# Red Hat Insights 2020-04

## Client Configuration Guide for Red Hat Insights

Configuration options and use cases for the Insights client

Last Updated: 2020-09-02

# Red Hat Insights 2020-04 Client Configuration Guide for Red Hat Insights

Configuration options and use cases for the Insights client

## Legal Notice



## Abstract

This guide is for Red Hat Insights users who want to configure Insights client features. The Insights client configuration settings on your system affect the interaction with Red Hat Insights. Providing Feedback: If you have a suggestion to improve this documentation, or find an error, submit a Bugzilla report at http://bugzilla.redhat.com. Select the Cloud Software Services (cloud.redhat.com) product and use the Documentation component.

# Table of Contents

# CHAPTER 1. RED HAT INSIGHTS CLIENT CONFIGURATION OVERVIEW

This guide provides information about configuring the Red Hat Insights client on your system. With the **insights-client** command and associated configuration files, you can control how your system interacts with Red Hat Insights.

- General information and overviews of the Insights client features are covered in the first few chapters.
- How-to information on using the Insights client commands and configuration files to accomplish specific tasks follows the overview information.
- Command reference and configuration file reference information is at the end of this guide.

Navigation links help you quickly find what you are looking for.

## 1.1. CLIENT CONFIGURATION OVERVIEW

The Red Hat Insights client collects information about your system and sends it to Red Hat Insights, which is a cloud application. Command options for the CLI and configuration file options modify the information that is collected and shared with Red Hat Insights. These options control the following:

- Data obfuscation
  - IP address obfuscation

    **NOTE**

    IP address obfuscation is supported only for IPv4 addresses.

  - Host name obfuscation
- Data redaction
  - Specific files
  - Output of specific commands
  - Pattern-match deletions
  - Keyword replacement
- Insights client scheduling
- Insights rule updates
- Insights client authentication method
  - Certificate-based
  - SSO-based, or Basic
- System tagging

Because the information collected by the Red Hat Insights client is saved in a **tar** file, that file is referred to as an **archive file**.

## 1.2. INSIGHTS CLIENT CLI AND CONFIGURATION FILE INTERACTIONS

The Red Hat Insights client runs according to its scheduler, which by default is every 24 hours. The client also runs when you enter the **insights-client** command.

When the client runs, its behavior is controlled, in order, by the following:

1. The values, if any, provided when you enter the **insights-client** command. Values entered in the CLI override configuration file settings and system environment settings for that execution of the Insights client.
2. The settings in the configuration files (**/etc/insights-client/insights-client.conf** and **/etc/insights-client/remove.conf**) override system environment settings.
3. The values of any system environment variables (**printenv**) not affected by the CLI or the client configuration files are used.

Any options you provide in the **insights-client** command are used only for that execution. Those values can temporarily override values set in the configuration file or the environment variables.

NOTE

Using the **insights-client** command to set the display name takes effect immediately but does not run the Insights client.

NOTE

If you are using RHEL 6.9 or earlier, the client command is **redhat-access-insights**.

## 1.3. INSIGHTS CLIENT DISTRIBUTION

Insights client is available on Red Hat Enterprise Linux (RHEL) as shown in the following table.

| RHEL release | Comments |
|---|---|
| RHEL 8 | Distributed with Insights client pre-installed. |
| RHEL 7 | Distributed with the Insights client RPM package loaded but not installed. |
| RHEL 6.10 and later | You must download the Insights client RPM package and install it. |

**Additional resources**

- Getting Started with Red Hat Insights

# CHAPTER 2. CONFIGURING RED HAT INSIGHTS CLIENT

The procedures in this section show you how to configure the Red Hat Insights client on your system.

**Prerequisites**

- You have root permissions or their equivalent. Making changes to configuration files or adding configuration files requires root permissions.
- The Red Hat Insights client is deployed on your system.

## 2.1. REGISTERING YOUR SYSTEM WITH RED HAT INSIGHTS

You must register your system with Red Hat Insights before you can use its services. Optionally, you can assign a display name for your host when you register your system.

**NOTE**

If you do not assign a display name when you register the system, Red Hat Insights uses the value in **/etc/hostname**.

**Prerequisites**

- Red Hat Insights client is deployed on your system.
  Deploying Red Hat Insights on existing RHEL systems managed by Red Hat Cloud Access

  Deploying Red Hat Insights on existing RHEL systems managed by Red Hat Update Infrastructure
- You can access the cloud-based Red Hat Insights services.
  Configuring Basic Authentication for Red Hat Insights

**Procedure**

1. Enter the **insights-client** command with the **--register** option.

```
[root@insights]# insights-client --register
```

2. Optionally, enter the **insights-client** command with the **--register** option and the **--display-name** option to specify the name you want to appear in the GUI.

```
[root@insights]# insights-client --register --display-name ITC-4
System display name changed from None to ITC-4
```

**Verification steps**

- Enter the **insights-client** command with the **--status** option.

```
[root@insights]# insights-client --status
System is registered locally via .registered file. Registered at 2019-08-20T12:56:48.356814
Insights API confirms registration.
```

## 2.2. CHANGING THE HOST DISPLAY NAME

You can change the host display name as it appears in the GUI. Make this change either when you register the system with Red Hat Insights, or after registration. If you do not assign a display name when you register the system, Red Hat Insights uses the value in **/etc/hostname**.

NOTE

If you obfuscate the host name, the **hostname** configured in **/etc/hostname** is obfuscated. Assign a **display name** so that you can identify hosts even when their **hostname** is obfuscated.

### Prerequisites

This procedure is optional. Determine if you want to use a display name in addition to the default **hostname**.

### Procedure

1. Enter the **insights-client** command with the **--display-name** option and specify a display name.

```
[root@insights]# insights-client --display-name ITC-4
System display name changed from None to ITC-4
```

2. To create a display name that contains spaces, use double quotes.

```
[root@insights]# insights-client --display-name "ITC-4 B9 4th floor"
System display name changed from None to ITC-4 B9 4th floor
```

### Additional resources

- Section 3.5, “Obfuscating the hostname”
- Section 2.1, “Registering your system with Red Hat Insights”

## 2.3. DISPLAYING THE CLIENT VERSION

You can display the client version and client core version.

### Procedure

- Enter the **insights-client** command with the **--version** option.

```
[root@insights]# insights-client --version
Client: 3.0.6-0
Core: 3.0.121-1
```

### Additional resources

These links provide client changelog information:

- Red Hat Insights Client Core Changelog
- Changelog file

# CHAPTER 3. RED HAT INSIGHTS CLIENT DATA OBFUSCATION

The Red Hat Insights client provides IP address obfuscation and host name obfuscation. The obfuscation is controlled by settings in the **/etc/insights-client/insights-client.conf** configuration file.

In the configuration file you select whether or not to enable obfuscation. You can choose IP address obfuscation and add host name obfuscation. You cannot select only host name obfuscation.

