



Red Hat Insights 2022

Assessing RHEL Configuration Issues Using the Red Hat Insights Advisor Service

Assess and monitor the configuration issues impacting your RHEL systems

Red Hat Insights 2022 Assessing RHEL Configuration Issues Using the Red Hat Insights Advisor Service

Assess and monitor the configuration issues impacting your RHEL systems

Legal Notice

Copyright © 2022 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Use the Insights Advisor service to assess and monitor configuration issues affecting the availability, stability, performance, and security of your RHEL systems.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	3
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION	4
CHAPTER 1. OVERVIEW OF INSIGHTS FOR RHEL ADVISOR SERVICE ASSESSMENT AND MONITORING .	5
CHAPTER 2. ADVISOR SERVICE RECOMMENDATIONS OVERVIEW	6
2.1. SYSTEM AND RECOMMENDATION PAIRING	7
CHAPTER 3. REFINING ADVISOR SERVICE RECOMMENDATIONS	8
3.1. VIEWING ALL ADVISOR RECOMMENDATIONS	8
3.2. FILTERING RECOMMENDATIONS	8
3.3. SORTING RECOMMENDATIONS	10
3.4. DISABLING A RECOMMENDATION	10
3.5. VIEWING AND ENABLING A PREVIOUSLY DISABLED RECOMMENDATION	11
CHAPTER 4. REFINING THE ADVISOR SERVICE SYSTEMS LIST	12
4.1. FILTER BY NAME	12
4.2. SORTING OPTIONS	12
CHAPTER 5. FILTERING TAGS, SAP WORKLOADS, AND GROUPS IN THE ADVISOR SERVICE	13
CHAPTER 6. DELETING A SYSTEM FROM INVENTORY	14
CHAPTER 7. SYSTEM FILTERING AND GROUPS	15
7.1. SAP WORKLOADS	15
7.2. SATELLITE HOST GROUPS	15
7.3. CUSTOM SYSTEM TAGGING	15
7.3.1. Filter structure	16
7.3.2. Creating a custom group and the tags.yaml file	16
7.3.3. Editing tags.yaml to add or change tags	17
7.4. ADDING FILTERS TO SYSTEMS	17
7.5. EDITING TAGS.YAML TO ADD OR CHANGE TAGS	18
CHAPTER 8. REFERENCE MATERIALS	20

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see [our CTO Chris Wright's message](#).

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. To provide feedback, highlight text in a document and add comments.

Prerequisites

- You are logged in to the Red Hat Customer Portal.
- In the Red Hat Customer Portal, the document is in the **Multi-page HTML** viewing format.

Procedure

To provide your feedback, perform the following steps:

1. Click the **Feedback** button in the top-right corner of the document to see existing feedback.



NOTE

The feedback feature is enabled only in the **Multi-page HTML** format.

2. Highlight the section of the document where you want to provide feedback.
3. Click the **Add Feedback** pop-up that appears near the highlighted text.
A text box appears in the feedback section on the right side of the page.
4. Enter your feedback in the text box and click **Submit**.
A documentation issue is created.
5. To view the issue, click the issue link in the feedback view.

CHAPTER 1. OVERVIEW OF INSIGHTS FOR RHEL ADVISOR SERVICE ASSESSMENT AND MONITORING

Use the advisor service to assess and monitor the health of your Red Hat Enterprise Linux (RHEL) infrastructure. Whether you are concerned with individual or groups of systems, or with your whole infrastructure, be aware of the exposure of your systems to configuration issues that can affect availability, stability, performance, and security.

After installing and registering the Insights for RHEL client, the client runs daily to check systems against a database of **Recommendations**, which are sets of conditions that can leave your RHEL systems at risk. Your data is then uploaded to the [Red Hat Enterprise Linux > Advisor > Recommendations](#) page where you can perform the following actions:

- See all of the recommendations for your entire RHEL infrastructure.
- Use robust filtering capabilities to refine your results to those recommendations, systems, groups, or workloads that are of greatest concern to you, including SAP workloads, Satellite host collections, and custom tags.
- Learn more about individual recommendations, details about the risks they present, and get resolutions tailored to your individual systems.
- Share results with other stakeholders. For more information, see [Generating Advisor Service Reports](#).
- Create and manage remediation playbooks to fix issues right from the Insights for RHEL application. For more information, see [Remediating Configuration Issues Using Red Hat Insights and Ansible Playbooks](#).

