Red Hat Insights 2020-10

Assessing and Monitoring Security Vulnerabilities on RHEL Systems

Understanding your Environmental Exposure to Potential Security Threats

Last Updated: 2020-11-02

Red Hat Insights 2020-10 Assessing and Monitoring Security Vulnerabilities on RHEL Systems

Understanding your Environmental Exposure to Potential Security Threats

Legal Notice

Abstract

Use the Vulnerability service to assess and monitor the status of security vulnerabilities on your RHEL systems, understand the level of exposure of your infrastructure, and plan a course of action. 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. VULNERABILITY SERVICE OVERVIEW

The Vulnerability service enables quick assessment and efficient monitoring of the exposure of your RHEL infrastructure to Common Vulnerabilities and Exposures (CVEs) so you can better understand your most critical issues and systems and effectively manage remediations.

With your data uploaded to the Vulnerability service, you can filter and sort groups of systems and CVEs to optimize your views. You can also add context to individual CVEs when they pose an extraordinary risk to systems.

After gaining an understanding of your risk exposure, create Ansible Playbooks to remediate issues to secure your organization and report on the status of the CVEs to appropriate stakeholders. For more information about remediations and reporting, see the following documentation:

- *Remediating Security Exposures using Vulnerability and Ansible Playbooks*
- *Generating Vulnerability Reports*

1.1. VULNERABILITY SERVICE REQUIREMENTS AND PREREQUISITES

The Vulnerability service is available for all supported versions of RHEL 6, 7, and 8. The following conditions must be met before you can use the Vulnerability service:

- **Each system has the Insights client installed and registered to the Insights application.** Follow the Get Started instructions to install the client and register your system(s).
- **The Vulnerability service is fully supported for RHEL systems managed by Red Hat Subscription Manager (RHSM) and Satellite 6 and later.** Using any other means to obtain package updates, other than Satellite 6 with RHSM or RHSM registered with subscription.redhat.com (Customer Portal), can lead to misleading results.
- **Vulnerability service remediations are not fully supported and may not work properly on Satellite 5 and Spacewalk-hosted RHEL systems.**
- **Some features require special privileges provided by your org admin.**Specifically, the ability to view Red Hat Security Advisories (RHSA) associated with certain CVEs and systems, and to view and patch those vulnerabilities in the Insights Patch service, requires permissions granted through User Access.

CHAPTER 2. COMMON VULNERABILITIES AND EXPOSURES (CVES)

Common Vulnerabilities and Exposures (CVEs) are security vulnerabilities identified in publicly released software packages. CVEs are identified and listed by the National Cybersecurity FFRDC (NCF), the federally funded research and development center operated by the Mitre Corporation, with funding from the National Cyber Security Division of the United States Department of Homeland Security. The complete list of CVEs is available at https://cve.mitre.org.

The Vulnerability service identifies CVEs impacting your RHEL systems and gives you the information you need to understand their potential risk and how to resolve them.

2.1. SECURITY RULES

What is a security rule and what is its significance?

Security rules are CVEs deemed worthy of additional visibility due to the risk and exposure associated with them and are written by Red Hat to help you configure your systems. Addressing systems with security rules should be considered highest priority.

Security rules are flaws that usually get significant coverage in the press. These CVEs have been scrutinized by the Red Hat Product Security team, which uses the Customer Security Awareness (CSAw) Program workflow to manually create algorithms to help determine your RHEL environment exposure, enabling you to take the appropriate action to protect your organization.

If the Vulnerability service identifies a system or systems as being exposed to a security rule, there is the potential for elevated security risk on those systems and issues should be addressed with urgency.