Obfuscation works by using a Python SoS process that replaces the host name and IP address with preset values when it processes the Insights client archive. The processed archive file is sent to Red Hat Insights.

You cannot choose the obfuscation replacement values.

## 3.1. IPV4 ADDRESS OBFUSCATION

When you choose IP address obfuscation, your host address in the archive file is changed to the value that is provided in the Python SoS file. The value provided for obfuscation is not configurable. You cannot mask or select which portion of the IPv4 host IP address to obfuscate.

Consider the following example that shows the original host IP address compared to how it appears when obfuscated:

- Original host IP address

  ```
  192.168.0.24
  ```

- Obfuscated host IP address as it appears in Red Hat Insights

  ```
  10.230.230.1
  ```

If you choose IP address obfuscation on another system, its IP address in the archive file is changed to the same obfuscated value, **10.230.230.1**. In the Red Hat Insights GUI, you might see multiple systems with the same IP address as a result of obfuscation.

NOTE

IP address obfuscation is supported only for IPv4 addresses.

## 3.2. HOST NAME OBFUSCATION

When you choose host name obfuscation, your **/etc/hostname** value in the archive file is changed to the value that is provided in the Python SoS file. The obfuscated host name is displayed in Red Hat Insights. Consider the following example:

- Original **/etc/hostname**

  ```
  RTP.data.center.01
  ```

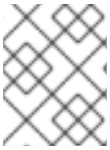
- Obfuscated **/etc/hostname** as it appears in Red Hat Insights

  ```
  host0
  ```

In order to use host name obfuscation, you must also enable IP address obfuscation.

NOTE

If you configure host name obfuscation on another system, its name uses the same obfuscation values. In the Red Hat Insights GUI, you might see multiple systems with the same **hostname** as a result of obfuscation.



NOTE

You can assign a display name to your system that is not obfuscated and will appear in Red Hat Insights. Only the **/etc/hostname** is obfuscated.

**Additional resources**

- Section 3.4, "Obfuscating the IPv4 address"
- Section 3.5, "Obfuscating the hostname"
- Section 2.2, "Changing the host display name"
- Python SoS Workflow System

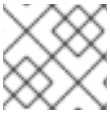
## 3.3. CONFIGURING RED HAT INSIGHTS CLIENT OBFUSCATION

The following procedures show how to configure obfuscation options in the Red Hat Insights client.

- Section 3.4, "Obfuscating the IPv4 address"
- Section 3.5, "Obfuscating the hostname"

## 3.4. OBFUSCATING THE IPV4 ADDRESS

You can obfuscate the IPv4 host address in the archive file before it is sent to Red Hat Insights.



NOTE

You must obfuscate the IP address if you want to obfuscate the host name.

**Procedure**

1. Open the **/etc/insights-client/insights-client.conf** file with an editor.
2. Locate the line that contains

```
#obfuscate=False
```

3. Remove the **#** and change **False** to **True**.

```
obfuscate=True
```

4. Save and close the the **/etc/insights-client/insights-client.conf** file.

## 3.5. OBFUSCATING THE HOSTNAME

You can obfuscate the host name in the archive file before it is sent to Red Hat Insights. The **hostname** in **/etc/hostname** changes to **host0** if you have a single host name assigned to your system. Additional host names change to **host1**, **host2**, up to the number of host names you configured for your system.

### Prerequisites

- Section 3.4, "Obfuscating the IPv4 address"

### Procedure

1. Open the **/etc/insights-client/insights-client.conf** file with an editor.
2. Locate the line that contains **obfuscate_hostname**.

```
#obfuscate_hostname=False
```

3. Remove the **#** and change **False** to **True**.

```
obfuscate_hostname=True
```

4. Save and close the the **/etc/insights-client/insights-client.conf** file.
5. (Optional) Use the **insights-client** command with the **--display-name** option to assign a display name for your system. The display name is not obfuscated.

```
[root@insights]# insights-client --display-name ITC-4
```

# CHAPTER 4. RED HAT INSIGHTS CLIENT DATA REDACTION

The Red Hat Insights client provides data redaction options. Depending on your version of RHEL, there are two methods for controlling data redaction.

**Table 4.1. Data redaction and RHEL versions**

| RHEL Version | Redaction method |
|---|---|
| RHEL 6.9, 7.8, 8.2, and earlier | Configuration file<br>**remove.conf** |
| RHEL RHEL 6.10, 7.9, 8.3 and later | YAM files<br>**file-redaction.yaml**<br>**file-content-redaction.yaml** |

You must create the **remove.conf** configuration file or YAML files. They are not installed by default.

**Additional resources**

- Section 4.1, "Configuring Red Hat Insights client redaction"

## 4.1. CONFIGURING RED HAT INSIGHTS CLIENT REDACTION

The Red Hat Insights client provides data redaction options. Depending on your version of RHEL, there are two methods for controlling data redaction.

- RHEL 6.9, 7.8, 8.2, and earlier
  Section 4.3, "Configuring Red Hat Insights client redaction using **remove.conf**"
- RHEL 6.10, 7.9, 8.3 and later
  Section 4.5, "Configuring Red Hat Insights client redaction using YAML files"

## 4.2. REDACTION AND REMOVE.CONF FILE USE

When you use a configuration file, redaction is controlled by the contents of **/etc/insights-client/remove.conf**. You can optionally configure the Insights client to use a different redaction configuration file.

Based on your entries in the redaction configuration file, you can specify one or more of the following actions:

- Eliminate specific files and their content from data collecting
- Eliminate selected command output from data collecting
- Eliminate information that matches a pattern
- Substitute specific strings with a default **keyword** string

When you configure redaction by elimination, the redacted information is never recorded in the archive file. Redaction is performed by preprocessing the data before it is captured in the archive file.

For redaction by string substitution, the archive file is processed by a Python SoS process before it is sent to Red Hat Insights.

**NOTE**

Regular expression matching is not supported by the **remove.conf** file.

You can use command line options to control the archive file output. For example, you can generate the archive file but not send it to Red Hat Insights. You can inspect and verify the redaction results before the archive is sent .

**NOTE**

When you redact files and command output, that information is not available to compare against the Insights rules. These omissions might cause Insights not to identify issues that apply to your system.

### Additional resources

- Section 4.1, "Configuring Red Hat Insights client redaction"

## 4.3. CONFIGURING RED HAT INSIGHTS CLIENT REDACTION USING REMOVE.CONF

The **/etc/insights-client/remove.conf** file controls redaction. You must create this file before you can use Insights client redaction.

