Red Hat Insights 2020-10

Assessing RHEL Configuration Issues Using the Red Hat Insights Advisor Service

Assess and monitor the configuration issues impacting your RHEL systems

Last Updated: 2020-11-02

Red Hat Insights 2020-10 Assessing RHEL Configuration Issues Using the Red Hat Insights Advisor Service

Assess and monitor the configuration issues impacting your RHEL systems

Legal Notice

Abstract

Use the Insights Advisor service to assess and monitor configuration issues affecting the availability, stability, performance, and security of your RHEL systems. 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. ASSESSING AND MONITORING RHEL CONFIGURATION ISSUES WITH THE ADVISOR SERVICE

Use the Advisor service to assess and monitor the health of your Red Hat Enterprise Linux (RHEL) infrastructure. Whether your 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 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 Advisor service > 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 application. For more information, see *Remediating Configuration Issues Using Red Hat Insights and Ansible Playbooks*.

CHAPTER 2. ADVISOR SERVICE RECOMMENDATIONS

The Advisor service bundles information about known configuration issues that can negatively affect the *availability*, *stability*, *performance*, or *security* of your RHEL systems. This information set is called a recommendation in the Advisor service (formerly called a rule in Insights) and includes the following information:

- **Description** or name. A concise description of the recommendation
- **Date published.** When the recommendation was published to the Advisor service archive
- **Type of issue.** Whether the issue has the potential to negatively affect the availability, stability, performance, or security of RHEL systems
- **Description.** A brief synopsis of the issue, including how it affects RHEL systems
- **Link to associated topics.** More information from Red Hat about the issue
- **Total risk.** A value derived from the *likelihood* that the condition will negatively affect your infrastructure, and the *impact* on system operations if that were to happen
- **Risk of change.** The risk to operations due to executing the resolution
- **Reboot required.** Whether the resolution requires the system to be rebooted, potentially causing downtime
- **Affected systems.** A list of systems on which the recommendation is detected

2.1. SYSTEM AND RECOMMENDATION PAIRING

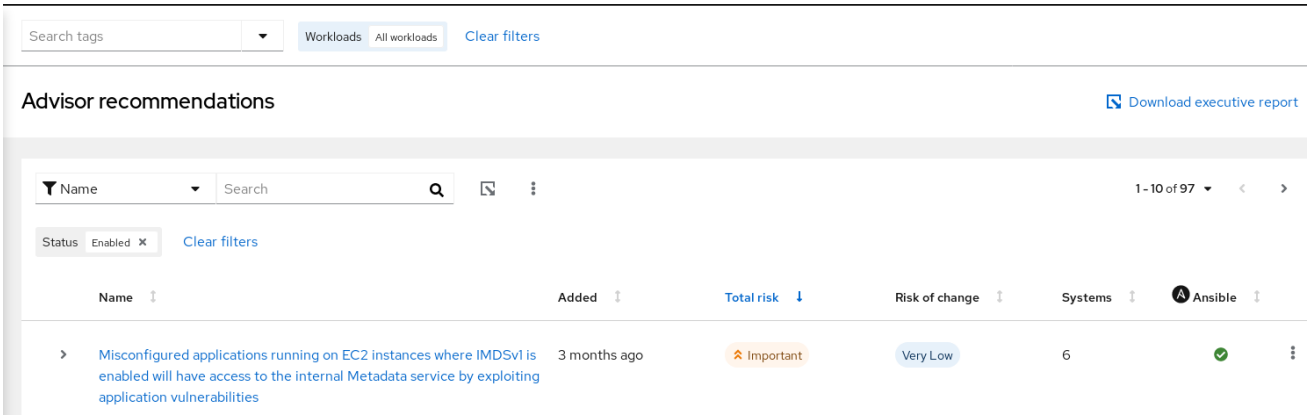
When a recommendation exists on a system, the Advisor service identifies whether, and how, the system has been impacted *and* provides specific mitigation or resolution instructions. This information is visible when viewing a recommendation and then selecting an affected system.

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 Red Hat Insights 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.



3.1. VIEWING ALL ADVISOR RECOMMENDATIONS

The Recommendations view, by default, only displays the recommendations that are detected on your systems. However, you can view *all* of the recommendations in the Advisor archive, and against which your systems are scanned, using the following procedure:

Procedure

1. Navigate to the Advisor service > Recommendations page and log in if necessary.
2. Located above the Recommendations list, click the **more-actions** icon, , and click **Show recommendations with no impacted systems**.
3. To resume viewing only impacting recommendations, click on the **more-actions** icon and click **Hide recommendations with no impacted systems**

3.2. FILTERING RECOMMENDATIONS

Select from the following filters to refine your recommendations list:

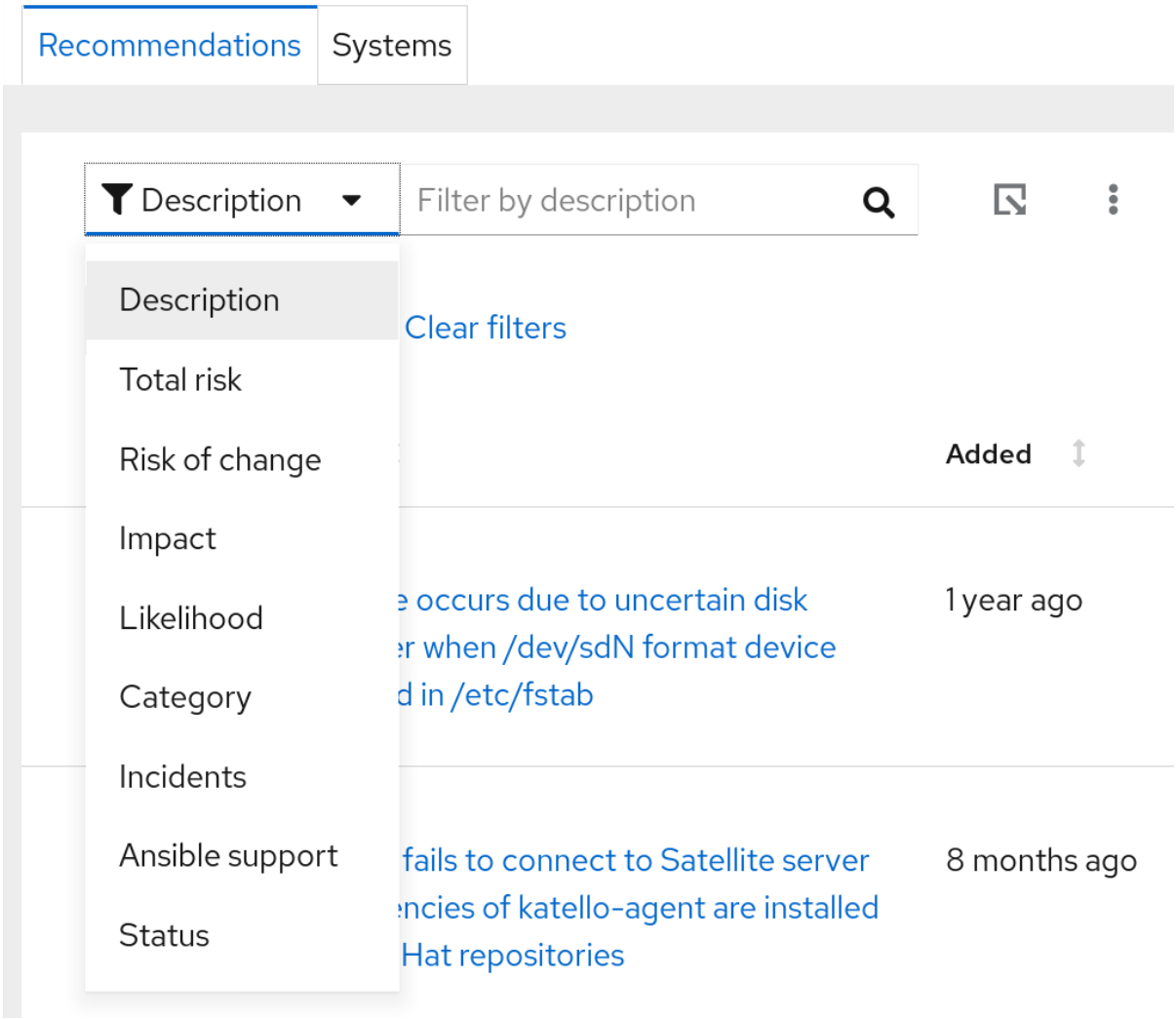
- **Name.** In the subfilter field, start typing the recommendation description or a keyword and select from the options presented.
- **Total risk.** In the subfilter field, select from one or more: Critical, Important, Moderate, or Low.
- **Risk of change.** In the subfilter field, select from High,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

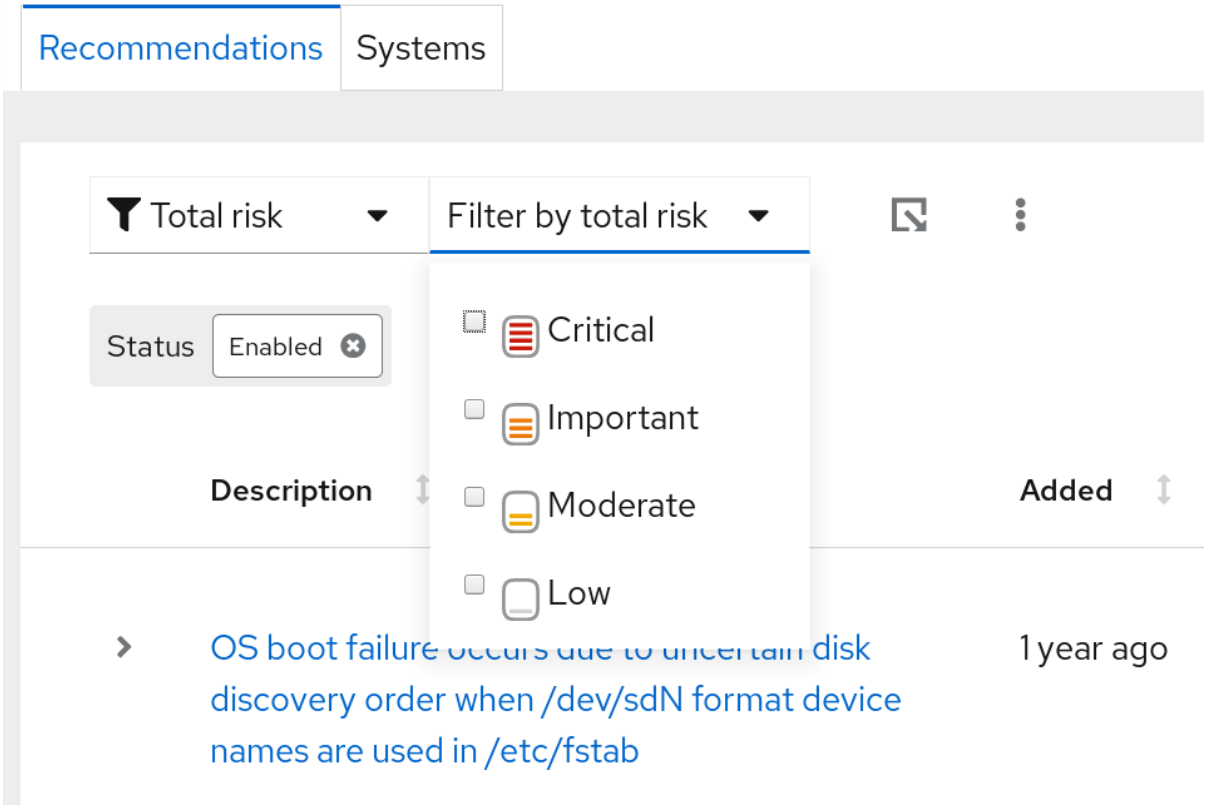
To set filters, complete the following steps:

Procedure

1. Navigate to the Advisor service > 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.



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

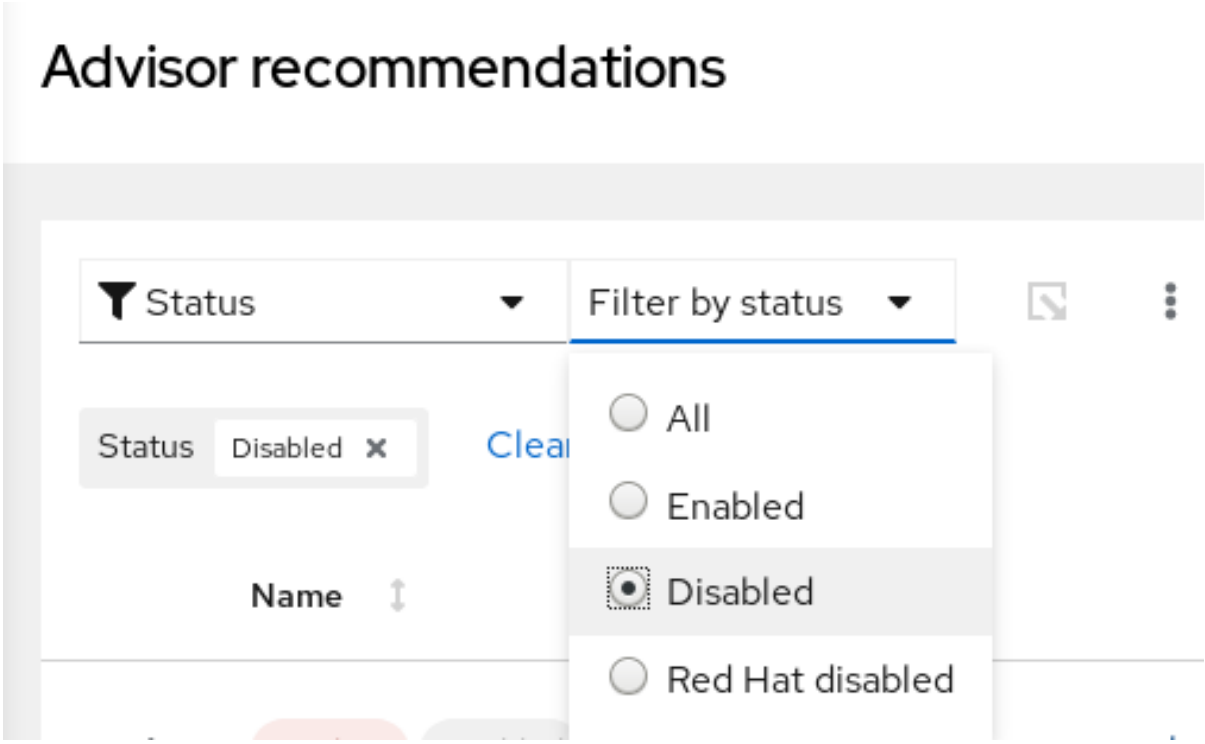
1. Navigate to the Advisor service > Recommendations page and log in if necessary.
2. Locate the recommendation to disable.
3. Click the **more-actions** icon, , at the far right of the row and click **Disable recommendation**.