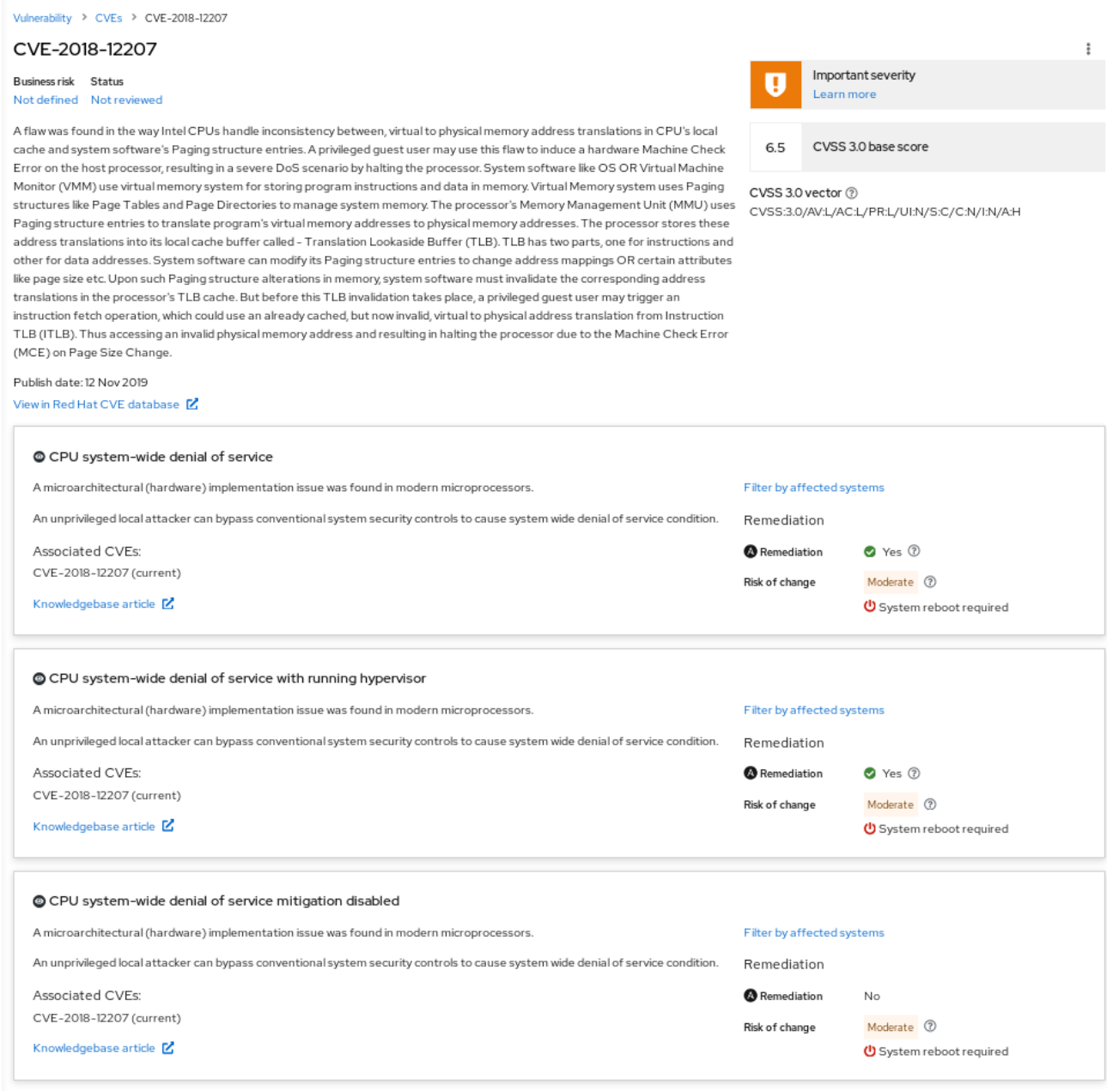
NOTE

Not all systems that are exposed to a given CVE will be exposed to a security rule associated with that CVE. While a CVE may be applicable to 10 systems, the number of systems exposed to a security rule for that CVE, if one exists, can be a subset of the 10 systems.

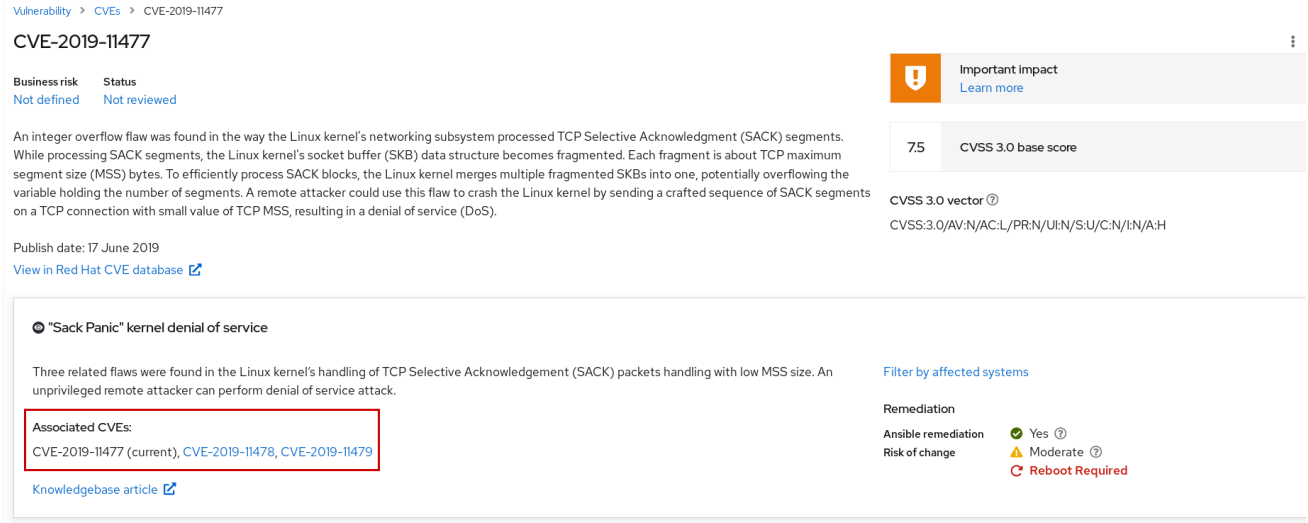
Where can I find Security rules?

The CVEs that have security rules are identifiable by the security-rule icon located to the left of the CVE ID, as well as next to systems that have current security rule vulnerabilities.

A CVE can have multiple security rules associated with it and the opposite is also true. If a CVE has multiple security rules, it is reflected in the CVE details view. A CVE with multiple security rules is shown in the following example:



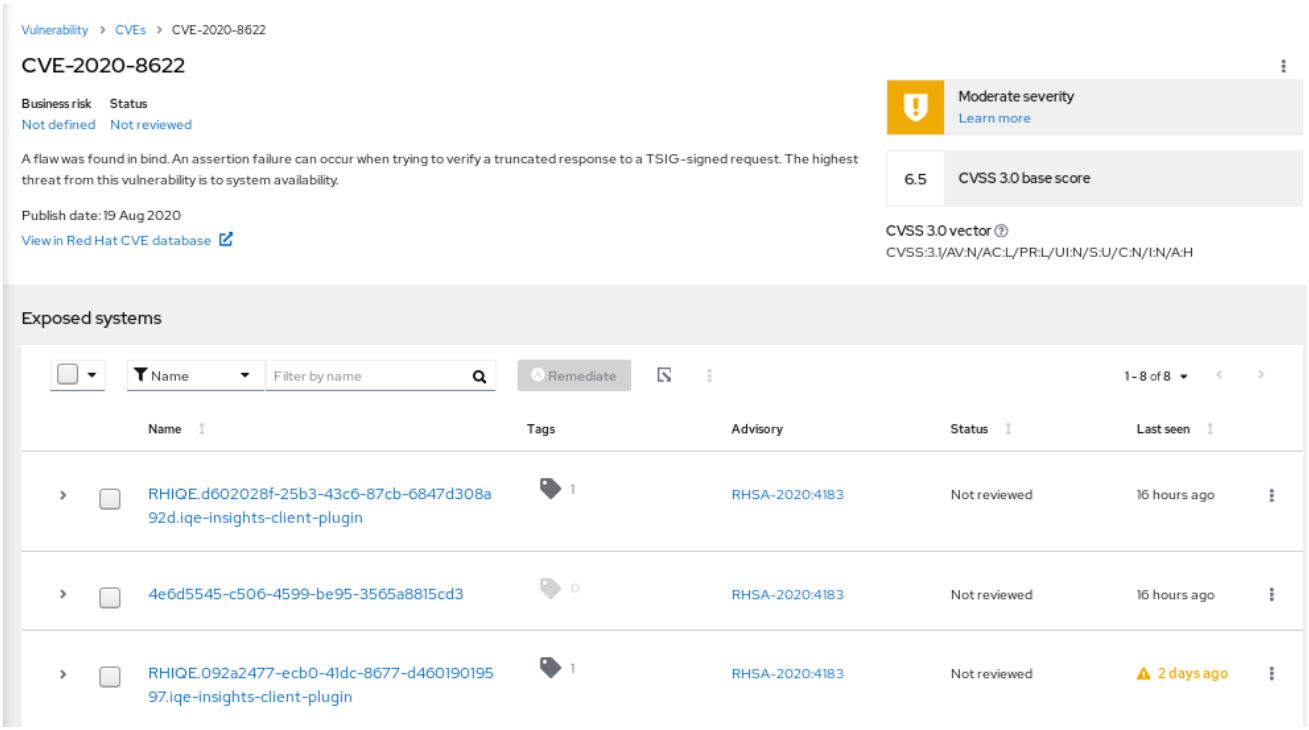
If a security rule has multiple CVEs associated to it, it will be visible as follows:



2.2. RED HAT SECURITY ADVISORIES (RHSAS)

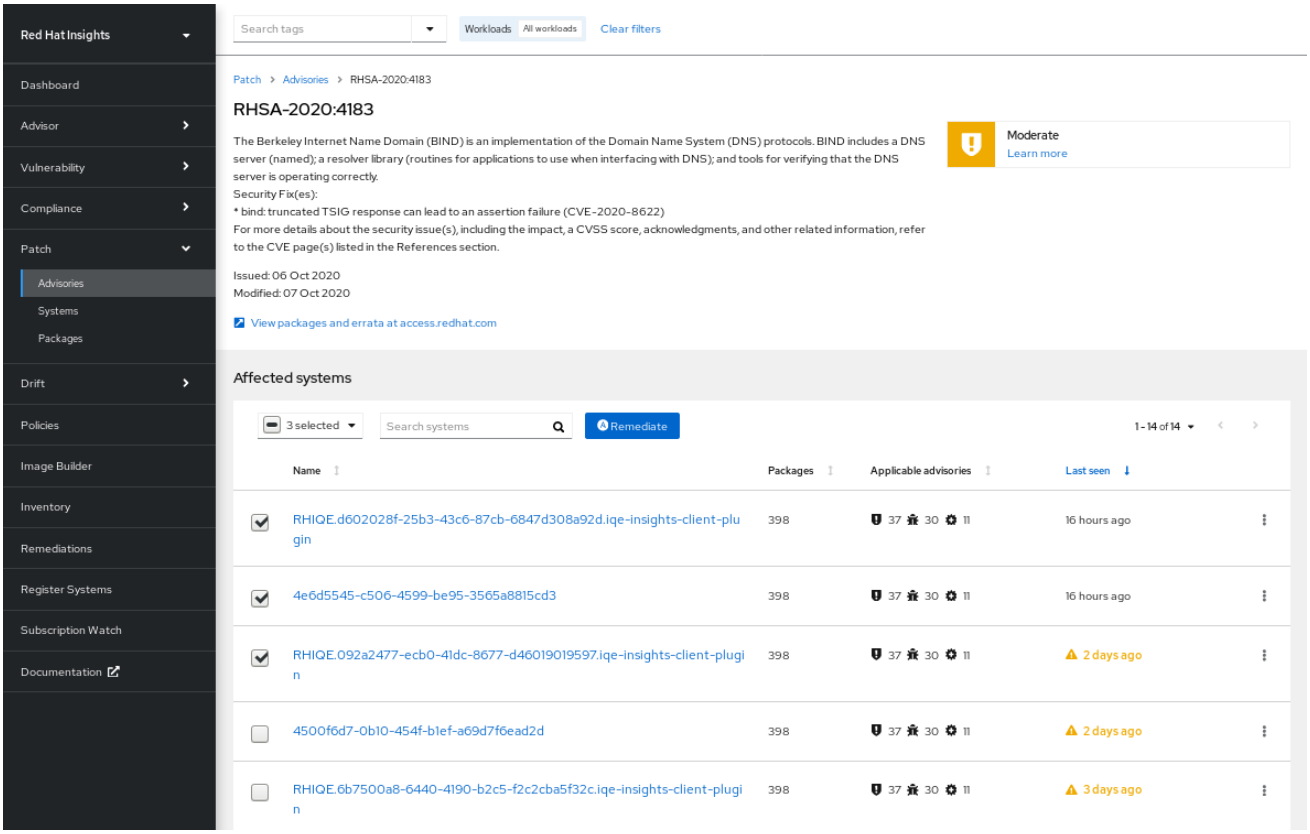
Red Hat Security Advisories (RHSAs) document the security flaws being fixed in Red Hat products. The Vulnerability service enables those users with the appropriate user access to see which advisory is tied to the systems exposed to a given CVE.

This information, if available, is displayed when selecting a CVE and viewing the information in the **Exposed systems** list. If an advisory exists for the system, an **Advisory** column is visible in the list with a link to the RHSA ID next to the system.



When there are no such advisories, the Advisory column is not visible, or only some system rows show an RHSA ID or will show **Not available** if an advisory is not available.

When an advisory exists for a system, you can click on the RHSA ID, which then takes you to the Insights Patch service where you can view more information about the RHSA, including a list of affected systems. In the Patch service, select systems to create an Ansible Playbook to apply the remediation.


Red Hat Insights
Dashboard
Advisor
Vulnerability
Compliance
Patch
Advisories
Systems
Packages
Drift
Policies
Image Builder
Inventory
Remediations
Register Systems
Subscription Watch
Documentation
Search tags
Workloads
All workloads
Clear filters
Patch > Advisories > RHSA-2020:4183
RHSA-2020:4183
The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.
Security Fix(es):
* bind: truncated TSIG response can lead to an assertion failure (CVE-2020-8622)
For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.
Issued: 06 Oct 2020
Modified: 07 Oct 2020
View packages and errata at access.redhat.com
Moderate
Learn more
Affected systems
3 selected
Search systems
Remediate
1 - 14 of 14
Name
Packages
Applicable advisories
Last seen
RHIQE.d602028f-25b3-43c6-87cb-6847d308a92d.iqe-insights-client-plugin
398
37 30 11
16 hours ago
4e6d5545-c506-4599-be95-3565a8815cd3
398
37 30 11
16 hours ago
RHIQE.092a2477-ecb0-41dc-8677-d46019019597.iqe-insights-client-plugin
398
37 30 11
2 days ago
4500f6d7-0b10-454f-b1ef-a69d7f6ead2d
398
37 30 11
2 days ago
RHIQE.6b7500a8-6440-4190-b2c5-f2c2cba5f32c.iqe-insights-client-plugin
398
37 30 11
3 days ago

