



## Red Hat Insights 2020-04

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

Assess and monitor the configuration issues impacting your RHEL systems



# Red Hat Insights 2020-04 Assessing RHEL Configuration Issues Using the Red Hat Insights Advisor Service

---

Assess and monitor the configuration issues impacting your RHEL systems

## Legal Notice

Copyright © 2020 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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

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

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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. 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](http://cloud.redhat.com)) product and use the Documentation component.

---

## Table of Contents

<b>CHAPTER 1. ASSESSING AND MONITORING RHEL CONFIGURATION ISSUES WITH THE ADVISOR SERVICE</b>	<b>3</b>
<b>CHAPTER 2. ADVISOR RECOMMENDATIONS</b> .....	<b>4</b>
2.1. SYSTEM AND RECOMMENDATION PAIRING	4
<b>CHAPTER 3. REFINING ADVISOR RECOMMENDATIONS TO FOCUS ON YOUR MOST IMPORTANT ISSUES</b> .	<b>5</b>
3.1. MODIFYING THE RECOMMENDATIONS LIST	5
3.1.1. Viewing all Advisor recommendations	5
3.1.2. Setting filters	5
3.1.3. Sorting options	7
3.1.4. Disabling a recommendation	7
3.1.5. View and enable a previously disabled recommendation	7
3.2. MODIFYING THE SYSTEMS VIEW	8
3.2.1. Filter by name	8
3.2.2. Sorting options	8
3.3. DELETING A SYSTEM FROM INVENTORY	8
3.4. DISABLING VISIBILITY OF SATELLITE-MANAGED SYSTEMS IN RED HAT INSIGHTS	9
<b>CHAPTER 4. RED HAT INSIGHTS TAGGING OVERVIEW</b> .....	<b>11</b>
4.1. CREATING TAGS AND TAGS.YAML	11
4.1.1. Tag structure	11
4.1.2. The tags.yaml file	11
4.2. ADDING TAGS TO SYSTEMS	12
4.3. EDITING TAGS.YAML TO ADD OR CHANGE TAGS	13
4.4. FILTERING BY TAGS IN THE ADVISOR SERVICE	14
<b>CHAPTER 5. REFERENCE MATERIALS</b> .....	<b>15</b>
<b>CHAPTER 6. IMPORTANT CHANGES WITH THE 2020-04 RELEASE OF RED HAT INSIGHTS</b> .....	<b>16</b>



# 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 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 client, the client runs daily to check systems against a database of *rules*, now called **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 (formerly called *rules*) for your entire RHEL infrastructure.
- Use robust filtering capabilities to refine your views to the systems of greatest concern to you.
- Learn more about individual recommendations, details about the risks they pose, 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 RECOMMENDATIONS

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

- **Description** or name. A concise description of the recommendation
- **Date published.** When the recommendation was published to the Advisor service archive
- Link to associated **knowledgebase articles.** 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 operation if that were to happen
- **Risk of change.** The risk to operations inherent in 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 offers even deeper knowledge of how that recommendation is impacting that specific system, including how it is manifesting and how to resolve it. This information is visible when viewing a recommendation and then selecting an affected system.

When an impacted system is selected, you can see each recommendation on 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 RECOMMENDATIONS TO FOCUS ON YOUR MOST IMPORTANT ISSUES

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 and systems from your Advisor results.

### 3.1. MODIFYING THE RECOMMENDATIONS LIST

#### 3.1.1. Viewing all Advisor recommendations

The Recommendations view, by default, only shows you the recommendations impacting your systems.

To see *all* of the recommendations in the Advisor archive, and against which your systems are scanned, complete 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 (three vertical dots) and click **Show recommendations with no impacted systems**
3. To return to the view of only seeing impacting recommendations, click on the more-actions icon again and click **Hide recommendations with no impacted systems**

#### 3.1.2. Setting filters

You can set a variety of filters to refine your recommendations list. The filters include:

- **Description.** 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.

The screenshot shows the 'Recommendations' tab selected in a navigation bar. Below it, a filter dropdown menu is open, displaying a list of filter categories. The 'Description' category is currently selected. The background shows a table of recommendations with columns for description, risk, and added date.