CHAPTER 2. ADVISOR SERVICE RECOMMENDATIONS OVERVIEW

The advisor service bundles information about known configuration issues that might negatively affect the *availability, stability, performance, or security* of your RHEL systems. This information bundle is used to create recommendations about how you can fix or remediate issues on your systems.

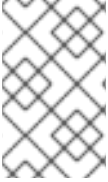
Recommendations are published to the advisor service database, and can be accessed through the advisor recommendations page. When you navigate to the page you can use various sort and filter methods to access information such as:

- **Modified.** The date or time frame when a recommendation was last modified (or published) to the advisor service database
- **Category.** The type of issue or what the issue affects—whether the issue has the potential to negatively affect the **availability, stability, performance, or security** of RHEL systems
- **Impact.** The *impact* (**Low, Medium, High** or **Critical**) on system operations if an incident related to the recommendation were to happen
- **Incidents.** The issue has been classified as an incident and is an issue that is already affecting your systems
- **Likelihood.** The *likelihood* (**Low, Medium, High** or **Critical**) that the issue will negatively affect your infrastructure
- **Name.** A brief description of the issue, including how it affects RHEL systems
- **Reboot Required.** A system reboot status (**Required** or **Not Required**) indicates whether the system needs to be rebooted or not as part of a remediation
- **Remediation.** The fix or remediation requires manual (not automated) steps or has an automated playbook
- **Risk of change.** The risk of change (**Very Low Low, Moderate, or Important**) for systems operations due to executing the recommended remediation
- **Status.** Describes a recommendation **Status** (**Enabled, Disabled, or Red Hat disabled**) and tells you if the recommendation is visible, or not visible. **Disabled** indicates that someone in your organization turned visibility of a recommendation off. **Red Hat disabled** indicates that Red Hat has turned visibility of a recommendation off because the issue does not pose an immediate risk to your systems)
- **Systems or Systems impacted.** The number of systems (**1 or more** or **None**) on which a recommendation is detected
- **Total risk.** Describes total risk level (**Low, Moderate, Important, or Critical**), which is determined by the *likelihood* that the issue will negatively affect your infrastructure, and the *impact* on system operations if that were to happen



NOTE

A recommendation was formerly called a rule in Insights for Red Hat Enterprise Linux.



NOTE

The default advisor service recommendations view shows a smaller subset of information, and is also filtered to show systems information for **1 or more systems** and has a status of **Enabled**. Information about filters is discussed in later sections of this documentation.

2.1. SYSTEM AND RECOMMENDATION PAIRING

When a recommendation exists on a system, the advisor service identifies whether, and how, the system has been impacted *and* provides specific mitigation or resolution instructions. This information is visible when viewing a recommendation and then selecting an affected system.

After selecting an affected system, view all recommendations available for the system along with the following information:

- **Detected issues.** Specific information about the fault on that system
- **Steps to resolve.** Steps to resolve the issue on *that* system
- **Related knowledgebase articles.** KB articles or solutions about the general issue
- **Additional info.** Other support articles on the issue or solutions for resolution
- **Ansible.** Playbook remediation availability

CHAPTER 3. REFINING ADVISOR SERVICE RECOMMENDATIONS

The advisor service puts a lot of information at your fingertips, especially when Insights for Red Hat Enterprise Linux is deployed at scale. However, there are several ways to refine advisor results to help you focus on your most critical systems and issues. This section describes the multiple options for filtering, sorting, and excluding specific recommendations from your advisor results.

The screenshot displays the 'Advisor recommendations' interface. At the top, there is a search bar and filters for 'Workloads' and 'All workloads'. Below this, a table lists recommendations. The visible recommendation is: 'Misconfigured applications running on EC2 instances where IMDSv1 is enabled will have access to the internal Metadata service by exploiting application vulnerabilities'. It was added '3 months ago', has an 'Important' risk level, a 'Very Low' risk of change, and affects 6 systems. The 'Ansible' column shows a green checkmark.