3.5. VIEWING AND ENABLING A PREVIOUSLY DISABLED RECOMMENDATION

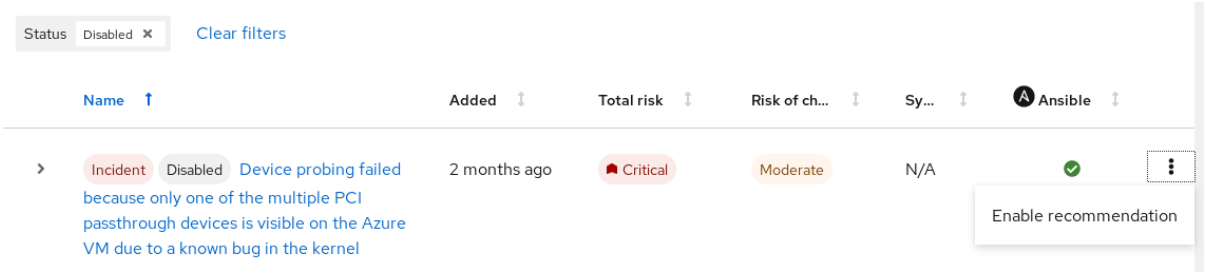
When a recommendation is disabled, you will no longer see the recommendation in your Advisor results. To reverse this action, complete the following steps:

Procedure

1. Navigate to the Advisor service > Recommendations page and log in if necessary.
2. Click the Filter dropdown and select **Status**.
3. In the subfilter dropdown list, select **Disabled**.

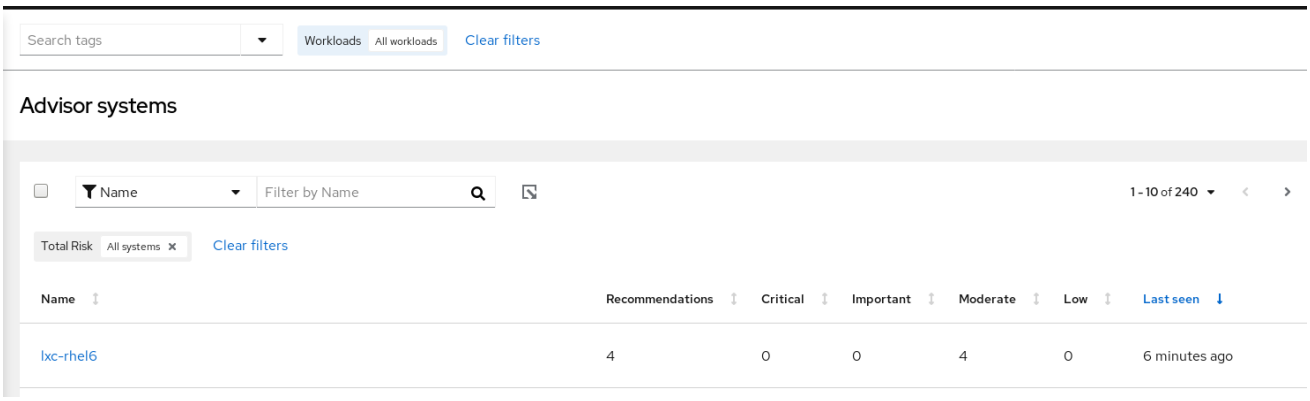


4. Locate the recommendation to enable.
5. Click the **more-actions** icon, , on the right side of the row, and click **Enable recommendation**.



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.



4.1. FILTER BY NAME

Search for the host or system name.

4.2. SORTING OPTIONS

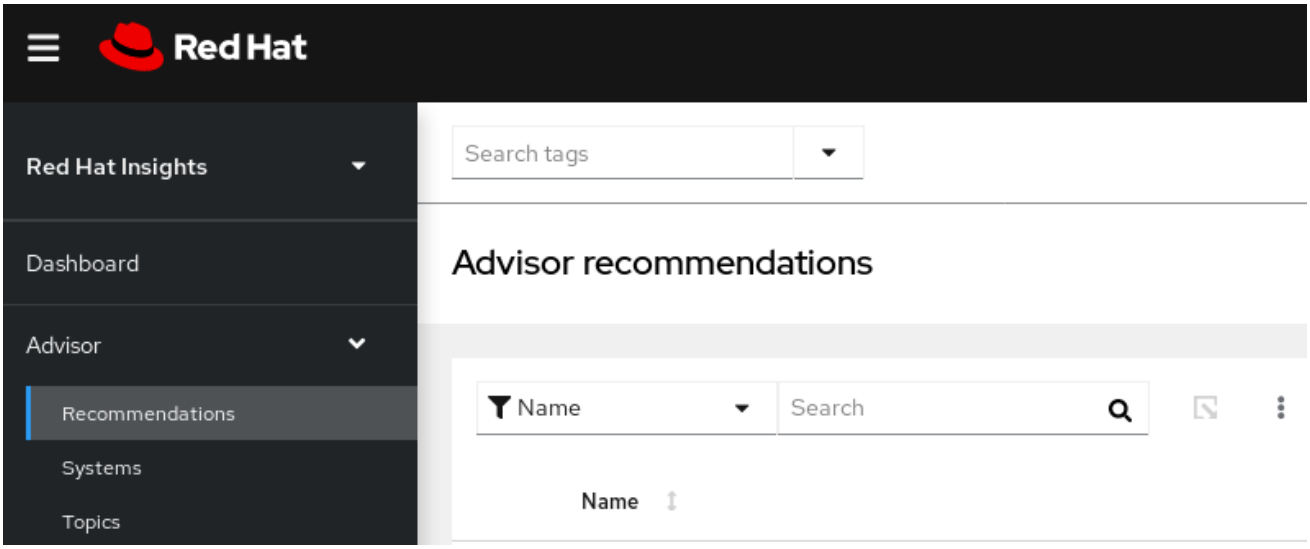
Use the sorting arrows above the following columns to order your systems table:

- **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 **Search tags** box, located in the upper left corner of the page in the Red Hat Insights application.