CHAPTER 3. VIEWING AND TRIAGING THE SECURITY VULNERABILITIES IMPACTING YOUR RHEL SYSTEMS

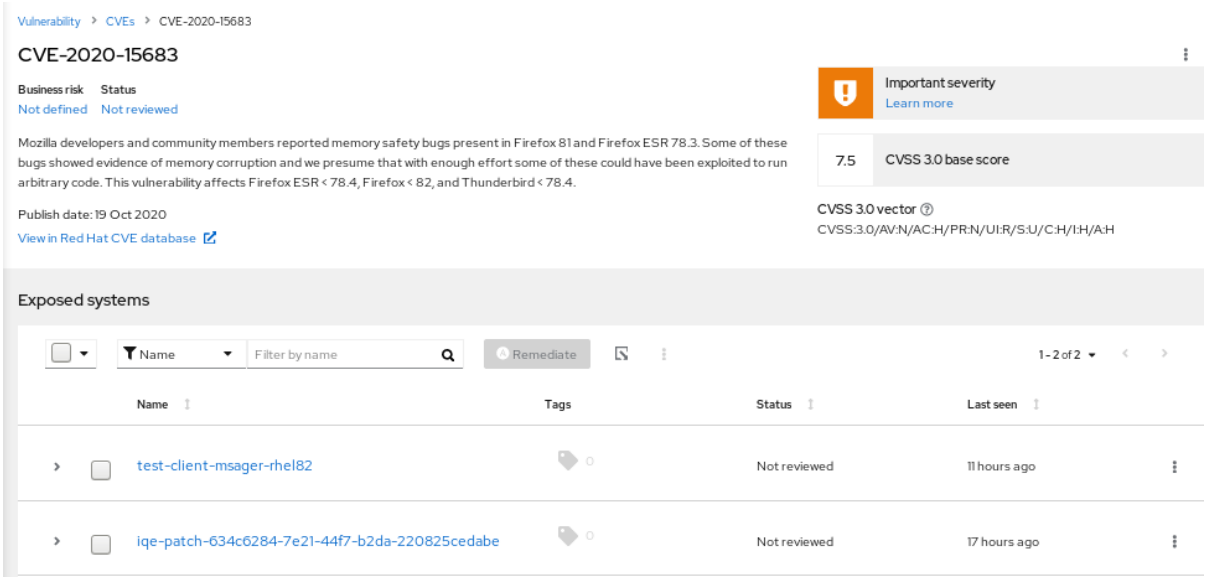
To view the CVEs impacting your RHEL systems, there are two approaches that you can use:

3.1. VIEW A LIST OF CVES IMPACTING YOUR SYSTEMS

Complete the following steps to view a list of CVEs impacting your systems:

Procedure

1. Navigate to the Vulnerability service > CVEs page and log in if necessary.
2. Optionally, apply filters or sort results to refine your CVEs list.
3. Click on a CVE to view the following information:



   a. Business risk
   b. Status
   c. Description
   d. Links to more information
   e. Impact severity rating
   f. Common Vulnerability Scoring System (CVSS 3.0) base score
   g. CVSS 3.0 vector data
   h. Exposed systems
4. Scroll down to view the list of impacted systems with exposure to that CVE.
5. Click on a system to view information about that system, all impacting CVEs, and to select CVEs to remediate with Ansible.

3.2. VIEW A LIST OF SYSTEMS AND THE CVES IMPACTING EACH SYSTEM

Complete the following steps to view a list of systems and the CVEs impacting each one:

Procedure

1. Navigate to Vulnerability service > Systems and log in if necessary.
2. Click on a system to view system information and a list of CVEs to which the system is exposed.
3. Optionally, apply filters or sort results to refine your view of impacting CVEs.
4. Select an individual CVE to see detailed information about it.

CHAPTER 4. REFINING VULNERABILITY RESULTS

The Vulnerability service enables many ways to refine the views of your data, helping you focus on your most critical systems, workloads, or issues. The following sections describe the organization of your data and the sorting, filtering, and contextual features you can use to refine and enrich your results.

4.1. INSIGHTS SYSTEM GROUP FILTERS

The ability to filter Vulnerability service results by groups of systems or workloads enables users to view only those systems tagged as belonging to a specific group. These can be systems running SAP workloads (or by SAP ID), by Satellite host groups, or by custom tags added to the Insights client configuration file.

Group filtering can be set globally in Insights using the **Search tags** box located at the top of the page throughout most of the Insights application. However, the functionality varies within the different Insights services.

Within the Vulnerability service, group filtering is most effective in systems list views. These are accessible from Vulnerability service > Systems , and in the details view for a specific CVE.

NOTE

System group and workload filtering from the Insights Dashboard and Vulnerability service > Reports is a work in progress. For the best user experience, view filtered system group and workload results from systems lists.

Learn more about group tags and configuring custom tags in *Tags and system groups* section of this document.

4.1.1. Filtering Systems lists by group

Use the following procedure to filter Vulnerability service systems lists by group.

Procedure

1. Navigate to the Vulnerability service > Systems page and log in if necessary.
2. Click the down arrow on the Search tags box located at the top of the page.

3. Select whether to limit visibility to SAP Workloads.
4. Search or scroll to view other available tags. To view the full list of available tags, scroll to the bottom of the list and click **View more**.
   a. In the pop-up card, locate the tag or tags by which to filter in the **All tags** tab, or select the **All SAP IDs (SID)**tab, clicking the check box next to each tag you wish to apply.
   b. Click **Apply selected**.
5. Returning to the Systems page, view only systems belonging to the group(s) or workloads you selected.

4.1.2. Filtering systems list in a CVE details view

Use the following procedure to filter the list of exposed systems for a specific CVE.

Procedure

1. Navigate to the Vulnerability service > CVEs page and log in if necessary.
2. Locate the CVE and click on the CVE ID.
3. Click the down arrow on the Search tags box located at the top of the page.

4. Select whether to limit visibility to SAP Workloads.
5. Search or scroll to view other available tags. To view the full list of available tags, scroll to the bottom of the list and click **View more**.
    a. In the pop-up card, locate the tag or tags by which to filter in the **All tags** tab, or select the **All SAP IDs (SID)**tab, clicking the check box next to each tag you wish to apply.
    b. Click **Apply selected**.
6. Returning to the Systems page, view only systems belonging to the group(s) or workloads you selected.

4.2. VULNERABILITY SERVICE FILTERS

Access filters from the CVEs list and, after clicking an individual CVE ID, from the list of affected systems. Filtering will narrow the visible list of CVEs and help you focus on the issues you're most interested in. When you select filters, they are visible below the Filters menu. Click on the **X** on a filter to remove it, or click **Clear filters** to remove all current filters.

The following primary filters are accessible from the CVEs page. Select the primary filter, then define a parameter in the subfilter:

- **CVE.** Search ID or description.
- **Security rules.** Show only CVEs with security rules.
- **Severity.** Select one or more values: Critical, Important, Moderate, Low, or Unknown.
- **CVSS base score.** Select one or more ranges: All, 0.0-3.9, 4.0-7.9, 8.0-10.0, N/A (not applicable)
- **Business risk.** Select one or more values: High, Medium, Low, Not defined.