3.1. VIEWING ALL ADVISOR RECOMMENDATIONS

When you first enter the Insights for Red Hat Enterprise Linux advisor service recommendations view, you see the the default view and results of **Systems Impacted** (set to 1 or more systems) and **Status** (set to Enabled) filters being applied. To get a comprehensive view of *all* recommendations, including those not impacting your systems and those in the advisor database, use the following procedure:

Prerequisites

*You must be logged into the [Red Hat Hybrid Cloud Console](#).

Procedure

1. Navigate to the [Red Hat Enterprise Linux > Advisor > Recommendations](#) page.



2. Click the close icon next to the **Systems Impacted** and **Status** filters. You can now browse through all of the potential recommendations for your systems.
3. Optionally, return to the default recommendations view that shows **1 or more of Systems impacted** and the **Status** set to **Enabled**, by clicking **Reset filters**.

3.2. FILTERING RECOMMENDATIONS

Select from the following filters to refine your recommendations list:

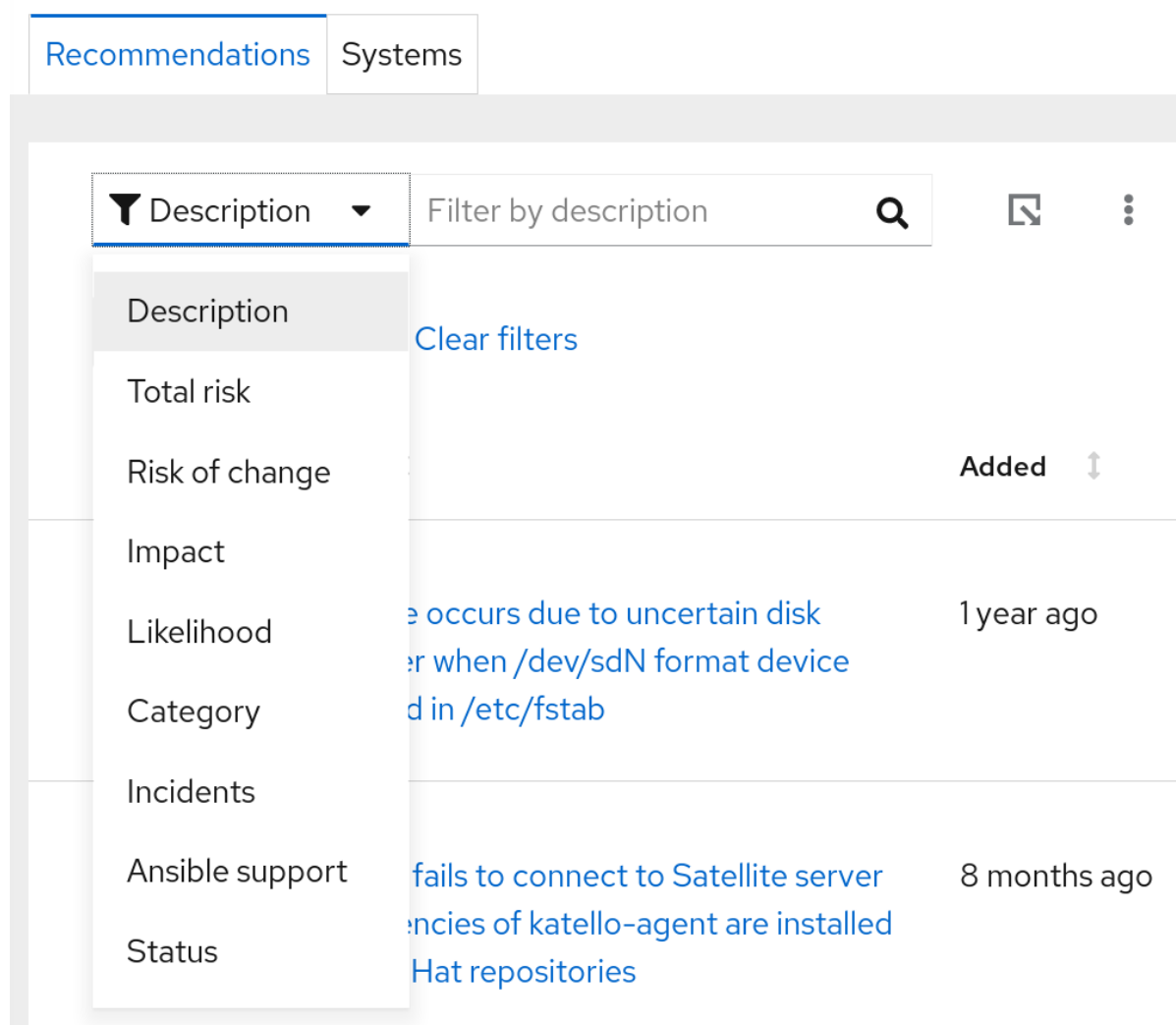
- **Name.** In the subfilter field, start typing the recommendation description or a keyword and select from the options presented.
- **Total risk.** In the subfilter field, select from one or more: Critical, Important, Moderate, or Low.
- **Risk of change.** In the subfilter field, select from High, Moderate, Low, or Very low.