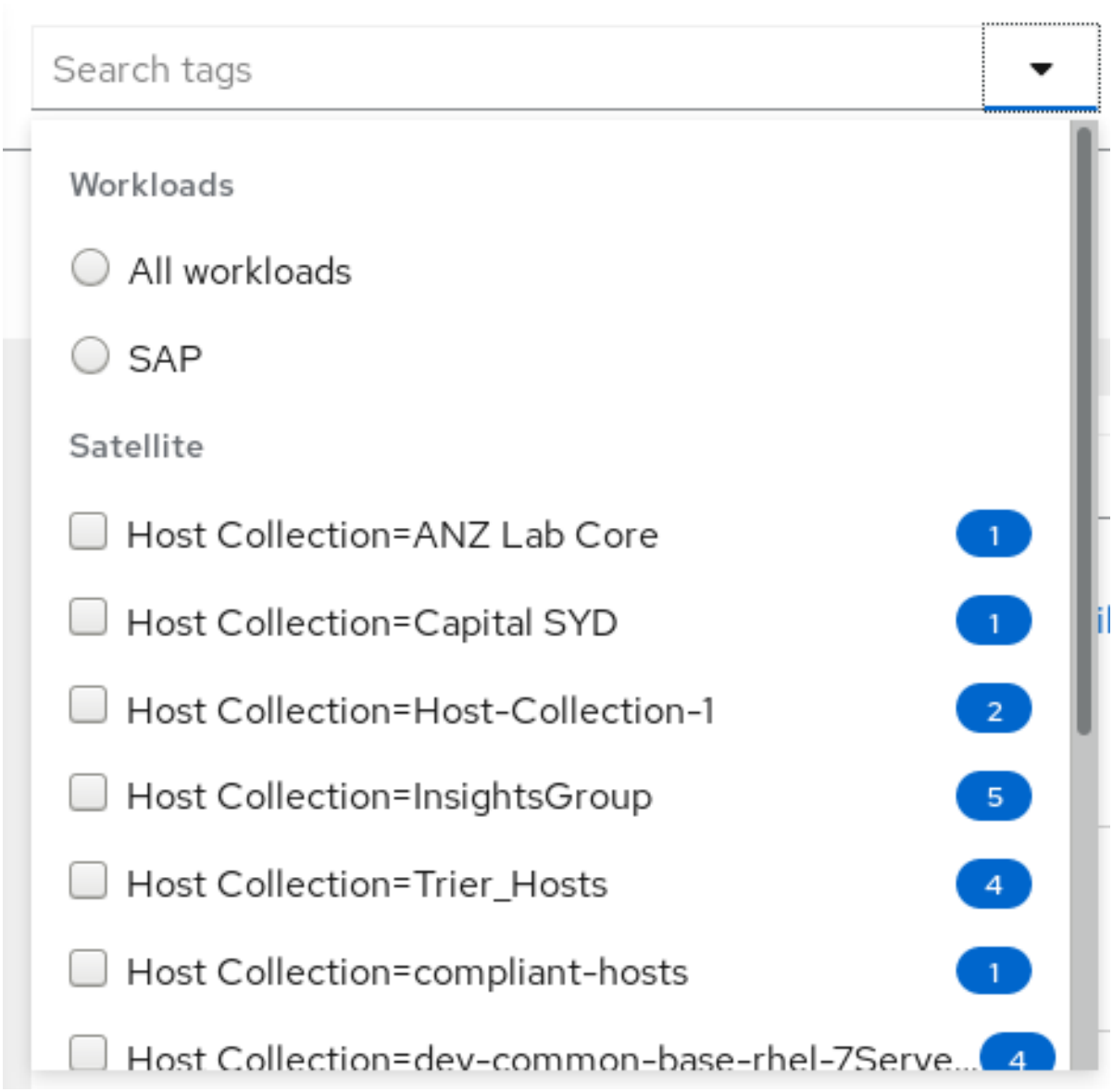


The filter dropdown menu shows all of the tags associated with the account, allowing you to click one or more parameters by which to filter. To filter by tags in the Advisor service, complete the following steps:

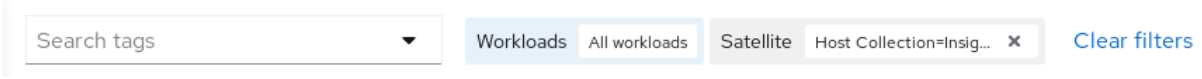
Procedure

1. Navigate to the Advisor service > Systems page and log in if necessary. The **Search tags** box is in most views in the Red Hat Insights application and these procedures work anywhere you access **Search tags**.

2. Click the arrow on the **Search tags** 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 **Search tags** box.



4. View the filtered results throughout the Advisor service.

5. To remove the tag, click **Clear filters**.

CHAPTER 6. DISABLING VISIBILITY OF SATELLITE-MANAGED SYSTEMS IN RED HAT INSIGHTS

With Org-admin privileges, you can choose whether Satellite-managed system results can be viewed in Satellite *and* Insights), or limit visibility to only the Insights tab in Satellite.