Filter Category	Filter Value	Added
Description	Filter by description	
Total risk		
Risk of change		Added ↑
Impact		
Likelihood	... occurs due to uncertain disk ... when /dev/sdN format device ... in /etc/fstab	1 year ago
Category		
Incidents		
Ansible support	... fails to connect to Satellite server ...encies of katello-agent are installed	8 months ago
Status	... Hat repositories	

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 a web interface. At the top, there are two tabs: 'Recommendations' (active) and 'Systems'. Below the tabs, there is a header area with a 'Total risk' dropdown menu and a 'Filter by total risk' dropdown menu. The 'Filter by total risk' menu is open, showing four options: 'Critical', 'Important', 'Moderate', and 'Low'. Each option has a corresponding icon and a checkbox. To the left of the filter menu, there is a 'Status' dropdown menu set to 'Enabled'. Below the filter menu, there is a table with columns for 'Description' and 'Added'. The 'Description' column contains 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'.

### 3.1.3. Sorting options

You can order 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:

- **Description.** Alphabetize by A to Z or reverse.
- **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.

### 3.1.4. Disabling a recommendation

Insight allows you to 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 (three vertical dots) at the far right of the row and click **Disable recommendation**.

### 3.1.5. View and enable 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 (three verticle dots) on the right side of the row, and click **Enable recommendation**.

## 3.2. MODIFYING THE SYSTEMS VIEW

The Systems tab 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.

### 3.2.1. Filter by name

Search for the host or system name.

### 3.2.2. 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.

## 3.3. 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
```

## 3.4. DISABLING VISIBILITY OF SATELLITE-MANAGED SYSTEMS IN RED HAT INSIGHTS



### NOTE

The following procedure can only be performed by a user account with org-admin privileges and is only available by using API calls.

Red Hat Insights offers multiple options for viewing results for systems that are managed by Satellite and are registered to Red Hat Insights. The Insights results for these systems can either be viewed only using the Satellite they are managed by, or these results can be available using Satellite and additionally using the Insights application on cloud.redhat.com.

As an org admin, you can choose whether to show Satellite-managed systems in both places (Satellite and Insights) or limit viewing the Insights results for Satellite-managed systems only using the Insights UI 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/insights.

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](https://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](https://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 4. 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.

## 4.1. CREATING TAGS AND TAGS.YAML

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

### 4.1.1. 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.

### 4.1.2. 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
```

## 4.2. 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.

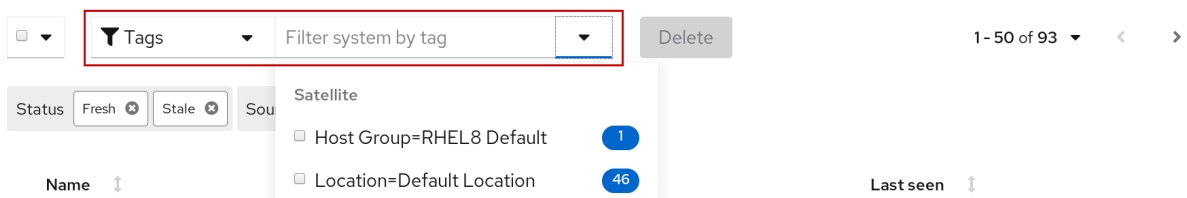
### Procedure

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.



- 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.

Name ↓	Tags	Last seen ↓
<input type="checkbox"/> <a href="#">rhel8desktop</a>	 5	1 hour ago
<input type="checkbox"/> <a href="#">ml.cockpit.lan</a>	 0	4 hours ago

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

### 4.3. 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.

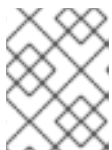
#### Procedure

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

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

- 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.

- Save your changes and close the editor.
- Generate an upload to Insights.

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

#### Verification steps

- Navigate to [Red Hat Insights > Inventory](#) and log in if necessary.
- Click the **Filters** dropdown menu and select **Tags**.
- 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.