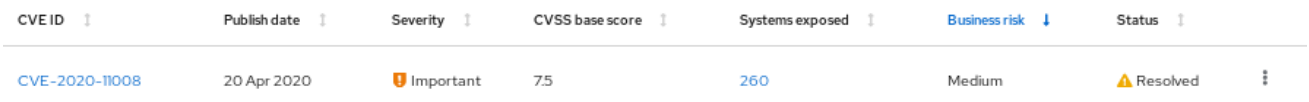
- **Status.** Select one or more values: Not reviewed, In review, On-hold, Scheduled for patch, Resolved, No action - risk accepted, Resolved via mitigation.
- **Publish date.** Select from All, Last 7 days, Last 30 days, Last 90 days, Last year, or More than 1 year ago.
- **Affects systems.** Select from Systems are affected or Systems are not affected.

4.3. DEFINING A BUSINESS RISK FOR A CVE

The Vulnerability service allows you to define the business risk of a CVE with the following options: High, Medium, Low, or Not Defined (default).

While the list of CVEs shows the severity of each CVE, assigning a business risk lets you rank CVEs based on the impact they could have on your organization. This can give you more control in managing your risk efficiently in a large environment, and enable you to make better operational decisions.

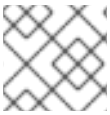
By default, the business risk field for a specific CVE is set to **Not Defined**. After you set the business risk, it is visible in the Vulnerability service > CVEs list, in the CVE row.



Business risk is also visible on the details card for each CVE, which shows more information and lists affected systems.

Procedure for setting a business risk for a single CVE

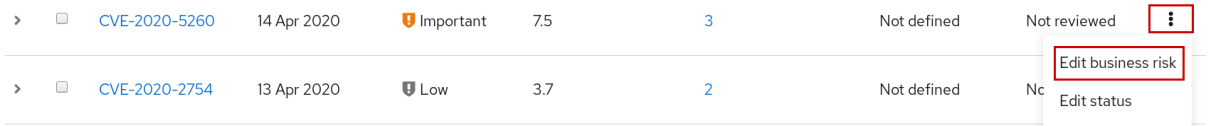
Complete the following steps to set the business risk for a single CVE:



NOTE

The business risk for that CVE will be the same on *all* systems impacted by it.

1. Navigate to the Vulnerability service > CVEs tab and log in if necessary.
2. Identify a CVE for which you want to set a business risk.
3. Click the **more-actions** icon (three vertical dots) on the right end of the CVE row and click **Edit business risk**.



4. Set a business risk value to the appropriate level and, optionally, add a justification for your risk assessment.

5. Click **Save**.

Procedure for setting a business risk for multiple CVEs

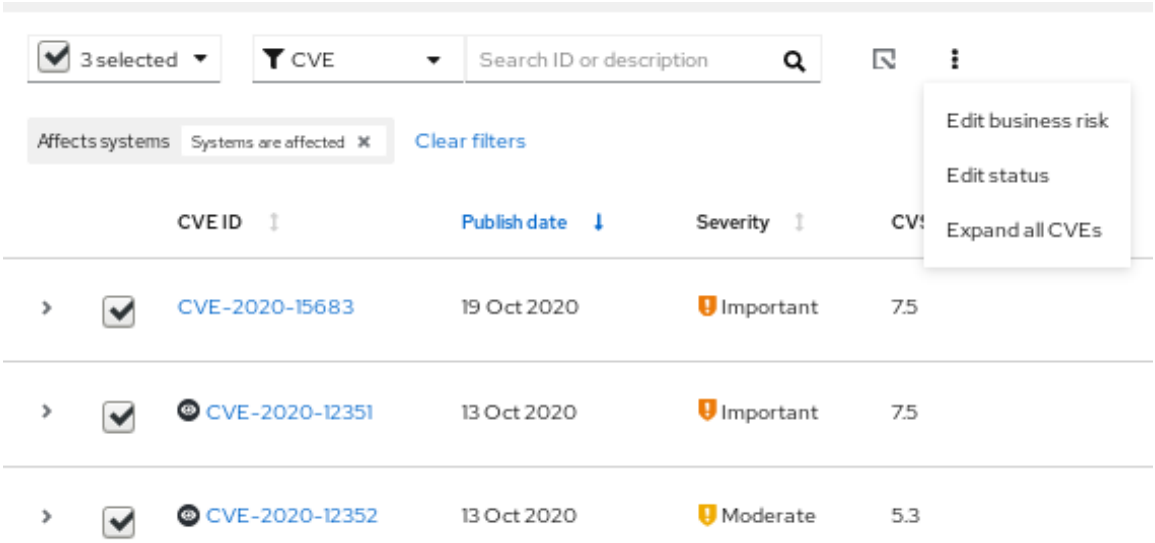
Complete the following steps to set the same business risk on multiple CVEs that you select:

1. Navigate to Vulnerability service > CVEs and log in if necessary.

2. Check the boxes for the CVEs for which you want to set a business risk.

3. Perform the following steps to set a business risk:

   a. Click the **more-actions** icon (three vertical dots) to the right of the Filters dropdown menu in the toolbar and click **Edit business risk**



   b. Set an appropriate business risk value and, optionally, add a justification for your risk assessment.

   c. Click **Save**.

4.4. EXCLUDING SYSTEMS FROM VULNERABILITY SERVICE ANALYSIS

The Vulnerability service allows you to exclude specific systems from vulnerability analysis. This can save you the time and attention required to review and re-review issues on systems that are not relevant to your organization's goals.