By default, this setting is not enabled, and all Insights results for Satellite-managed systems will be visible in both the Satellite integration and on cloud.redhat.com.

This setting can be enabled or disabled at any time by a user account with org-admin privileges. The ability to modify this setting is only supported using an API call, at this time.

Procedure 1:

1. Disable visibility of Satellite-managed systems at cloud.redhat.com/insights.

```
curl -X POST -u [USERNAMEHERE] \
  https://cloud.redhat.com/api/insights/v1/account_setting/ \
  -H 'Content-Type: application/json' \
  -d '{
    "show_satellite_hosts": false
}'
```

Procedure 2:

1. Enable the visibility of Satellite-managed systems at cloud.redhat.com/insights.

```
curl -X POST -u [USERNAMEHERE] \
  https://cloud.redhat.com/api/insights/v1/account_setting/ \
  -H 'Content-Type: application/json' \
  -d '{
    "show_satellite_hosts": true
}'
```

CHAPTER 7. DELETING A SYSTEM FROM INVENTORY

You can delete a system from the cloud.redhat.com inventory so that the system is no longer visible in the Red Hat Insights Inventory or Advisor service Systems list. The Insights client will be unregistered on the system and no longer report data to Red Hat Insights. 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/reinstalled. 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
```

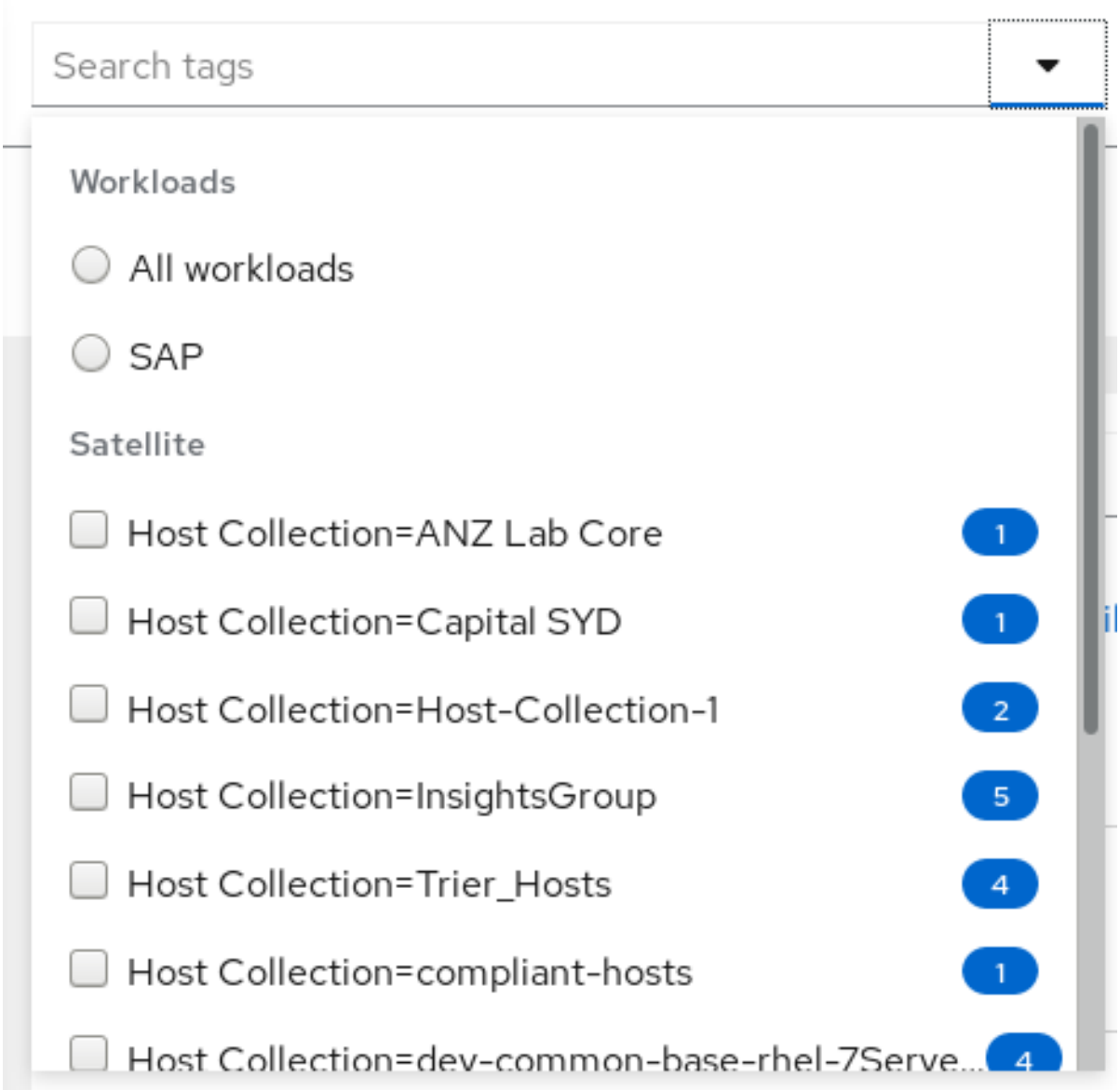
CHAPTER 8. SYSTEM TAGS AND GROUPS

