



## Red Hat Insights 1-latest

# Viewing and managing system inventory with FedRAMP

Using inventory groups to organize system inventory and manage User Access to groups of systems



# Red Hat Insights 1-latest Viewing and managing system inventory with FedRAMP

---

Using inventory groups to organize system inventory and manage User Access to groups of systems

## Legal Notice

Copyright © 2024 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

This document helps Insights for Red Hat Enterprise Linux administrators with FedRAMP<sup>®</sup> to organize their system inventory into logical groups (called Inventory groups) and control User Access to systems. 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.

## Table of Contents

<b>CHAPTER 1. INVENTORY OVERVIEW</b> .....	<b>4</b>
1.1. DATA GOVERNANCE	4
1.1.1. Data obfuscation	4
1.1.2. Data redaction	4
1.1.3. Data retention	5
1.2. DATA COLLECTORS FOR INVENTORY	5
1.2.1. Identifying which data collector is reporting to inventory	6
<b>CHAPTER 2. ASSESSING AND FILTERING YOUR INVENTORY</b> .....	<b>7</b>
2.1. INVENTORY APPLICATION PROGRAMMING INTERFACE (API)	7
2.2. REFINING YOUR VIEW OF SYSTEMS IN INVENTORY	7
2.3. DELETING SYSTEMS FROM INVENTORY	8
<b>CHAPTER 3. USER ACCESS FOR RBAC IN SYSTEMS INVENTORY</b> .....	<b>9</b>
3.1. USER ACCESS FOR INVENTORY	9
3.1.1. How User Access works	9
3.1.2. Inventory predefined roles and permissions	9
3.2. USER ACCESS TO INVENTORY GROUPS	10
3.2.1. Managing user access to Inventory groups	11
3.2.1.1. Creating a custom User Access role	11
3.2.1.2. Assigning custom roles	13
3.2.1.3. Configuring user access	13
3.2.1.4. Configuring Inventory Hosts Administrator access	14
3.3. USER SCENARIOS	14
3.3.1. Scenario 1: Two different IT teams must manage their systems with Insights	14
3.3.1.1. Initial phase	15
3.3.1.2. Restricting access	15
3.3.1.3. Adjustment considerations	23
3.3.2. Scenario 2: Access to ungrouped systems	23
3.3.3. Known limitations	26
<b>CHAPTER 4. EXPORTING INVENTORY DATA</b> .....	<b>28</b>
4.1. INVENTORY DATA FILES	28
4.2. EXPORTING SYSTEM INVENTORY FROM THE INSIGHTS UI	29
4.3. EXPORTING SYSTEM INVENTORY USING THE EXPORT API	29
4.3.1. Requesting the system inventory export	30
4.3.2. Deleting export files	31
4.3.3. Automating inventory export using Ansible playbooks	32
4.3.4. Using the inventory export service for multiple Insights services	32
<b>CHAPTER 5. SYSTEMS LIFECYCLE IN THE INVENTORY APPLICATION</b> .....	<b>33</b>
5.1. DETERMINING SYSTEM STATE IN INVENTORY	33
5.1.1. Modifying system staleness and deletion time limits in inventory	34
<b>CHAPTER 6. INVENTORY GROUPS</b> .....	<b>36</b>
6.1. CREATING INVENTORY GROUPS	36
6.2. ADDING SYSTEMS TO A NEWLY CREATED INVENTORY GROUP	36
6.2.1. Adding a system and creating a group from the Inventory systems page	37
6.3. REMOVING SYSTEMS FROM THE INVENTORY GROUP	38
6.3.1. Removing systems from the Inventory group using the Inventory groups page	38
6.3.2. Removing systems from the Inventory group using the Systems page	38
6.4. RENAMING THE INVENTORY GROUP	39

6.5. DELETING THE INVENTORY GROUP	39
<b>CHAPTER 7. CONFIGURING NOTIFICATIONS FOR INVENTORY EVENTS</b> .....	<b>41</b>
7.1. SETTING UP ORGANIZATION NOTIFICATIONS FOR INVENTORY EVENTS	41
7.2. SETTING UP USER EMAIL NOTIFICATIONS FOR INVENTORY EVENTS	42
<b>PROVIDING FEEDBACK ON RED HAT DOCUMENTATION</b> .....	<b>44</b>



# CHAPTER 1. INVENTORY OVERVIEW

Inventory provides a comprehensive view of all the systems in your organization, which allows you to easily track and manage your infrastructure. You can access inventory in two ways:

- through the Hybrid Cloud Console, and
- by the Managed inventory API

Systems must be registered with Red Hat to be visible in inventory. There are multiple ways to register with Red Hat. For more information about registering systems with Red Hat Insights, see the following resources:

[Client Configuration Guide for Red Hat Insights with FedRAMP](#) .

## Insights Analysis

When your system is registered with Red Hat Insights, Insights performs an initial analysis of the system. Status information, such as system state and whether a system is active, is stored in inventory. You can access additional details about the system from the [Red Hat Insights > RHEL > Inventory](#) page in the Hybrid Cloud Console. After the initial analysis is complete, Insights runs analyses daily, providing feedback to you and reporting system status to inventory.

Insights analysis results can include alerts that identify issues in your systems, and recommendations about how to resolve those issues.

Insights also monitors your systems for system staleness, and uses specific staleness criteria to flag systems that are not reporting regularly. If systems do not report after a specified period of time, Insights flags them for deletion.