### Procedure

1. Use an editor to create the **/etc/insights-client/remove.conf** file template.

```
[remove]
files=/etc/cluster/cluster.conf,/etc/hosts
commands=/bin/dmesg,/bin/hostname
patterns=password,username
keywords=super$ecret,ultra$ecret+
```

2. Optionally, delete any lines that you do not want to apply to archive redaction.

3. Make sure the **remove.conf** file permissions are set for **root** owner only.

```
[root@insights]# ll remove.conf
-rw-------. 1 root root 145 Sep 25 17:39 remove.conf
```

4. Refer to the additional resources for procedures on how to apply each available redaction option.

### Additional resources

- Section 4.3.1, "Redacting specific file content"
- Section 4.3.2, "Redacting specific commands"

- Section 4.3.3, “Redacting string patterns”
- Section 4.3.4, “Redacting keywords”
- Section 4.3.5, “Validating the **remove.conf** file”

### 4.3.1. Redacting specific file content

You can select specific files that are redacted by using the **remove.conf** file. The files you select and their content are not included in the archive file.

#### Prerequisites

- You must create a **/etc/insights-client/remove.conf** file.
  Section 4.1, “Configuring Red Hat Insights client redaction”

#### Procedure

1. Use an editor and open the **/etc/insights-client/remove.conf** file.

```
[remove]
files=/etc/cluster/cluster.conf,/etc/hosts
commands=/bin/dmesg,/bin/hostname
patterns=password,username
keywords=super$ecret,ultra$ecret+
```

2. On the **files=** line, add or remove the files that you want to redact from the archive file.

NOTE

Each file name is separated by a single comma. Do not use spaces.

3. To redact no files from the Insights client archive, remove the **files=** line.
4. Save and close the file.

### 4.3.2. Redacting specific commands

You can select specific commands that are redacted by using the **remove.conf** file. The output of these commands is not included in the archive file.

#### Prerequisites

- You must create a **/etc/insights-client/remove.conf** file.
  Section 4.1, “Configuring Red Hat Insights client redaction”

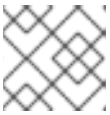
#### Procedure

1. Use an editor and open the **/etc/insights-client/remove.conf** file.

```
[remove]
files=/etc/cluster/cluster.conf,/etc/hosts
commands=/bin/dmesg,/bin/hostname
```

```
patterns=password,username
keywords=super$ecret,ultra$ecret+
```

2. On the **commands=** line, add or remove the commands that you want to redact from the archive file.



NOTE

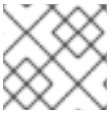
Each command name is separated by a single comma. Do not use spaces.

3. To redact no command from the Insights client archive, remove the **command=** line.

4. Save and close the file.

### 4.3.3. Redacting string patterns

You can select specific string patterns that are redacted by using the **remove.conf** file. The string pattern that you specify is redacted from the archive file by removing the entire line. For example, if the string pattern is **name**, that pattern matches and redacts **hostname**, **filename**, **username**.



NOTE

Regular expressions and wildcard matching (**egrep**) are not supported.

**Prerequisites**

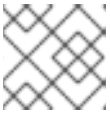
- You must create a **/etc/insights-client/remove.conf** file.
  Section 4.1, “Configuring Red Hat Insights client redaction”

**Procedure**

1. Use an editor and open the **/etc/insights-client/remove.conf** file.

```
[remove]
files=/etc/cluster/cluster.conf,/etc/hosts
commands=/bin/dmesg,/bin/hostname
patterns=password,username
keywords=super$ecret,ultra$ecret+
```

2. On the **patterns=** line, add any string patterns that you want to redact from the archive file.



NOTE

Each pattern is separated by a single comma. Do not use spaces.

3. To redact no patterns from the Insights client archive, remove the **patterns=** line.

4. Save and close the file.

### 4.3.4. Redacting keywords

You can select specific keywords that are redacted by using the **remove.conf** file. The keywords you specify are replaced with **keyword0**, **keyword1**, **keyword2**, etc., in the archive file.

**Prerequisites**

- You must create a **/etc/insights-client/remove.conf** file.
  Section 4.1, "Configuring Red Hat Insights client redaction"

**Procedure**

1. Use an editor and open the **/etc/insights-client/remove.conf** file.

```
[remove]
files=/etc/cluster/cluster.conf,/etc/hosts
commands=/bin/dmesg,/bin/hostname
patterns=password,username
keywords=super$ecret,ultra$ecret+
```

2. On the **keywords=** line, add any keywords that you want to redact from the archive file.

NOTE

Each keyword is separated by a single comma. Do not use spaces.

3. To redact no keywords from the Insights client archive, remove the **keyword=** line.

4. Save and close the file.

### 4.3.5. Validating the remove.conf file

You can validate the **remove.conf** file to make sure its syntax is correct before using it for redaction.

**Prerequisites**

- You must create a **/etc/insights-client/remove.conf** file.
  Section 4.1, "Configuring Red Hat Insights client redaction"

**Procedure**

1. Enter the **insights-client** command with the **--validate** option.

```
[root@insights]# insights-client --validate
```

2. Correct any errors that the command displays.

## 4.4. REDACTION AND YAML FILE USE

When you use YAML files for redaction, two files control the redaction actions. You can use one or both files, depending on the content you want to redact. The specified content is redacted before it is captured in the archive file.

**Table 4.2. Redaction and YAML files**

| YAML file | Description |
|---|---|
| **/etc/insights-client/file-redaction.yaml** | This file lists commands and files that you want redacted. The output of the listed commands or files is readacted. |
| **/etc/insights-client/file-content-redaction.yaml** | This file defines pattern redaction and keyword replacement. Pattern redaction is done by pattern match or regular expression match. Keyword replacement is done by a Python SoS process that replaces the keyword with a generic identifier. |

**Additional resources**

- Section 4.5, "Configuring Red Hat Insights client redaction using YAML files"

## 4.5. CONFIGURING RED HAT INSIGHTS CLIENT REDACTION USING YAML FILES

Two YAML files control Insights client redaction. You must create each YAML file before you can use redaction in RHEL 6.10, 7.9, 8.3 and later.

- Section 4.5.1, "Configuring YAML command and file redaction"
- Section 4.5.2, "Configuring YAML pattern and keyword redaction"

### 4.5.1. Configuring YAML command and file redaction

The **/etc/insights-client/file-redaction.yaml** file is a YAML file. It lists the commands and system files that you want redacted. The output of the listed commands or files is not included in the uploaded archive file.

If you want to redact based on keyword replacement or pattern matching, see Section 4.5.2, "Configuring YAML pattern and keyword redaction".

**Prerequisites**

- You must be familiar with the basics of YAML syntax. Explaining YAML is beyond the scope of this procedure.
- You must have **root** permission or its equivalent to create files in **/etc/insights-client/**

**Procedure**

1. Use an editor to create the **/etc/insights-client/file-redaction.yaml** file.

   **Example**

   ```
   # file-redaction.yaml
   ---
   # Exclude the entire output of commands
   #   Specify the full command path or the symbolic name in .cache.json
   ```

```
 commands:
- /bin/rpm -qa
- /bin/ls
- ethtool_i

# Exclude the entire output of files
#  Specify the full filename path or the symbolic name in .cache.json

files:
- /etc/audit/auditd.conf
- cluster_conf
```

2. Make sure the **file-redaction.yaml** file permissions are set for **root** owner only.

```
[root@insights]# ll file-redaction.yaml
-rw-------. 1 root root 145 Sep 25 17:39 file-redaction.yaml
```

### Additional resources

Section 4.6, “Verifying the Insights client archive”

## 4.5.2. Configuring YAML pattern and keyword redaction

The **/etc/insights-client/file-content-redaction.yaml** file is a YAML file that defines redaction based on pattern redaction and keyword replacement. Pattern redaction is done by pattern match or regular expression match. Keyword replacement is done by a Python SoS process that replaces the keyword with a generic identifier.