Red Hat Insights enables administrators to filter systems in inventory and in individual services using group tags. Groups are identified by the method of system data ingestion to Insights. Insights enables filtering groups of systems by those running SAP workloads, by Satellite host group, and by custom tags 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 and tags. Other services will follow.

Use the global, **Search tags** box to filter by SAP workloads, Satellite host groups, or custom tags added to the Insights client configuration file.



Prerequisites

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

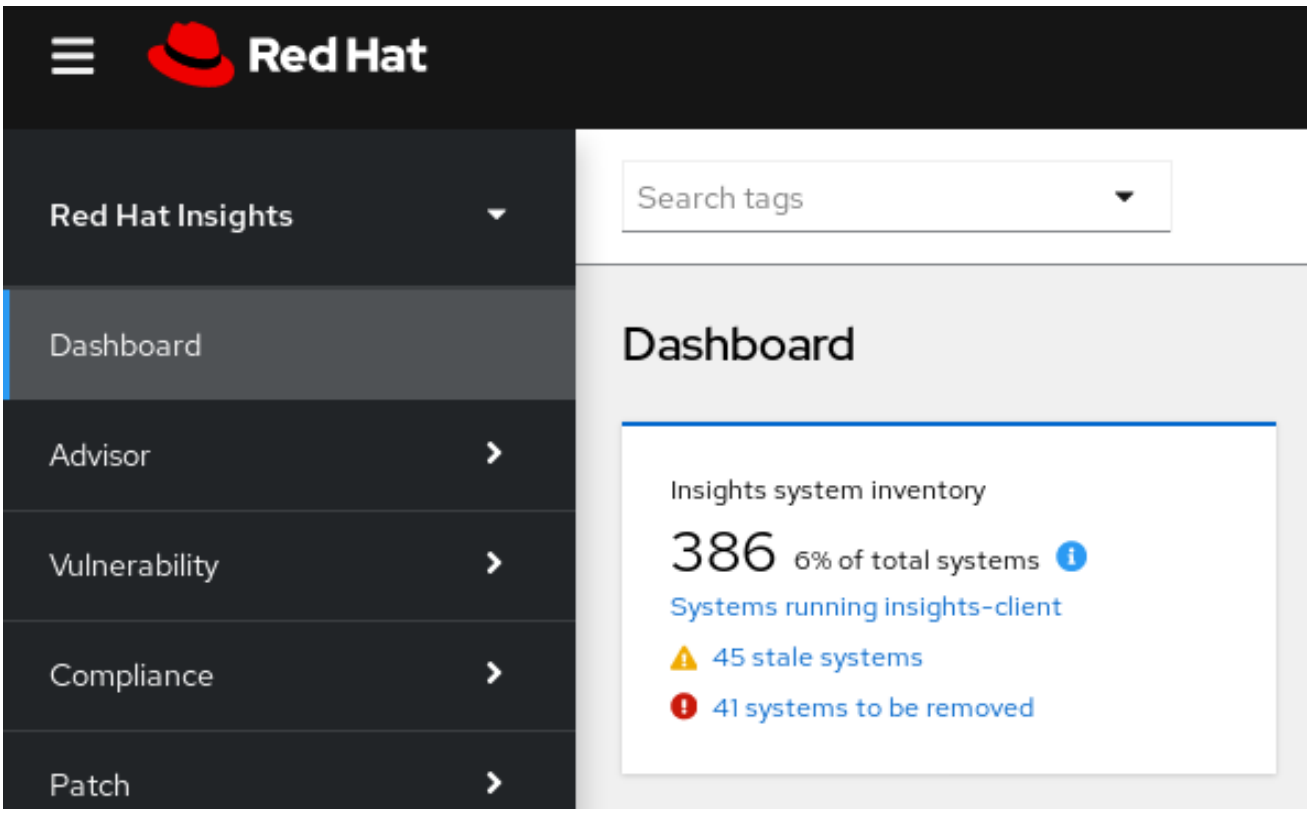
- The Red Hat Insights client is installed and registered on each system.

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

8.1. SAP WORKLOADS

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

As part of this ongoing effort, Insights 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 application by using the global **Search tags** dropdown menu.

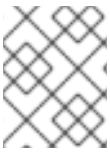


8.2. SATELLITE HOST GROUPS

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

8.3. 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 application, and more easily focus on related systems. This functionality can be especially valuable when deploying Insights at scale, with many hundreds or thousands of systems under management.



NOTE

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

8.3.1. 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.

8.3.2. 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
```

8.3.3. 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 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 inventory.