- **Impact.** In the subfilter field, select from Critical, Important, Moderate, or Low.
- **Likelihood.** In the subfilter field, select from Critical, Important, Moderate, or Low.
- **Category.** In the subfilter field, select from Availability, Performance, Stability, or Security.
- **Incidents.** In the subfilter field, select to show recommendations with or without incidents having occurred.
- **Ansible support.** In the subfilter field, select to show recommendations with or without Ansible Playbook support.
- **Status.** In the subfilter field, select from All, Enabled, or Disabled.

To set filters, complete the following steps:

Procedure

1. Navigate to the [Red Hat Enterprise Linux > Advisor > Recommendations](#) page and log in if necessary.
2. Click the filter icon and select a filter category from the dropdown list.



3. Click the dropdown arrow in the subfilter menu and check a box (or boxes) to activate a subfilter or, in the case of Description, begin typing the name or description of a recommendation.

The screenshot shows the 'Recommendations' tab in the Red Hat Insights Advisor interface. At the top, there are two tabs: 'Recommendations' (active) and 'Systems'. Below the tabs, there is a filter section with a 'Total risk' dropdown set to 'Filter by total risk'. A dropdown menu is open, showing four risk levels: 'Critical' (selected), 'Important', 'Moderate', and 'Low'. To the left of the dropdown, there is a 'Status' dropdown set to 'Enabled'. Below the filter section, there is a table with columns for 'Description' and 'Added'. The 'Description' column shows a recommendation: 'OS boot failure occurs due to uncertain disk discovery order when /dev/sdN format device names are used in /etc/fstab'. The 'Added' column shows '1 year ago'.

3.3. SORTING RECOMMENDATIONS

Sort your results using the sorting arrows above each column in the recommendations list. You can sort by one column at a time using the following parameters:


- **Name.** Alphabetize by A to Z or Z to A.
- **Added.** Order by number of days since recommendation was added to the archive, from newest or oldest.
- **Total risk.** View in order of criticality.
- **Systems.** View by the number of your systems that are impacted.
- **Ansible.** View the recommendations with or without Ansible Playbook support.

3.4. DISABLING A RECOMMENDATION

Disable specific recommendations impacting your systems so that they no longer appear in your results. To disable a recommendation, complete the following steps:

Procedure

1. Navigate to the [Red Hat Enterprise Linux > Advisor > Recommendations](#) page and log in if necessary.
2. Locate the recommendation to disable.