If you want to redact based on command output or specific files, see Section 4.5.1, “Configuring YAML command and file redaction”.

### Prerequisites

- You must be familiar with the basics of YAML syntax. Explaining YAML is beyond the scope of this procedure.
- You must have **root** permission or its equivalent to create files in **/etc/insights-client/**

### Procedure

1. Use an editor to create the **/etc/insights-client/file-content-redaction.yaml** file.

#### Example

```
# file-content-redaction.yaml
---
# Pattern redaction per matching line
#  Lines that match a pattern are excluded from files and command output.
#  Patterns are processed in the order that they are listed.
# Example

patterns:
 - "a_string_1"
 - "a_string_2"
```

```
# Regular expression pattern redaction per line
#  Patterns with regular expressions (regex) are wrapped with "regex:"
# Example

patterns:
 regex:
 - "abc.*def"
 - "localhost[[:digit:]]"


# Keyword replacement redaction
#  Replace keywords in files and command output with generic identifiers
#  Keyword does not support regex
# Example

keywords:keywords:
- "1.1.1.1"
- "My Name"
- "a_name"
```

2. Make sure the **file-content-redaction.yaml** file permissions are set for **root** owner only.

```
[root@insights]# ll file-content-redaction.yaml
-rw-------. 1 root root 145 Sep 25 17:39 file-content-redaction.yaml
```

### Additional resources

Section 4.6, “Verifying the Insights client archive”

## 4.6. VERIFYING THE INSIGHTS CLIENT ARCHIVE

You can verify the contents of the archive file. By inspecting the archive file, you can confirm what data is sent to Red Hat Insights.

- If you use obfuscation or redaction, you can inspect the archive before it is sent.
  Section 4.6.1, “Verifying the archive before upload”
- If you want to preserve the archive file, you can keep it on your system.
  Section 4.6.2, “Verifying the Insights client archive after upload”

### 4.6.1. Verifying the archive before upload

You can inspect the archive before it is sent to Red Hat Insights by running the client and saving the file without uploading it. This allows you to view what information the client sends to Insights, and to verify obfuscation or redaction settings.

The archive is stored in the **/var/tmp/** directory. The file name is displayed when **insights-client** completes.

#### Prerequisites

- If you use redaction, make sure the **/etc/insights-client/remove.conf** file is properly set up.
  Section 4.3.5, “Validating the **remove.conf** file”

- If you use obfuscation, make sure the **/etc/insights-client/insights-client.conf** file is properly set up.
  Section 3.3, "Configuring Red Hat Insights client obfuscation"

**Procedure**

1. Enter the **insights-client** command with the **--no-upload** option.

```
[root@insights]# insights-client --no-upload
```

   The command displays informational messages when redaction or obfuscation is applied.

```
WARNING: Excluding data from files
Starting to collect Insights data for ITC-4
WARNING: Skipping patterns found in remove.conf
WARNING: Skipping command /bin/dmesg
WARNING: Skipping command /bin/hostname
WARNING: Skipping file /etc/cluster/cluster.conf
WARNING: Skipping file /etc/hosts
Archive saved at /var/tmp/qsINM9/insights-ITC-4-20190925180232.tar.gz
```

2. Navigate to the temporary storage directory as shown in the **Archive saved at** message.

```
[root@insights]# cd /var/tmp/qsINM9/
```

3. Unpack the compressed **tar.gz** file.

```
[root@insights]# tar -xzf insights-ITC-4-20190925180232.tar.gz
```

   The result will be a new directory containing the files.

### 4.6.2. Verifying the Insights client archive after upload

You can keep the archive for inspection after it is sent to Red Hat Insights by running the client and saving the file. This allows you to verify what information the client sends Insights, and to verify obfuscation or redaction settings.

**Prerequisites**

- If you use redaction, make sure the **/etc/insights-client/remove.conf** file is properly set up.
  Section 4.3.5, "Validating the **remove.conf** file"
- If you use obfuscation, make sure the **/etc/insights-client/insights-client.conf** file is properly set up.
  Section 3.3, "Configuring Red Hat Insights client obfuscation"

**Procedure**

1. Enter the **insights-client** command with the **--keep-archive** option.

```
[root@insights]# insights-client --keep-archive
```

   The command displays informational messages.

```
Starting to collect Insights data for ITC-4
Uploading Insights data.
Successfully uploaded report from ITC-4 to account 6229994.
Insights archive retained in /var/tmp/ozM8bY/insights-ITC-4-20190925181622.tar.gz
```

2. Navigate to the temporary storage directory as shown in the **Insights archive retained in** message.

```
[root@insights]# cd /var/tmp/ozM8bY/
```

3. Unpack the compressed **tar.gz** file.

```
[root@insights]# tar -xzf insights-ITC-4-20190925181622.tar.gz
```

The result will be a new directory containing the files.

# CHAPTER 5. RED HAT INSIGHTS TAGGING OVERVIEW

You can add descriptive tags to systems managed by Red Hat Insights, allowing you to add contextual markers to individual systems then filter by those tags in the Insights application to find unique or related systems. This functionality can be especially valuable when deploying Insights at scale, with many hundreds or thousands of systems under Insights management.

NOTE

The initial release of tagging is supported by Red Hat Insights Inventory and the Advisor service.

### Prerequisites

The following prerequisites and conditions must be met to use the tagging feature in Red Hat Insights:

- Root permissions, or their equivalent, are required to add to or change the **tags.yaml** file.
- The Red Hat Insights client is installed and registered on each system.

## 5.1. CREATING TAGS AND TAGS.YAML

This section includes more information about creating tags and using the **tags.yaml** file.

### 5.1.1. Tag structure

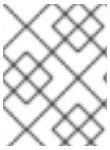
Tags use a **namespace/key=value** paired structure.

- **Namespace.** The namespace is the name of the ingestion point, *insights-client*, and cannot be changed. The **tags.yaml** file is abstracted from the namespace, which is injected by the client before upload.
- **Key.** The key can be a user-chosen key or a predefined key from the system. You can use a mix of capitalization, letters, numbers, symbols and whitespace.
- **Value.** Define your own descriptive string value. You can use a mix of capitalization, letters, numbers, symbols and whitespace.

### 5.1.2. The tags.yaml file

User-defined tags are added to the **/etc/insights-client/tags.yaml** file. You can add any number of key=value pairs to **tags.yaml**, as needed. The YAML syntax makes the contents easy to understand and modify.