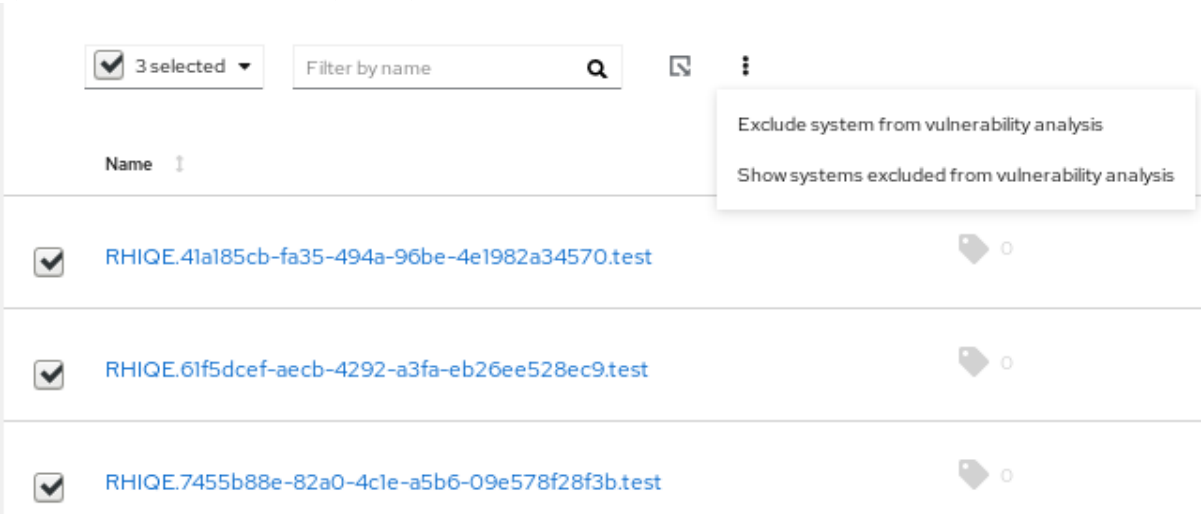
As an example, if you have the following category of servers: QA, Dev, and Production, you may not care to review the vulnerabilities for your QA servers and therefore want to exclude these systems from the analysis performed by the Vulnerability service.

When you exclude systems from vulnerability analysis, the Insights client still runs per schedule on the system, but the results for the system are not visible in the Vulnerability service. The continued operations of the client ensure that other Red Hat Insights services can still upload the data they need. It also means that you can still view results for those systems using filtering.

Complete the following steps to exclude selected RHEL systems from Vulnerability service analysis:

Procedure

1. Navigate to the Vulnerability service > Systems tab and log in if necessary.
2. Check the box for each system you want to exclude from vulnerability analysis.
3. Click the **more-actions** icon in the toolbar, at the top of the list of systems, and select **Exclude systems from vulnerability analysis**.



4. Optionally, you can exclude a *single* system by clicking the **more-actions** icon in the system row and selecting **Exclude system from vulnerability analysis**.

4.5. SHOWING PREVIOUSLY EXCLUDED SYSTEMS

Complete the following steps to show a previously excluded system:

Procedure

1. Navigate to the Vulnerability service > Systems tab and log in if necessary.
2. Click the **more-actions** icon in the toolbar, at the top of the list of systems, and select **Show systems excluded from analysis**.
3. See systems excluded from vulnerability analysis. This can be verified by the value of **Excluded** in the **Applicable CVEs** column.

4.6. RESUMING VULNERABILITY ANALYSIS FOR A SYSTEM

Complete the following steps to resume vulnerability analysis for a system:

Procedure

1. Navigate to the Vulnerability service > Systems tab and log in if necessary.
2. Click the **more-actions** icon in the toolbar, at the top of the list of systems, and select **Show systems excluded from analysis**.

3. In the list of results, check the box for each system for which you want to resume vulnerability analysis.

4. Click the **more-actions** icon again and select **Resume analysis for system**

4.7. CVE STATUS

Another method of managing CVEs impacting your systems is by setting a status for CVEs. The Vulnerability service enables the following ways of setting a status for a CVE:

- Set a status for a CVE for *all* systems.
- Set a status for a *specific CVE + system pair* .

Status values are preset and include the following options:

- Not reviewed (default)
- In-review
- On-hold
- Scheduled for patch
- Resolved
- No action - risk accepted
- Resolved via mitigation

Setting a status for a CVE can facilitate better triaging through its lifecycle, from becoming aware of it to remediating it. Defining a status allows your organization to keep better tabs on where the most critical CVEs are in their lifecycle and where you should focus your efforts to address the most critical issues per your business need. The status for a CVE is visible in all CVE tables in the Vulnerability service and in individual CVE views.

4.7.1. Setting a status for a CVE on all affected systems

Complete the following steps to set a status for a CVE and have that status apply to that CVE on all of the systems it impacts:

Procedure

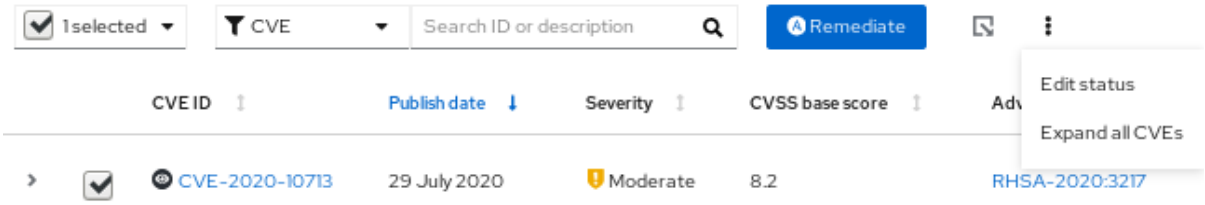
1. Navigate to the Vulnerability service > CVEs tab and log in if necessary.
2. Click the **more-actions** icon located on the right end of the CVE row and select **Edit status**.
3. Select the appropriate status and, optionally, enter a rationale for your decision in the **Justification** text box.
4. Check **Do not overwrite individual system status** if there are statuses set for this CVE on individual systems and that you want to preserve. Otherwise, leave the box unchecked to apply this status to all of the systems it is impacting.
5. Click **Save**.

4.7.2. Setting a status for a CVE and system pair

Complete the following steps to set a status on a CVE and system pair:

Procedure

1. Navigate to the Vulnerability service > Systems tab and log in if necessary.
2. Identify the system and click the system name to open it.
3. Select a CVE from the list and check the box next to the CVE ID.
4. Click the **more-options** icon in the toolbar and select **Edit status**.



5. In the popup card, take the following actions:
   a. Set a status for the CVE and system pair.

NOTE

If the box to **Use overall CVE status** is checked, you cannot set a status for the pair.

   b. Optionally, enter a justification for your status determination.
   c. Click **Save**.
6. Locate the CVE in the list and verify the status is set.

4.8. USING THE SEARCH BOX

The search function in the Vulnerability service works in the context of the page you are viewing.

- **CVEs page.** The search box is located in the toolbar at the top of the CVEs list. With the CVE filter set, search CVE IDs and descriptions.

- **Systems page.** The search box is located in the toolbar at the top of the list. Search for system name or UUID.

4.9. SORTING CVE LIST DATA

The sorting functions in the Vulnerability service differ based on the context of the page you are viewing.