## 4.4. FILTERING BY TAGS IN THE ADVISOR SERVICE

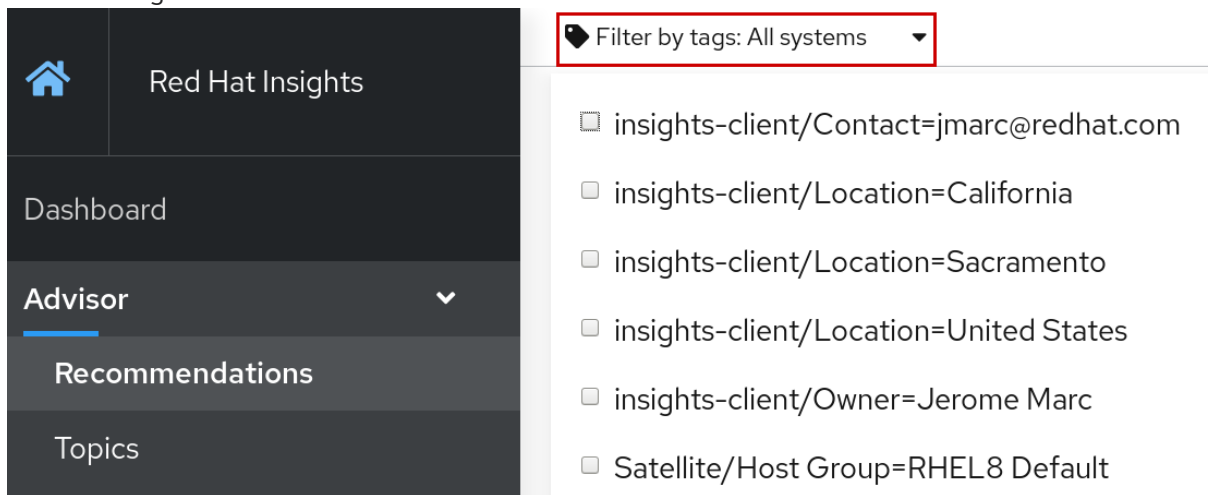
After adding system tags to `etc/insights-client/tags.yaml`, you can filter systems lists by those tags in the Advisor service, enabling you to quickly locate and view the systems you want to focus on.

In the Advisor service, tag filtering is accessible from the Recommendations and the Systems views. 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 > Recommendations](#) page and log in if necessary.
2. In the Recommendations view, click **Filter by tags: All systems** and select one or more of the available tags.



3. You will only see results from a system or systems with that tag. To remove the tag, click **Filter by tags:** and clear the check box.

## CHAPTER 5. 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](#)

## CHAPTER 6. IMPORTANT CHANGES WITH THE 2020-04 RELEASE OF RED HAT INSIGHTS

The 2020-04 release of Red Hat Insights includes significant changes to the application features and services.

### Changes to the Red Hat Insights application

The Red Hat Insights application now includes the services that were previously bundled with the Cloud Management Services for RHEL application, and were part of the Red Hat Smart Management bundle, along with Red Hat Satellite.

The former cloud management services, plus a couple of new services, are now included in the value that Insights brings to each Red Hat Enterprise Linux (RHEL) subscription.

### Insights Advisor

The tools and capabilities that constituted Red Hat Insights prior to this release are now available as the **Advisor** service. The *rules* that have always been the currency of Insights are now called **Advisor Recommendations**.

### Insights security rules have moved

The CVE security rules that were previously curated by the Insights rules team are now included with all other Red Hat CVEs in the Vulnerability service. Security rules are high profile CVEs, some of which have been through the Customer Security Awareness Program. They are identifiable in the Vulnerability service by a security rule icon. You can also filter security rules in the Vulnerability service.

### Services included with Red Hat Insights

The services included with Red Hat Insights in the 2020-04 release are:

- **Advisor.** Identify and fix configuration issues that can negatively impact the availability, performance, stability, and security of RHEL systems.
- **Vulnerability.** Assess and monitor the exposure of your RHEL environment to CVEs and security rules.
- **Compliance.** Assess and monitor the compliance of your RHEL systems with SCAP security policies.
- **Patch.** Enable consistent patch workflows for RHEL systems across the open hybrid cloud.
- **Drift.** Compare system configurations of a system over time, or to other systems and baselines, to identify discrepancies in your environment and perform drift analysis.
- **Policies.** Evaluate and react to system configuration changes in your environment.

The integrated tools that work with each of the services above are:

- **Inventory.** Topological inventory of RHEL systems under Red Hat Insights management
- **Remediations.** Repository of Ansible Playbooks that you create and manage using Red Hat Insights
- **Subscription Watch.** Comprehensive, product-by-product, account-level subscription reporting service across hybrid cloud deployments

## Resources

- [Red Hat Insights Product Support page](#)
- [Red Hat Insights Documentation](#)
- [Red Hat Insights Release Notes](#)
- [Red Hat Insights blog channel](#)