Procedure

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

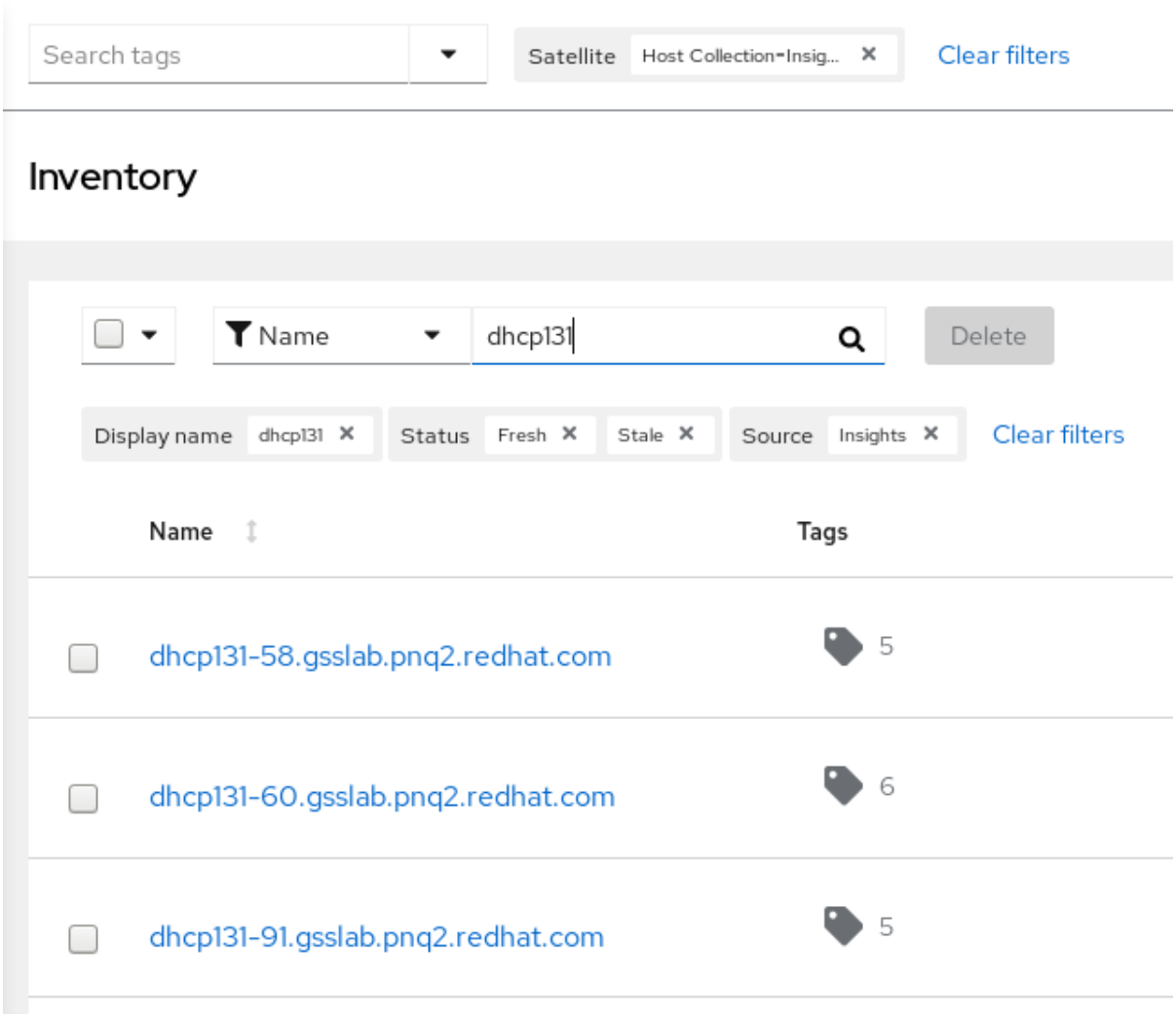
```
[root@server ~]# insights-client --group=<name-you-choose>
```

Verify your custom group was created

1. Navigate to Red Hat Insights > Inventory and log in if necessary.
2. Click the **Search tags** dropdown menu.
3. Scroll through the list or use the search function to locate the tag.
4. Click the tag to filter by it.
5. Verify that your system is among the results on the Advisor systems list.

Verify the system is tagged

1. Navigate to Red Hat Insights > Inventory and log in if necessary.
2. Activate the **Name** filter and begin typing the system name until you see your system, then select it.
3. Verify that, next to the system name, the tag symbol is darkened and shows a number representing the correct number of tags applied.



8.3.4. Editing tags.yaml to add or change tags

After creating the group tag, edit the contents of **/etc/insights-client/tags.yaml** as needed to add or modify tags. You can 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 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
```

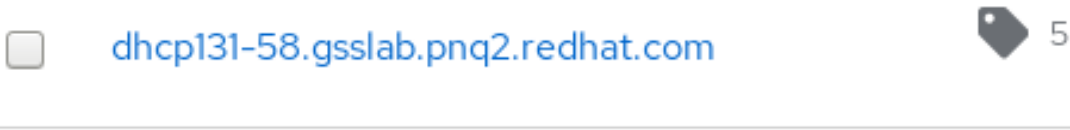
NOTE

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.
   [root@server ~]# insights-client

Verification steps

1. Navigate to Red Hat Insights > Inventory and log in if necessary.
2. In the **Search tags** box, click the down arrow and select one of the tags or enter the name of the tag and select it.
3. Find your system among the results.
4. 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.

CHAPTER 9. REFERENCE MATERIALS

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

Documentation

- *Remediating Configuration Issues Using Red Hat Insights and Ansible Playbooks*
- *Generating Advisor Service Reports*
- Red Hat Insights Documentation
- Red Hat Insights Product Support page