Running **insights-client --group=eastern-sap** creates the tagging configuration file, **/etc/insights-client/tags.yaml** and adds the entry **group: eastern-sap**. The following example of a **tags.yaml** file shows additional tags added for the group "eastern-sap."



NOTE

You can use any mix of capitalization, letters, numbers, symbols, and whitespace when creating key=value pairs.

### Example

```
# tags
---
group: eastern-sap
name: Jane Example
contact: jexample@corporate.com
Zone: eastern time zone
Location:
- gray_rack
- basement
Application: SAP
```

## 5.2. ADDING TAGS TO SYSTEMS

The easiest way to start adding tags to **tags.yaml** is by using **insights-client --group=<name-you-choose>**, which performs the following actions:

1. Creates the **etc/insights-client/tags.yaml** file
2. Adds the **group** key and <name-you-choose> value to **tags.yaml**
3. Uploads a fresh archive from the system to cloud.redhat.com so that the new tag is immediately visible along with your latest results

After creating the initial **group** tag, can add additional tags as needed by editing **tags.yaml**.

The following procedure shows how to create the initial group, as well as the **tags.yaml** file, then verify the tag in the Insights inventory.

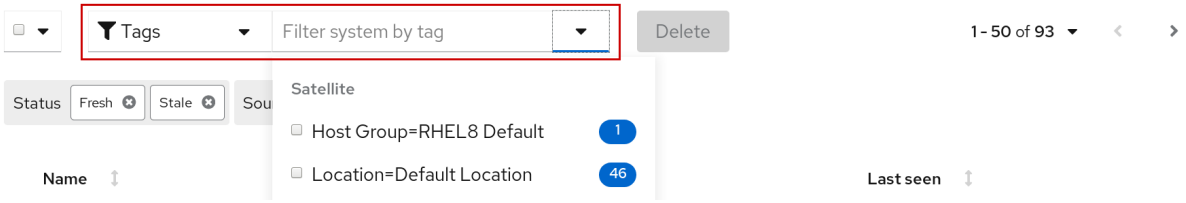
### Procedure

1. Run the following command, adding your group name after **--group=**:

```
[root@server ~]# insights-client --group=<name-you-choose>
```

### Verification steps

1. Navigate to Red Hat Insights > Inventory and log in if necessary.
2. Click the **Filters** dropdown menu and select **Tags**.

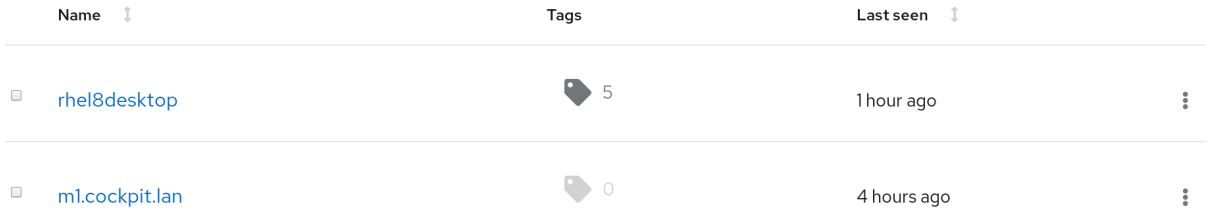



3. In the search box, click the down arrow and select one of the tags or enter the name of the tag.

**NOTE**

You can search by the tag key or value.

4. Find your system among the results and verify that the tag icon is darkened and shows a number representing the number of tags applied to the system.




5. Click the tag to see each of the tags applied to that system.

## 5.3. EDITING TAGS.YAML TO ADD OR CHANGE TAGS

After creating the **group** tag, you can edit the contents of **tags.yaml** to add or modify tags, as needed. You to add multiple, filterable tags to a system.

### Procedure

1. Using the command line, open the tag configuration file for editing.

```
[root@server ~]# vi /etc/insights-client/tags.yaml
```

2. Edit content or add additional key=value pairs as needed. The following example shows how you can organize **tags.yaml** when adding multiple tags to a system.

```
# tags
---
group: eastern-sap
location: Boston
description:
- RHEL8
- SAP
key 4: value
```

**NOTE**

Add as many key=value pairs as you need. Use a mix of capitalization, letters, numbers, symbols, and whitespace.

3. Save your changes and close the editor.

4. Generate an upload to Insights.

```
[root@server ~]# insights-client
```

### Verification steps

1. Navigate to Red Hat Insights > Inventory and log in if necessary.

2. Click the **Filters** dropdown menu and select **Tags**.

3. In the search box, click the down arrow and select one of the tags or enter the name of the tag and select it.

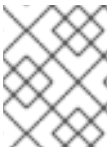
**NOTE**

You can search by the tag key or value.

4. Find your system among the results.
5. Verify that the tag icon is darkened and shows a number representing the number of tags applied to the system.
6. Click the tag to see each of the tags applied to that system.

# CHAPTER 6. CHANGING THE INSIGHTS-CLIENT SCHEDULE

You can disable, enable, and modify the schedule that controls when the Insights client runs. By default, the Insights client runs every 24 hours. The timers in the default schedules vary so that all systems do not run the client at the same instant.



**NOTE**

The procedure you use for changing the **insights-client** schedule depends on the RHEL version as shown in **/etc/redhat-release**.

- Section 6.1, “Disabling the client schedule”
- Section 6.2, “Enabling the Insights client schedule”
- Section 6.3, “Modifying the client schedule”

## 6.1. DISABLING THE CLIENT SCHEDULE

You must disable the client schedule before you can change the default Insights client settings and create a new schedule.

Depending on which version of Insights client is installed and the RHEL version, you select the procedure steps as shown in the following table.

**Table 6.1. Disabling the client schedule based on client version and RHEL release**

| RHEL version | Client version | Actions |
|---|---|---|
| RHEL 6 through RHEL 7.4 | Client 1.x<br>  <br>**NOTE**<br>Client 1.x is no longer supported. | Modify the configuration file **/etc/insights-client/insights-client.conf** and use the CLI |
| RHEL 7.5 and later | Client 1.x<br>  <br>**NOTE**<br>Client 1.x is no longer supported. | Use the CLI |
| RHEL 6, RHEL 7, and later | Client 3.x | Use the CLI |

**Procedure to disable for RHEL 7.4 and earlier with Client 1.x**

**NOTE**

Client 1.x is no longer supported.

1. Verify the client version by entering the **insights-client** command with the **--version** option.

```
[root@insights]# insights-client --version
Client: 1.0.2-0
Core: 1.0.76-1
```

2. Disable the client schedule by entering the **insights-client** command with the **--no-schedule** option. This command removes the symbolic link that is in **/etc/cron.daily**.

```
[root@insights]# insights-client --no-schedule
```

NOTE

The **--no-schedule** option is deprecated in Client 3.x and later.

3. Open the **/etc/insights-client/insights-client.conf** file with an editor and add the following line.

```
no_schedule=True
```

**Procedure to disable for RHEL 7.5 and later with Client 1.x**

NOTE

Client 1.x is no longer supported.