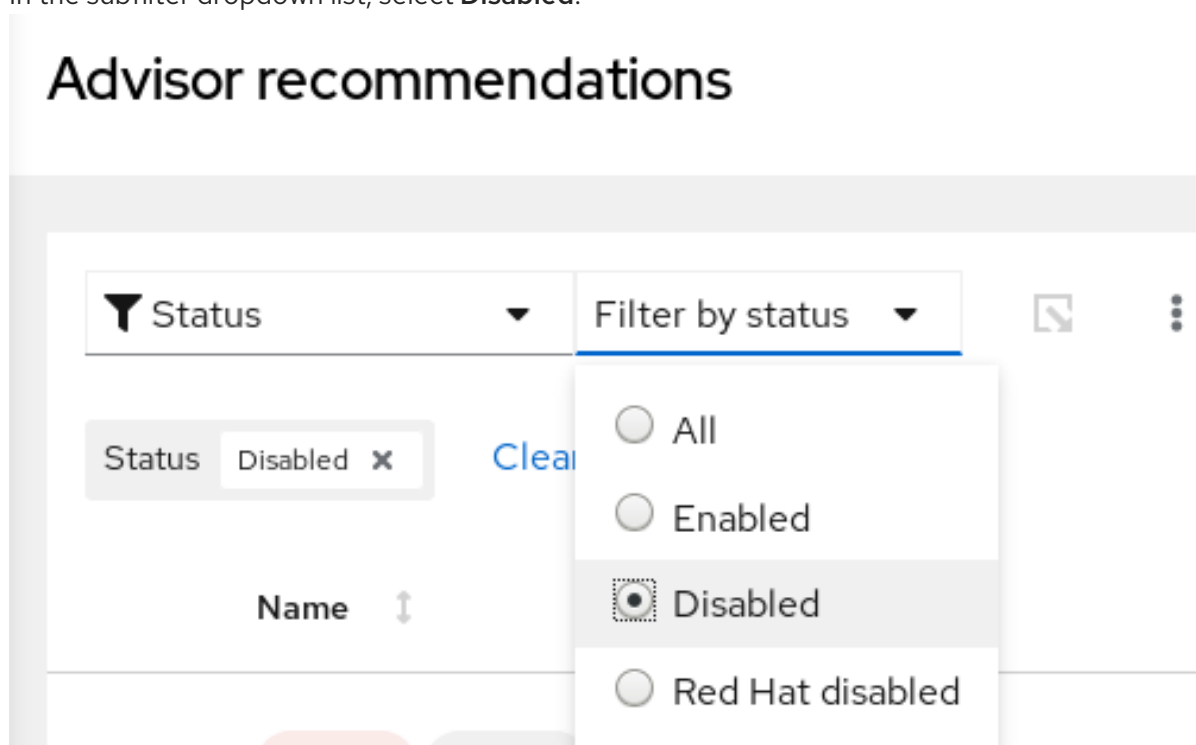
3. Click the **more-actions** icon,  , at the far right of the row and click **Disable recommendation**.

3.5. VIEWING AND ENABLING A PREVIOUSLY DISABLED RECOMMENDATION


When a recommendation is disabled, you will no longer see the recommendation in your advisor results. To reverse this action, complete the following steps:

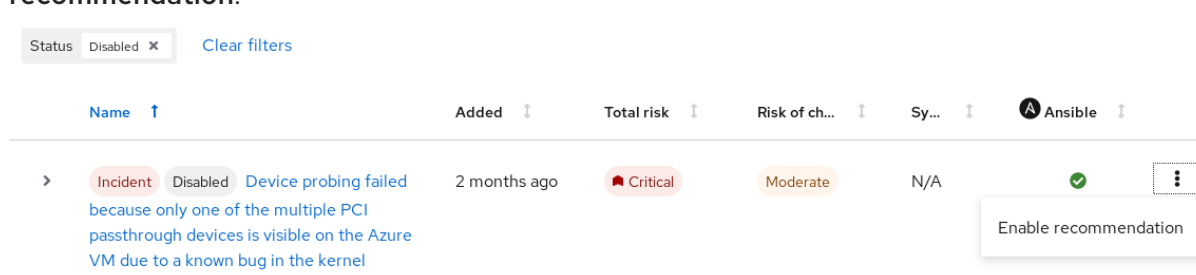
Procedure

1. Navigate to the [Red Hat Enterprise Linux > Advisor > Recommendations](#) page and log in if necessary.
2. Click the Filter dropdown and select **Status**.
3. In the subfilter dropdown list, select **Disabled**.



4. Locate the recommendation to enable.

5. Click the **more-actions** icon,  , on the right side of the row, and click **Enable recommendation**.



CHAPTER 4. REFINING THE ADVISOR SERVICE SYSTEMS LIST

The **Systems** view shows all of your systems that have the Insights client installed and reporting advisor data. The Systems list can be refined in the following ways.

Name	Recommendations	Critical	Important	Moderate	Low	Last seen
lxc-rhel6	4	0	0	4	0	6 minutes ago

4.1. FILTER BY NAME

Search for the host or system name.

4.2. SORTING OPTIONS

Use the sorting arrows above the following columns to order your systems table:

- **Name.** Alphabetize by A to Z or Z to A.
- **Number of recommendations.** Order by the number of recommendations impacting each system.
- **Last seen.** Order by the number of minutes, hours, or days since an archive was last uploaded from the system to the advisor service.

