data
`--pgdbpath`	`/opt/pgdata`		Path for placing PostgreSQL database data
`--dsdatapath`	`/opt/dsdata`		Path for placing binary data
`--advertise`	`0.0.0.0`		IP address of the network interface on which the `kubelet` service is running. Specify the value when installing the Platform central node
`--guiport`	`443`		Web interface connection port. Specify the value when installing the Platform central node
`--cluster`			Address of the Platform central node in the cluster. Specify the value when installing the Platform office node
`--clustertoken`			The token to connect to the Platform central node. To get the token, in the Platform central node terminal, run the command: `kubeadm token list`

Key	Default value	Available values	Description
			Specify the value when installing the Platform office node
`--nodelabel`	`office`		The node label. Specify the value when installing the Platform office node

To install DAT:

1. Run the DAT installer specifying the parameters.

   - **Example command to install the central Platform and DAT 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 --guiport=443 --natspath=/opt/natsdata
     ```

   - **Example command to install the branch Platform and DAT in the central mode:**

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

   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.
2. Wait for the installation of the Platform to finish. Read the Platform installation report. The `web ui` row contains the address and port for connecting to the web interface.
3. Wait for the DAT installation to complete. Read the product installation report.
4. To display information about the Platform and products in the cluster, run the command:

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

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

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

   The command will display the list of services. Each service should have the `Running` status.
6. To start using the product, connect to the Investigation Centre web interface. To do this, enter the central Platform node address and port in your browser.

7 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.

To reset the System installation, go to the directory with the unpacked distribution kit of the product and run the following command:

```
/setup.py reset
```

Important!

After the reset, all data is saved in the System. When reinstalling DAT, you will be prompted to delete the existing data. Choose **no**.

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 DAT, you should reinstall other products in the cluster.

8 Configuring Network Access Rules

For correct operation of DAT, make sure that the following connections are allowed:

Connection	Port	Description
Access to the web interface and SSH console		
Administrator's workstation → DAT Server	TCP 22	Used for managing DAT Server via the SSH protocol
Security Officer workstation → Investigation centre	TCP 443	Port for connection to the Investigation centre web interface (the Platform central node). The default value is **`443`**. You can specify the value during the Platform installation.
Connections to external systems		
DAT server → Domain controller	TCP 5985	Used for secure HTTP connection with NTLM authentication
DAT server → Domain controller	TCP 5986	Used for HTTPS connection
DAT server → SMTP server	TCP 25	Used for sending email notifications
Integration with MS Exchange server		
Domain controller → MS Exchange server	TCP 5985	Used for synchronization between the product and the mail server.
Domain controller → MS Exchange server	TCP 80	
Work in the cluster		
Platform server in the `office` mode → Platform server in the `central` mode	TCP 6443 TCP 2379, 2380 TCP 10251, 10252, 10255	Ports of the Platform server 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	Ports of the Platform server in the `office` mode

Connection	Port	Description
		Used for communication between Platform in the `central` mode and 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

9 Updating Data Access Tracker

The distribution kit is an archive named `iw_dat_setup_2.2.0.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 Vision components without access to the Internet (offline installation). The archive also contains the updater.

To update DAT, use the command line.

You can update DAT 2.2 only by installation reset.

In order to **update a distributed Investigation Centre cluster**:

1. **Update the central node** and all products installed on it.
2. **Update office nodes** and all products installed on them.

Important!

In case you are updating DAT in the cluster together with other InfoWatch products, then make sure that the Platform version is the same in all the products on all nodes. For the list of compatible versions, see "Installation Types, Compatibility with Other Products, Hardware and Software Requirements".

Important!

During the update, the System is unavailable in the entire cluster. In case products were installed in different clusters before the update, joining them into a single cluster after the update is not supported.

In case automatic synchronization with directory and/or mail service is configured, then after updating you need to configure the syncronization again.