In the **CVEs tab**, you can apply sorting to the following columns:

- CVE ID
- Publish date
- Severity
- CVSS base score
- Systems exposed
- Business risk
- Status

In the **Systems tab**, the following column can be sorted:

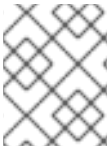
- Name
- Applicable CVEs
- Last seen

After selecting a system in the Systems tab, the system-specific list of CVEs allows the following sorting options:

- CVE ID
- Publish date
- Impact
- CVSS base score
- Business risk
- Status

CHAPTER 5. SYSTEM TAGS AND GROUPS

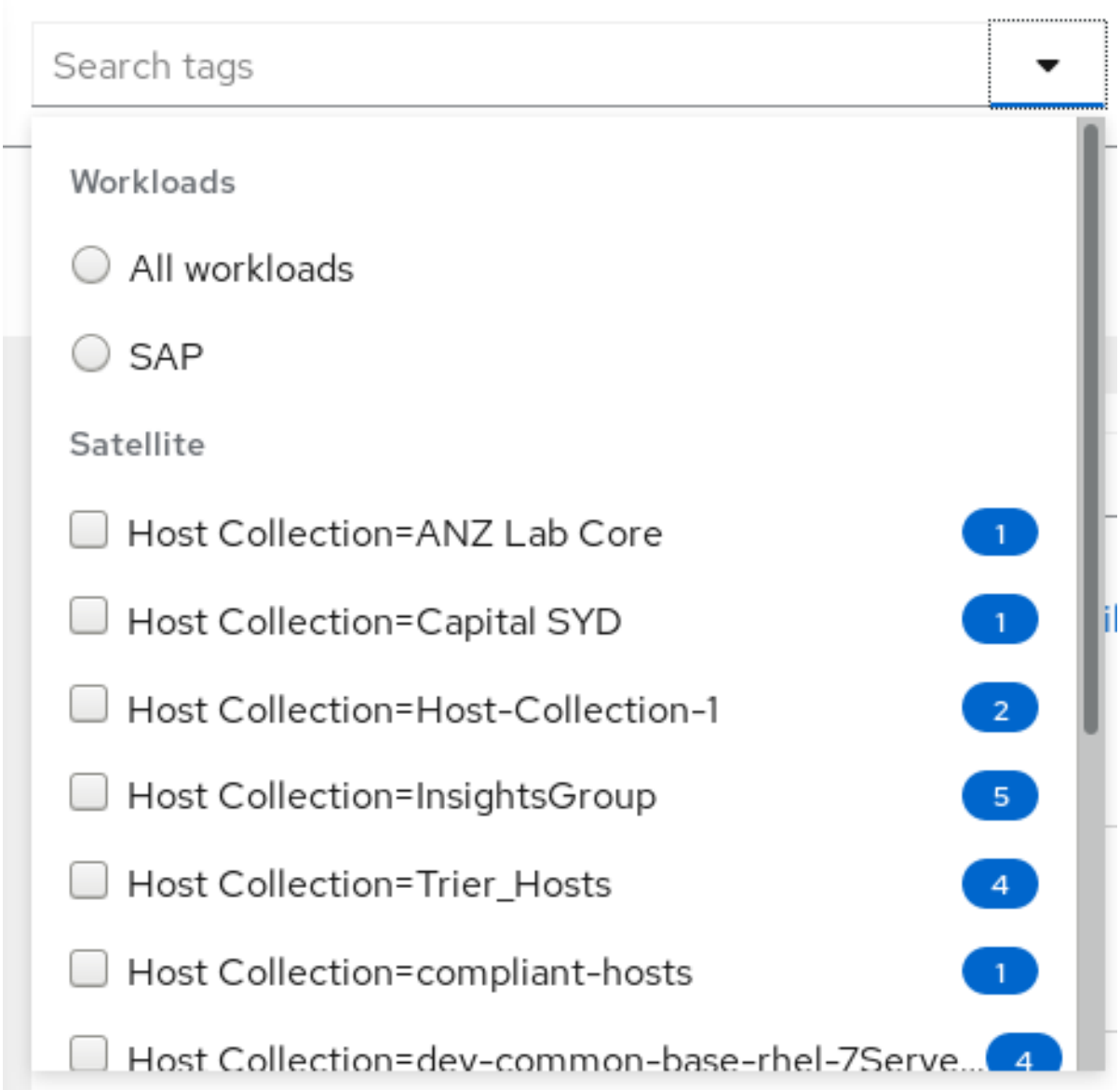
Red Hat Insights enables administrators to filter systems in inventory and in individual services using group tags. Groups are identified by the method of system data ingestion to Insights. Insights enables filtering groups of systems by those running SAP workloads, by Satellite host group, and by custom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

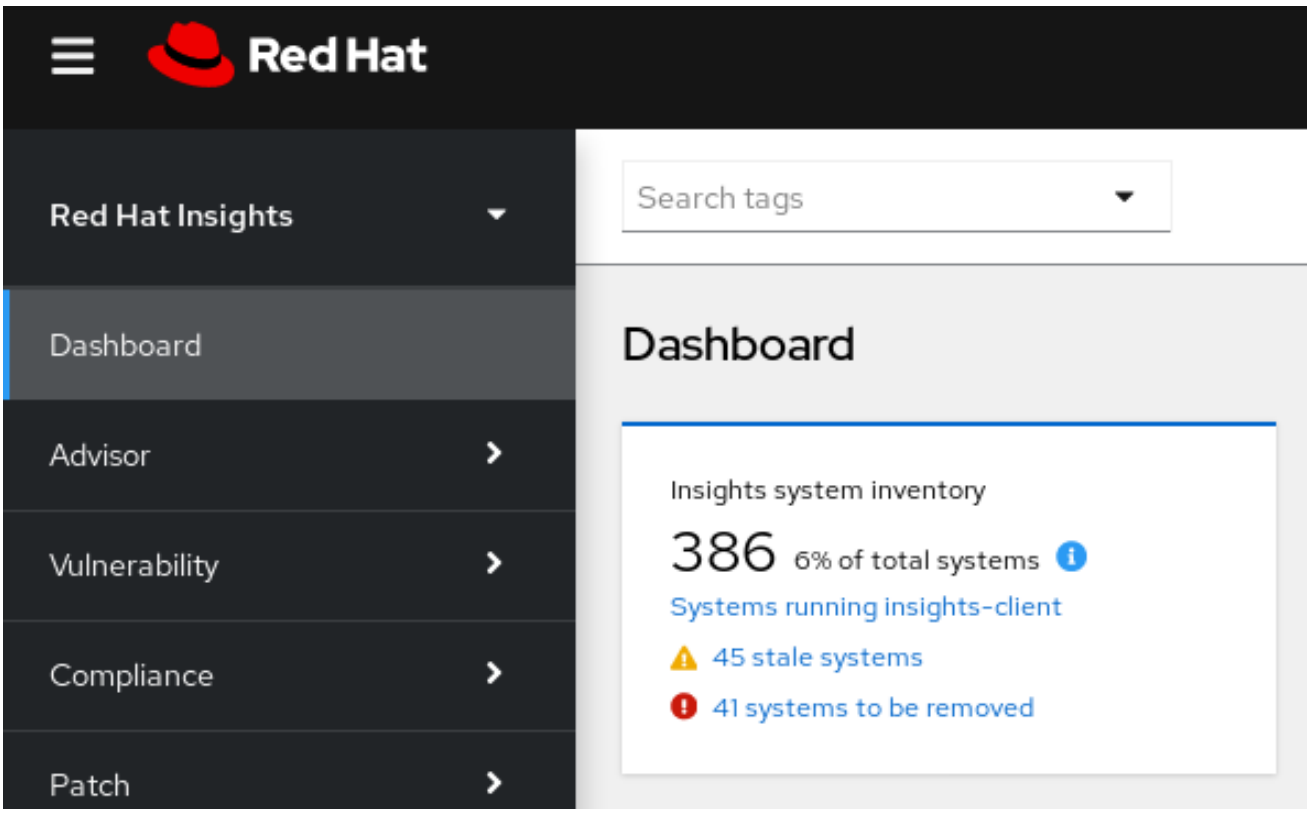
- The Red Hat Insights client is installed and registered on each system.