CHAPTER 5. FILTERING TAGS, SAP WORKLOADS, AND GROUPS IN THE ADVISOR SERVICE

Filter results in the advisor service UI by custom group tags, SAP workloads, and Satellite groups to quickly locate and view the systems you want to focus on.

In the advisor service, access tag, workload, and group filters using the **Filter results** box, located in the upper left corner of the page in the Insights for Red Hat Enterprise Linux application.

The filter dropdown menu shows all of the tags associated with the account, allowing you to click one or more parameters by which to filter. To filter by tags in the advisor service, complete the following steps:

Procedure

1. Navigate to the [Red Hat Enterprise Linux > Advisor > Systems](#) page and log in if necessary. The **Filter results** box is in most views in the Insights for Red Hat Enterprise Linux application and these procedures work anywhere you access **Filter results**.
2. Click the arrow on the **Filter results** box and scroll to see the tags available for systems on this account.
3. Select one or more tags to filter by SAP workloads, Satellite host group, or a custom group. Applied tags are visible next to the **Filter results** box.
4. View the filtered results throughout the advisor service.
5. To remove the tag, click **Clear filters**.

CHAPTER 6. DELETING A SYSTEM FROM INVENTORY

You can delete a system from the [Red Hat Hybrid Cloud Console](#) inventory so that the system is no longer visible in the Insights for Red Hat Enterprise Linux Inventory or advisor service Systems list. The Insights client will be unregistered on the system and no longer report data to Insights for Red Hat Enterprise Linux. To delete a system, complete the steps in the procedure below that is most relevant to your use case.

Procedure 1: Delete using the Insights client

1. Enter the following command on the system command line:

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

Procedure 2: Delete from the Red Hat Satellite 6 UI

1. Log in to the Satellite web UI.
2. Navigate to Insights > Inventory.
3. Select the system profile to be unregistered.
4. Click **Actions** > **Unregister**.

Procedure 3: Delete using the cloud.redhat.com API

Use this option only when the actual system is destroyed/re-installed. If you use the **DELETE** API without unregistering the client, hosts will reappear the next time the client uploads data.

1. Get the list of system profiles from inventory.

```
# curl -k --user PORTALUSERNAME https://cloud.redhat.com/api/inventory/v1/hosts |  
json_pp > hosts.json
```

2. If the **json_pp** command does not exist on the system then install the **perl-JSON-PP** package.

```
# yum install perl-JSON-PP
```

3. Get the ID of the system from the **hosts.json** file and confirm system details; for example, "id" : "f59716a6-5d64-4901-b65f-788b1aee25cc".

```
# curl -k --user PORTALUSERNAME  
https://cloud.redhat.com/api/inventory/v1/hosts/f59716a6-5d64-4901-b65f-788b1aee25cc
```

4. Delete the system profile using the following command:

```
# curl -k --user PORTALUSERNAME -X "DELETE"  
https://cloud.redhat.com/api/inventory/v1/hosts/f59716a6-5d64-4901-b65f-788b1aee25cc
```

CHAPTER 7. SYSTEM FILTERING AND GROUPS

Insights for Red Hat Enterprise Linux enables administrators to filter systems in inventory and in individual services. Groups are identified by the method of system data ingestion to Insights for RHEL. Insights for RHEL enables filtering groups of systems by those running SAP workloads, by Satellite host group, and by custom filters that are defined by system administrators with root access to configure the Insights client on the system.



NOTE

As of Fall 2020, inventory, advisor, vulnerability, patch, drift, and policies enable filtering by groups. Other services will follow.

Use the global, **Filter Results** box to filter by SAP workloads, Satellite host groups, or custom filters added to the Insights client configuration and file filters added to the Insights client configuration file.

Prerequisites

The following prerequisites and conditions must be met to use the filters features in Insights for Red Hat Enterprise Linux:

- The Insights client is installed and registered on each system.
- To create custom tags, root permissions, or their equivalent, are required to add to or change the `/etc/insights-client/tags.yaml` file.

7.1. SAP WORKLOADS

As Linux becomes the mandatory operating system for SAP ERP workloads in 2025, Red Hat Enterprise Linux and Insights for Red Hat Enterprise Linux are working to make Insights for RHEL the management tool of choice for SAP administrators.

As part of this ongoing effort, Insights for RHEL automatically tags systems running SAP workloads and by SAP ID (SID), without any customization needed by administrators. Users can easily filter those workloads throughout the Insights for RHEL application by using the global **Filter Results** dropdown menu.