1. Verify the client version by entering the **insights-client** command with the **--version** option.

```
[root@insights]# insights-client --version
Client: 1.0.2-0
Core: 1.0.76-1
```

2. Disable the client schedule by entering the **insights-client** command with the **--no-schedule** option.

```
[root@insights]# insights-client --no-schedule
```

NOTE

The **--no-schedule** option is deprecated in Client 3.x and later.

**Procedure to disable for RHEL 6, RHEL 7 and later with Client 3.x**

1. Verify the client version by entering the **insights-client** command with the **--version** option.

```
[root@insights]# insights-client --version
Client: 3.0.6-0
Core: 3.0.121-1
```

2. Disable the client schedule by entering the **insights-client** command with the **--disable-schedule** option.

```
[root@insights]# insights-client --disable-schedule
```

## 6.2. ENABLING THE INSIGHTS CLIENT SCHEDULE

You can enable the client schedule so that it runs on its default settings. If you changed the schedule, those settings take precedence.

### Prerequisites

- The client schedule is disabled.
  Section 6.1, “Disabling the client schedule”
- (Optional) You modified the default schedule.
  Section 6.3, “Modifying the client schedule”

### Procedure to enable with RHEL 7.4 or earlier and Client 1.x

**NOTE**

Client 1.x is no longer supported.

1. Verify the client version by entering the **insights-client** command with the **--version** option.

```
[root@insights]# insights-client --version
Client: 1.0.2-0
Core: 1.0.76-1
```

2. Open the **/etc/insights-client/insights-client.conf** file with an editor and add change following line to **False**.

```
no_schedule=False
```

3. Enable the client schedule by entering the **insights-client** command with the **--register** option.

```
[root@insights]# insights-client --register
```

### Procedure to enable with RHEL 7.5 or later and Client 1.x

**NOTE**

Client 1.x is no longer supported.

1. Verify the client version by entering the **insights-client** command with the **--version** option.

```
[root@insights]# insights-client --version
Client: 1.0.2-0
Core: 1.0.76-1
```

2. Enable the client schedule by entering the **insights-client** command with the **--register** option.

```
[root@insights]# insights-client --register
```

**Procedure to enable with RHEL 7 or later and Client 3.x**

1. Verify the client version by entering the **insights-client** command with the **--version** option.

```
[root@insights]# insights-client --version
Client: 3.0.6-0
Core: 3.0.121-1
```

2. Enable the client schedule by entering the **insights-client** command with the **--enable-schedule** option.

```
[root@insights]# insights-client --enable-schedule
```

## 6.3. MODIFYING THE CLIENT SCHEDULE

You can modify when the Insights client runs by modifying the schedule. Which method you use depends on which RHEL release and which client version your system is running. Select the procedure that matches your version of RHEL.

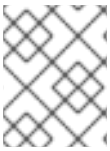
- RHEL 7.4 and ealier
  Section 6.3.1, "Scheduling **insights-client** with **cron**"
- RHEL 7.5 and later
  Section 6.3.2, "Scheduling **insights-client** with **systemd** settings"

**Prerequisites**

- Section 6.1, "Disabling the client schedule"

### 6.3.1. Scheduling insights-client with cron

You can change the default schedule for running **insights-client** by updating a system **cron** file.



NOTE

The procedure for modifying **insights-client** with **cron** applies to RHEL 7.4 releases and earlier that are running Client version 1.x.

**Prerequisites**

- Section 6.1, "Disabling the client schedule".
- Review the man pages for **crontab(1)** and **cron(8)** to understand the **cron** dependencies.

**Procedure**

1. After disabling the Insights client schedule, set up **cron** to execute **insights-client** on a schedule you prefer.

2. Enable the **insights-client** schedule for RHEL 7.4 and earlier when you finish making changes.

**Additional resources**

- Section 6.2, "Enabling the Insights client schedule"
- What is **cron** and how is it used?

### 6.3.2. Scheduling insights-client with systemd settings

You can change the default schedule for running **insights-client** by updating the system **systemd** settings and the **insights-client-timer** file.

NOTE

The **systemd** procedure applies to RHEL 7.5 and later.

**Prerequisites**

- Section 6.1, "Disabling the client schedule"
- Review the man pages for **systemctl(1)**, **systemd.timer(5)**, and **systemd.time(7)** to understand **systemd** before proceeding.

**Procedure**

1. Enter the **systemctl** command to override the settings in the **insights-client.timer** systemd unit.

```
[root@insights]# systemctl edit insights-client.timer
```

   This action opens an empty file with the default system editor.

2. The following settings are default values for the **systemd** unit. Enter different settings to modify the schedule.

```
[Timer]
OnCalendar=daily
RandomizedDelaySec=14400
```

3. Enable the **insights-client** schedule by entering the **insights-client** command with the **--enable-schedule** option.

```
[root@insights]# insights-client --enable-schedule
```

# CHAPTER 7. CHANGING RED HAT INSIGHTS AUTOMATIC RULE UPDATES

The following procedures show how to change automatic rule update settings in the Insights client.

- Section 7.1, “Disabling automatic rule updates for Red Hat Insights”
- Section 7.2, “Enabling automatic rule updates for Red Hat Insights”

## 7.1. DISABLING AUTOMATIC RULE UPDATES FOR RED HAT INSIGHTS

You can disable the automatic collection rule updates for Red Hat Insights. If you do so, you risk using outdated rule definition files and not getting the most recent validation updates.

### Procedure

1. Open the **/etc/insights-client/insights-client.conf** file with an editor.
2. Locate the line that contains

```
#auto_update=True
```

3. Remove the **#** and change **True** to **False**.

```
auto_update=False
```

4. Save and close the the **/etc/insights-client/insights-client.conf** file.

### Additional resources

- Section 7.2, “Enabling automatic rule updates for Red Hat Insights”

## 7.2. ENABLING AUTOMATIC RULE UPDATES FOR RED HAT INSIGHTS

You can enable the automatic collection rule updates for Red Hat Insights if you previously disabled updates. By default, automatic rule update is enabled.

### Prerequisites

Automatic rule collection must be disabled.

Section 7.1, “Disabling automatic rule updates for Red Hat Insights”

### Procedure

1. Open the **/etc/insights-client/insights-client.conf** file with an editor.
2. Locate the line that contains

```
auto_update=False
```

3. Change **False** to **True**.

```
auto_update=True
```

4. Save and close the the **/etc/insights-client/insights-client.conf** file.

# CHAPTER 8. SETTING THE AUTHENTICATION METHOD

Depending on how you use Red Hat Insights, you must use one of two authentication methods:

- Certificate-based authentication (CERT)
  The default authentication method is through certificates. Certificates are generated when you register a system with Red Hat Subscription Manager (RHSM) or when your system is managed by Red Hat Satellite system management. No additional configuration changes are required.