In case DAT is the only product installed and the integration with Traffic Monitor is configured, then after updating you need to remove the integration, create a new one and configure it to use the new functionality of the InfoWatch Investigation Centre in **Events** and **Analytics > Violation statistics** sections.

9.1 Updating DAT by Installation Reset

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 consists of the following steps:

1. Resetting the installation. Resetting the installation does not delete the System data.

2. Installing new versions of the Platform and product and specifying already existing folders with data.

> **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 started processes will not be interrupted and you may safely continue the System update.

To update Data Access Tracker:

1. Follow the steps to prepare the server for the update (see "Preparing the Server").
2. Create a new directory on the disk, for example, `dat_2.2`, and navigate to it.

```
mkdir /dat_2.2
cd /dat_2.2
```

3. Copy **`iw_dat_setup_2.2.0.xxx.tar.xz`** archive to the directory you have created. Here, we are using version `2.2.0.064`, so the archive name is `iw_dat_setup_2.2.0.064.tar.xz`.
4. Unpack the archive with the distribution kit:

```
tar -xvf iw_dat_setup_2.2.0.064.tar.xz
```

5. In case of joint installation of DAT and Prediction, stop Prediction data calculation for the duration of DAT update, see "Required Steps to Update Products that are Installed on Platform together with Prediction" article in the Knowledge Base for details.
6. Reset the current installation:

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

> **Important!**
>
> In case you have already updated another product on this server to a compatible version, do not reset Platform installation again when updating Prediction, because the Platform is already of the required version.
>
> If there are other Platform-based products installed on the server, installation of these products will be reset. Products in `office` mode connected to the products in `central` mode will stop working.
>
> After installing the new Vision version, reinstall the Platform products and specify directories with existing data.
>
> If DAT is installed on `office` Platform node, access to products will be reset for the added user roles after resetting the installation.

7. Wait for the Platform and product installation reset process to complete.

8. Reboot the server:

```
reboot
```

9. In case you are also upgrading to a different server or a new OS:
   a. Copy directories with the data that were specified during installation and paste them to another partition or to a new server.

> **Note:**
>
> By default, the directories are located:
>
> - Starting with version 2.2 – along the `/opt` path;
> - In earlier versions – along the `/mnt` path.
>
> Be sure to preserve rights and owners when copying the directories. For copying, use standard tools, such as the **`rsync`** utility.

   b. After resetting the current installation, copy `/var/lib/iwplatform/` **`dbadmin.yaml`** file with the database passwords from the old server to the new one.
10. To free up some space on your disk, delete `/var/lib/` **`containerd`** directory with container images of previous versions. Use the command:

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

11. Go to the distribution kit directory:

```
cd /dat_2.2
```

12. Install the new version of DAT (see "Installing DAT Interactively" or "Installing DAT with Command-Line Parameters").

> **Important!**
>
> - In case Activity Monitor was installed on the server before the reset, install it first, then install DAT.
> - During the installation, specify directories with data of the previous version.
> - In case you are updating DAT from version 2.1 and earlier, keep in mind that default installation paths has been changed in version 2.2. If you previously used the default path (`/mnt`), then during the installation of DAT 2.2 or later versions, by default the installer will not be able to find data from the previous version and will create directories along `/opt` path. To avoid this, move the data (`chdata` , `natsdata` , `pgdata` , `dsdata` folders) to `/opt` directory or specify the old directories when installing the new version.
> - When the System asks you if you want to delete the existing folders, select " **`n`** ".

13. Clear the cache of the browser you were using before updating the product. The Investigation Centre web interface is available at the `central` Platform node address.

Important!

If DAT is installed on `office` Platform node, access to products will be reset for the added user roles after resetting the installation. After the update is complete, go to **Settings** and reconfigure access to products for these roles. For details, see "*InfoWatch Data Access Tracker. Administration Guide*", "Roles" article.

10 Uninstalling DAT

To uninstall DAT:

1. Open the directory on the server, to which you unpacked the distribution archive during DAT installation.
2. Run the command:

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

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

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