7.2. SATELLITE HOST GROUPS

Satellite host groups are configured in Satellite and recognized automatically by Insights.

7.3. CUSTOM SYSTEM TAGGING

By applying custom grouping and tagging to your systems, you can add contextual markers to individual systems, filter by those tags in the Insights for RHEL application, and more easily focus on related systems. This functionality can be especially valuable when deploying Insights for RHEL at scale, with many hundreds or thousands of systems under management.



NOTE

To create custom tags, root permissions, or their equivalent, you are required to add to or change the `/etc/insights-client/tags.yaml` file.

7.3.1. Filter structure

Filters 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.

7.3.2. Creating a custom group and the tags.yaml file

Create and add tags to **/etc/insights-client/tags.yaml** simply by using **insights-client --group=<name-you-choose>**, which performs the following actions:

- Creates the **etc/insights-client/tags.yaml** file
- Adds the **group=** key and **<name-you-choose>** value to **tags.yaml**
- Uploads a fresh archive from the system to the Insights for RHEL application so the new tag is immediately visible along with your latest results

After creating the initial **group** tag, add additional tags as needed by editing the **/etc/insights-client/tags.yaml** file.

The following procedure shows how to create the initial group, as well as the **/etc/insights-client/tags.yaml** file, then verify the tag exists in the Insights for RHEL inventory.

Procedure

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

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

2. Navigate to [Red Hat Insights > Inventory](#) and log in if necessary.
3. Click the **Filter results** dropdown menu.
4. Scroll through the list or use the search function to locate the tag.
5. Click the tag to filter by it.
6. Verify that your system is among the results on the advisor systems list.
7. Navigate to [Red Hat Insights > Inventory](#) and log in if necessary.
8. Activate the **Name** filter and begin typing the system name until you see your system, then select it.
9. Verify that, next to the system name, the tag symbol is darkened and shows a number representing the correct number of tags applied.

7.3.3. Editing tags.yaml to add or change tags

After creating the group filter, edit the contents of `/etc/insights-client/tags.yaml` as needed to add or modify tags. You can add multiple filters 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 values 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 for RHEL.
[root@server ~]# insights-client
5. Navigate to [Red Hat Insights > Inventory](#) and log in if necessary.
6. In the **Filter Results** box, click the down arrow and select one of the filters or enter the name of the filter and select it.
7. Find your system among the results.
8. Verify that the filter icon is darkened and shows a number representing the number of filters applied to the system.

7.4. ADDING FILTERS 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:

- Creates the **etc/insights-client/tags.yaml** file
- Adds the **group** key and <name-you-choose> value to **tags.yaml**
- Uploads a fresh archive from the system to Insights for Red Hat Enterprise Linux application so that the new tag is immediately visible along with your latest results

After creating the initial **group** tag, you 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 for RHEL inventory.

Procedure

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

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

2. Navigate to inventory and log in if necessary.
3. Click the **Filters** dropdown menu and select **Tags**.
4. 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.

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

7.5. 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 can add multiple, filterable tags to a system.



NOTE

Insights for Red Hat Enterprise Linux collects a minimal amount of data, including data that might contain personally identifiable information (PII). Prevent PII (or other configuration data) from being collected by applying data redaction options. For more information about data redaction options for some of your configuration files, see [Insights client data redaction](#) and [Redaction and YAML file use](#).

For information about how Red Hat handles data collection, see [Red Hat Insights Data & Application Security](#).

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: _group-name-value_
location: _location-name-value_
```

```
description:  
- RHEL8  
- SAP  
key 4: value
```

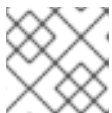
**NOTE**

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 for RHEL.

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

5. Navigate to inventory and log in if necessary.
6. Click the **Filters** dropdown menu and select **Tags**.
7. 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.

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

CHAPTER 8. REFERENCE MATERIALS

To learn more about Insights for Red Hat Enterprise Linux, the following resources might also be of interest:

Documentation

- [Remediating Configuration Issues Using Red Hat Insights and Ansible Playbooks](#)
- [Generating Advisor Service Reports](#)
- [Insights for Red Hat Enterprise Linux Documentation](#)
- [Insights for Red Hat Enterprise Linux Product Support page](#)