- SSO credential-based Authentication (BASIC)
  The alternative authentication method is through SSO credentials. A valid Red Hat SSO credential is created when you have a valid Red Hat Customer Portal user name. To use SSO credentials with Red Hat Insights, you must configure your system to use basic authentication.

**Additional resources**

- Configuring BASIC authentication for Red Hat Insights

# CHAPTER 9. CREATING A DIAGNOSTIC LOG FOR SUPPORT

You can create a diagnostic log to share with the support team.

**Procedure**

1. Enter the **insights-client** command with the **--support** option.

```
[root@insights]# insights-client --support
```

   The command displays informational messages while creating the support file.

```
Collecting logs...
Insights version: insights-core-3.0.121-1
Registration check:
status: True
unreachable: False
. . . .
Copying Insights logs to archive...
Support information collected in /var/tmp/H_Y43a/insights-client-logs-20190927144011.tar.gz
```

2. Navigate to the collection directory as shown in the **Support information collected in** message.

```
[root@insights]# cd /var/tmp/H_Y43a
```

3. Unpack the compressed **tar.gz** file.

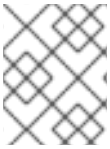
```
[root@insights]# tar -xzf insights-client-logs-20190927144011.tar.gz
```

   The result will be a new directory containing the files. You can share the **tar.gz** file with the support team if requested.

# CHAPTER 10. COMMAND OPTIONS FOR INSIGHTS-CLIENT

You can use the **insights-client** command and its options to control the Insights client operation on your system. Because the **insights-client.rpm** is updated less frequently than individual components in Insights, the man page might not include the most recent information about **insights-client** command operation.

As a system administrator with root privileges, each time you enter the **insights-client** command the client collects data and sends it to Red Hat Insights.



NOTE

Using the **insights-client --display-name** command to set the display name takes effect immediately but does not run the Insights client.

**Table 10.1. insights-client user command options**

| Option | Description |
|---|---|
| **--help**<br>**-h** | Display help information |
| **--register** | Register the host to Insights using the information in **/etc/hostname**. Will automatically enable the nightly cron job unless **--disable-schedule** is set. |
| **--unregister** | Unregister the host from Insights. |
| **--display-name=DISPLAY_NAME** | Set or change the host display name in the GUI. Use with **--register** to set a display_name when the host is registered if you want a different name than is in **/etc/hostname**. |
| **--group=GROUP** | Add host to GROUP during registration. Group names are defined in **/etc/insights-client/tags.yaml** |
| **--retry=RETRIES** | Set the number of times to retry an upload. The default is 1. The retry interval is 180 seconds, which is how long the Insights client waits until retrying the upload.<br>NOTE: In the scheduler, the number of retries is 3. |
| **--validate** | Validate the structure of the **/etc/insights-client/remove.conf** file. |
| **--quiet** | Only log error messages to console. |
| **--silent** | Log nothing to console. |

| Option | Description |
|---|---|
| **--enable-schedule** | Enable the job schedule. By default, the Insights client runs daily, at or near midnight.<br><br>NOTE: If you are using Client 1.x, use the **--register** option to enable the schedule. |
| **--disable-schedule** | Disable the nightly job schedule. |
| **--conf=CONF**<br><br>**-c=CONF** | Use a custom configuration file CONF instead of the default **/etc/insights-client/insights-client.conf** file. |
| **--compressor** | Select the compressor that is used when creating the archive. Available options are **gz, bz2, xz, none**. Defaults to **gz**. The **none** option creates a tar file with no compression. |
| **--no-upload** | Runs the client but does not upload the archive to Red Hat Insights or CMSfR web application. The archive is stored in the **/var/tmp/** directory. The file name is displayed when **insights-client** completes. |
| **--offline** | Run the client without using network functionality. Implies **--no-upload**. |
| **--logging-file=LOGFILE** | Output the log data to the specified LOGFILE. The default log file is **/var/log/insights-client/insights-client.log**. |
| **--diagnosis** | Fetch diagnostic information from the API. The system must be registered and uploaded at least once before using **--diagnosis**. |
| **--compliance** | Scan the system with OpenSCAP and upload the report. |
| **--payload=PAYLOAD** | Upload a specific archive PAYLOAD file to Red Hat Insights. Requires **--content-type**. |
| **--content-type=TYPE** | Set the content-type for the PAYLOAD file. Type can be gz, bz2, xz, and none. The TYPE must match the **--compressor** used with the PAYLOAD. |
| **--check-results** | Retrieve analysis results from Red Hat Insights. |
| **--show-results** | Display analysis results fetched by **--check-results**. |

| Option | Description |
|---|---|
| **--output-dir=DIR** | Write collection to a specified directory instead of uploading. |
| **--output-file=FILE** | Write collection to a specified archive instead of uploading. |

The **insights-client** command has several options that are useful when debugging its operation.

Table 10.2. **insights-client** debug options

| Option | Description |
|---|---|
| **--version** | Print the versions of **insights-client** Client and Core. |
| **--test-connection** | Test connectivity to the Red Hat Insights services. |
| **--force-reregister** | Re-register the system with Insights and use a new ID. This action duplicates an already-registered system. |
| **--verbose** | Log all debug output to the console. |
| **--no-upload** | Runs the client but does not upload the archive. The archive is stored in the **/var/tmp/** directory. The file name is displayed when **insights-client** completes. |
| **--keep-archive** | Keep the archive after uploading. |
| **--support** | Generate a diagnostic log for support. |
| **--status** | Display host registration status. |
| **--net-debug** | Log network calls to the console. |

# CHAPTER 11. OPTIONS FOR INSIGHTS CLIENT REMOVE.CONF REDACTION CONFIGURATION FILE

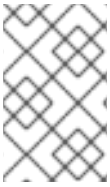
NOTE

As of RHEL RHEL 6.10, 7.9, 8.3 and later, using **remove.conf** is deprecated and replaced by two YAML files. See Chapter 12, *Options for Insights client YAML redaction configuration files*.

A configuration file, **/etc/insights-client/remove.conf**, controls how data is redacted. The Insights client performs redaction on the archive file based on the information in **remove.conf**. Most redaction activity occurs before the archive file is generated and sent to the Red Hat Insights service.

## File name and location

The suggested name is **/etc/insights-client/remove.conf** for the redaction configuration file. You must have root permission in order to create this file. It is not created automatically as part of the Insights client deployment.



NOTE

The **/etc/insights-client/insights.client.conf** configuration file specifies the name and location of the redaction configuration file. See Chapter 13, *Options for the Insights client configuration file*.

## File template for remove.conf

The following is an example template for the **remove.conf** file:

```
[remove]
files=/etc/cluster/cluster.conf,/etc/hosts
commands=/bin/dmesg,/bin/hostname
patterns=password,username
keywords=super$ecret,ultra$ecret+
```

- A single comma with no space separates each entered value.
- Do not include the line for data you do not want redacted.
- Regular expressions and wildcard matching (**egrep**) are not supported.
- All entries are case-sensitive.