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

5.1. 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.

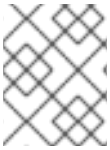


5.2. SATELLITE HOST GROUPS

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

5.3. 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.

5.3.1. 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.

5.3.2. 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
```

5.3.3. 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=**:

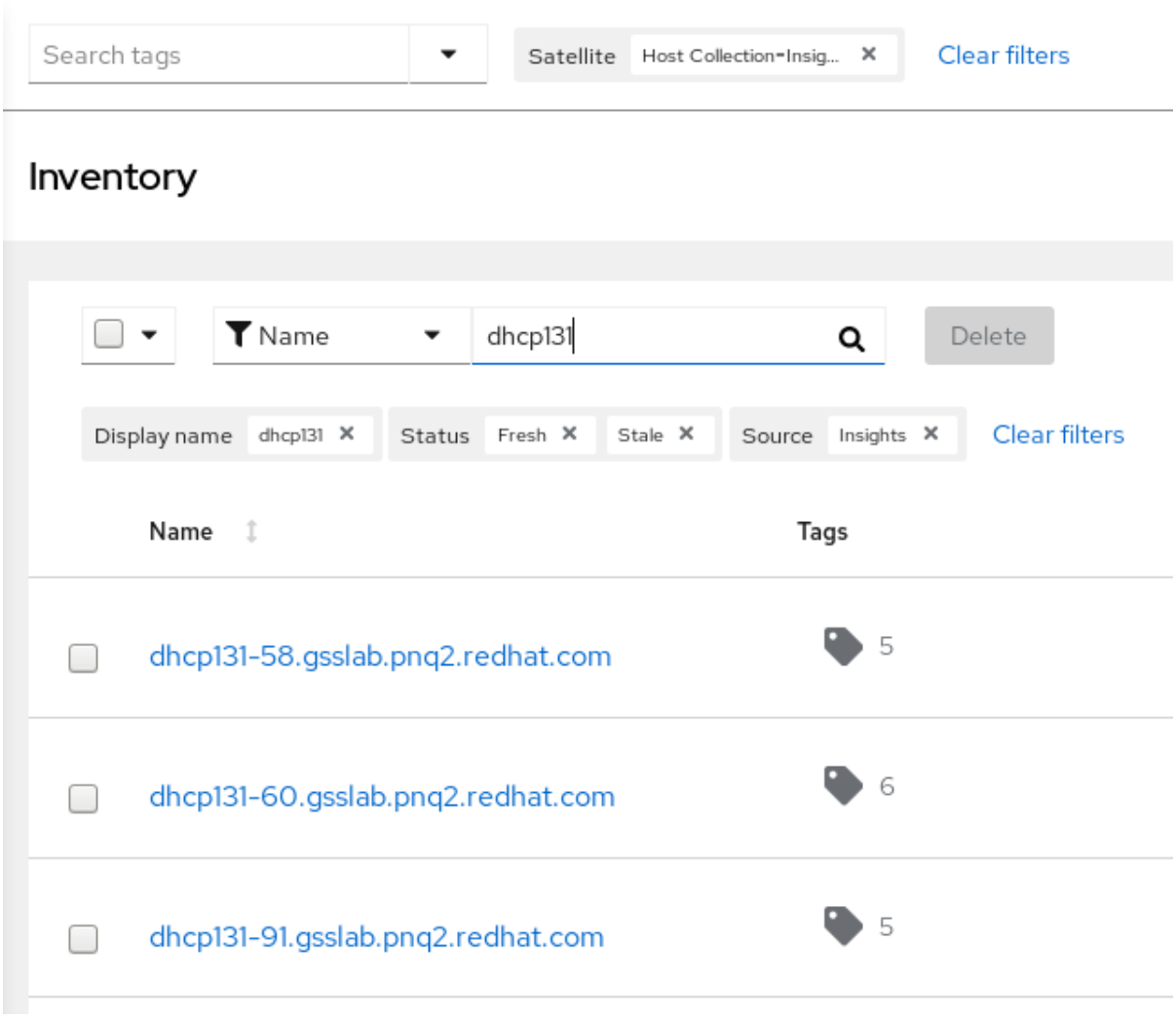
```
[root@server ~]# insights-client --group=<name-you-choose>
```

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.



5.3.4. Editing tags.yaml to add or change tags

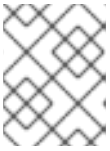
After creating the group tag, edit the contents of **/etc/insights-client/tags.yaml** as needed to add or modify tags. You can add multiple, filterable tags to a system.

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
```



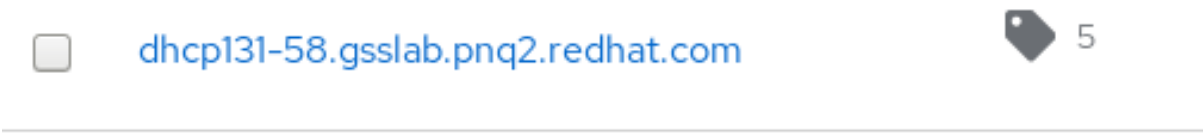
NOTE

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 6. REFERENCE MATERIALS

To learn more about the Vulnerability service, see the following resources:

- *Remediating Security Exposures using Vulnerability and Ansible Playbooks*
- *Generating Vulnerability Reports*
- Red Hat Insights Documentation
- Red Hat Insights Product Support page