**Table 11.1. remove.conf configuration options**

| Option | Description |
|---|---|
| **[remove]** | This must be the first line of the **remove.conf** file. |
| **files=** | The listed files are excluded from data collecting. |

| Option | Description |
| --- | --- |
| **commands=** | The output from commands listed here is excluded from data collecting. The command names must exactly match the command names in the collection rules. |
| **patterns=** | Any line in the archive file that matches all or part of a **pattern** is deleted. |
| **keywords=** | The keyword is replaced with an actual value of **keyword** and a number.<br><br>For example, if you define two keywords, **keywords=host,domain**, each instance of **host** is replaced with the string **keyword0** and each instance of **domain** is replaced with **keyword1**. Each additional keyword you define is replaced with an incremental **keywordn**. |

# CHAPTER 12. OPTIONS FOR INSIGHTS CLIENT YAML REDACTION CONFIGURATION FILES

NOTE

As of RHEL RHEL 6.10, 7.9, 8.3 and later, Insights client uses YAML files to configure redaction. In earlier releases a **remove.conf** file controls redaction. See Chapter 11, *Options for Insights client* ***remove.conf*** *redaction configuration file* for **remove.conf** reference information.

**Table 12.1. File redaction example for file-redaction.yaml**

| Content | Description |
|---|---|
| `# file-redaction.yaml`<br>`---` | An optional comment containing the file name. |
| `# Exclude the entire output of commands`<br>`#  Specify the full command path or the symbolic name in .cache.json`<br><br>`commands:`<br>`- /bin/rpm -qa`<br>`- /bin/ls`<br>`- ethtool_i` | The entire output from **/bin/rpm -qa** and **bin/ls** are excluded from the archive file.<br><br>In the **.cache.json** file, the full command **/sbin/ethtool -i** is mapped to the symbolic name **ethtool_i**. |
| `# Exclude the entire output of files`<br>`#  Specify the full filename path or the symbolic name in .cache.json`<br><br>`files:`<br>`- /etc/audit/auditd.conf`<br>`- cluster_conf` | For the specified files, the file name and the file content are excluded from the archive file.<br><br>In the **.cache.json** file, the full file path **/etc/cluster/cluster.conf** is mapped to the symbolic name **cluster_conf.** |

**Table 12.2. Content redaction example for file-content-redaction.yaml**

| Content | Description |
|---|---|
| `# file-content-redaction.yaml`<br>`---` | An optional comment containing the file name. |

| Content | Description |
| --- | --- |
| # Pattern redaction per matching line<br># Lines that match a pattern are excluded from files and command output.<br># Patterns are processed in the order that they are listed.<br># Example<br><br>patterns:<br>- "a_string_1"<br>- "a_string_2" | When the patterns match exactly any lines that contain **a_string_1** or **a_string_2** are excluded from files and command output. Enclose the pattern string in quotes. |
| #<br># Regular expression pattern redaction per line<br># Patterns with regular expressions (regex) are wrapped with "regex:"<br># Example<br><br>patterns:<br>regex:<br>- "abc.*def"<br>- "localhost[[:digit:]]"<br># | Regular expressions are wrapped with **regex**. You can use any regular expression (regex) recognized by the **egrep** command. Enclose the regex in quotes. |
| # Lines matching these regular expressions are excluded<br># from output.<br>patterns:<br>regex:<br>- "*\.conf"<br>- "^include" | The **egrep** expressions are enclosed in quotes to make sure the regex characters are properly recognized.<br><br>In this example, lines are redacted from the archive file if any string contains **.conf** or if any line begins with **include**. |
| # Replace keywords in files and command output with generic identifiers by the Python soscleaner module<br>keywords:<br>- "1.1.1.1"<br>- "My Name"<br>- "a_name" | The strings in the **keywords:** array are replaced with the actual value **keyword** and a number.<br><br>For example, each instance of the string **1.1.1.1** is replaced with **keyword0**. All instances of the string **My Name** are replaced with **keyword1**. The **a_name** is replaced with **keyword3** Each additional keyword you define is replaced with an incremental **keywordn** The value of the substituted **keywordn** is determined by a Python SoS process and cannot be changed.<br><br>The strings that you define in the **keywords:** array are case sensitive. |

# CHAPTER 13. OPTIONS FOR THE INSIGHTS CLIENT CONFIGURATION FILE

You can use the settings in the **/etc/insights-client/insights-client.conf** configuration file to change how the Red Hat Insights client operates on your system.

Where the configuration file and the CLI have similar options, the CLI option is executed when you enter the **insights-client** command. When the scheduler runs the client, the configuration file options are executed.

NOTE

All choices must be entered as shown. **True** and **False** use initial capital letters.

To enable an option in the configuration file, remove the **#** as the first character of the line and provide a value. The changes take effect either at the next scheduled run, or when you enter the **insights-client** command.

**Table 13.1. insights-client.conf configuration options**

| Option | Description |
|---|---|
| [insights-client] | Required first line of the configuration file, even if you specify a different location or name for the client configuration file. |
| #loglevel=DEBUG | Change the log level. Options are: DEBUG, INFO, WARNING, ERROR, CRITICAL. The default is DEBUG. The default log file location is **/var/log/insights-client/insights-client.log**. |
| #auto_config=True | Attempt to auto configure with Satellite server. Values can be **True** (default) or **False**.<br>  <br>NOTE<br>When **auto_config=True** (default), the authentication method used is **CERT**. |
| #authmethod=BASIC | Set the authentication method. Valid options BASIC, CERT. The default value is BASIC even though CERT is used when **auto_config=True**. |
| #username= | **username** to use when authmethod is BASIC. The **username** is stored in clear text. |
| #password= | **password** to use when authmethod is BASIC. The **password** is stored in clear text. |

| Option | Description |
| --- | --- |
| #base_url=cert-api.access.redhat.com:443/r/insights | Base URL for the API. |
| #proxy= | URL for your proxy. Example: http://user:pass@192.168.100.50:8080 |
| #auto_update=True | Automatically update the dynamic configuration. The default is **True** Change to **False** if you do not want to automatically update. |
| #obfuscate=False | Obfuscate IPv4 addresses. The default is **False**. Change to **True** to enable address obfuscation. |
| #obfuscate_hostname=False | Obfuscate hostname. You must set **obfuscate=True** to obfuscate the host name, which enables IPv4 address obfuscation. You cannot obfuscate only the host name. |
| #display_name= | Display name for registration. The default is to use **/etc/hostname**. NOTE: This value interacts with the **insights-client --display-name** command. If you use the CLI to change the display name but a different display name is enabled in the configuration file, the display name reverts to the configuration file value when the scheduler runs the Insights client. |
| #cmd_timeout=120 | Timeout for commands run during collection, in seconds. The command processes are terminated when the timeout value is hit. |
| #http_timeout=120 | Timeout for HTTP calls, in seconds |
| #remove_file=/etc/insights-client/remove.conf | Location of redaction file |