## Additional Resources

[Getting Started with Red Hat Insights](#)

## 1.1. DATA GOVERNANCE

Red Hat Insights helps to identify and address operational and vulnerability risks, before they result in system downtime. This functionality requires that Insights collects small pieces of system metadata for processing and analysis. Here is how we ensure the security of your data:

- Red Hat Insights collects only the minimum system metadata needed to analyze and identify issues for supported platforms.
- Before data is sent to Red Hat, you have the option to inspect and redact your data.
- Data is encrypted throughout the process, with a customizable collection schedule. Red Hat data collection rules are signed and the signature is verified before proceeding.
- Only one uploaded data set is stored at a time for each cluster, host or instance.

### 1.1.1. Data obfuscation

You have full control over the data collected by Insights. It is possible to anonymize the data by obfuscating IP addresses and host names in the Insights client.

### 1.1.2. Data redaction



You can exclude specific data from the Insights client collection process, by using data redaction commands in the command line interface. This method can be used to ensure personally identifiable information (PII) is not collected. However, data redaction reduces the quantity and quality of system recommendations.

### 1.1.3. Data retention

The Insights client collects and uploads your data once a day with the default configuration. The collected data is kept 24 hours for analysis. Data is replaced by new uploads from the Insights client every day. Data is automatically deleted after 14 days if there is no upload from the Insights client.

Results from the analysis are retained for historical reporting purposes and might be used by Red Hat as input into feature enhancements.

#### Additional Resources

For more information on Red Hat data governance, see the Red Hat Insights data and application security page: [Red Hat Insights data and application security](#)

For more information on obfuscating data, see Red Hat Insights client documentation: [Insights client data obfuscation](#)

For more information on configuring a denylist, see Red Hat Insights client documentation: [Insights client data redaction](#)

## 1.2. DATA COLLECTORS FOR INVENTORY

Each system registered in inventory gets its data from one of many data collectors. Data collectors run on a regular cadence and synchronize their collected data with the Red Hat Hybrid Cloud Console.

A system can be reported by one or more collectors. When multiple collectors provide information for the same system, inventory uses a deduplication mechanism to merge the information. This process ensures that systems appear only once in inventory.

The following data collectors upload system information to the Red Hat Hybrid Cloud Console:

- **Red Hat Insights.** Insights registers and aggregates system data. By default, it runs daily on each system and uploads the system data to the Red Hat Hybrid Cloud Console for processing. The data that Insights collects is used to formulate all the recommendations Insights provides.
- **Red Hat Subscription Manager (RHSM)** The subscription-manager tool runs daily to provide a list of all systems in your organization that are registered with Red Hat. Note that unless Insights is also enabled, data collected by Subscription Manager alone does not provide recommendations.
- **Remote Host Configuration (rhc).** The rhc client allows you to register systems to Insights and RHSM, and configure Insights connections for all RHEL systems in your organization. In addition, the rhc client makes it easy to find system issues, and to fix them with remediation playbooks generated by Insights.
- **Red Hat Discovery tool** Discovery tool scans systems for Red Hat software installations and provides a report to Red Hat Hybrid Cloud Console for inclusion in inventory. You will run this tool manually.

- **Red Hat Satellite.** Satellite provides an integration with Red Hat Hybrid Cloud Console. When configured, Satellite uploads its inventory of registered systems daily and synchronizes it with the inventory application. This includes all systems registered with Satellite and Capsule servers.



#### NOTE

Data collected and reported by Subscription manager and Satellite alone will *NOT* result in analysis and recommendations. Red Hat Insights must also be enabled.

### 1.2.1. Identifying which data collector is reporting to inventory

You can determine which data collector(s) have reported for an individual system by visiting the Red Hat Hybrid Cloud Console:

#### Prerequisites

- You have Inventory Hosts Viewer access.

#### Procedure

1. Navigate to the [Red Hat Insights > RHEL > Inventory](#) page.
2. Click the system you want to view.
3. You will notice that you are in the **General information** tab. Remain in that tab and scroll to the bottom of the page.
4. Reference the **Data collectors** card at the bottom of the page. There you will see the data collector(s) **Name**, **Status** and **Last upload** details.



#### NOTE

You can also filter your systems by data collectors in the inventory **Systems** page. This is explained in Section 2.2, Refining your view of systems in inventory.

#### Additional Resources

[Red Hat Insights client](#)

[Red Hat Satellite](#)

[Red Hat Subscription Manager \(RHSM\)](#)

[Getting started with the Subscriptions Service](#)

[Red Hat Discovery tool](#)

[Remote Host Configuration and Management \(rhc\)](#)

## CHAPTER 2. ASSESSING AND FILTERING YOUR INVENTORY

Assessing and filtering your inventory will help you identify and eliminate security, operations, and business risks in your fleet.

### 2.1. INVENTORY APPLICATION PROGRAMMING INTERFACE (API)

Red Hat Insights provides a set of APIs that you can use to interact with specific Insights for Red Hat Enterprise Linux applications, to obtain system details and recommendations.

We have designed our APIs to ensure the security of your data. All Insights APIs are Representational State Transfer (REST) APIs. REST APIs are stateless. Statelessness means that servers do not save client data between requests. Our APIs also use token-based authentication, which provides granular control over access permissions and enhances security.

Review the following resources to learn more about how you can use the inventory API to locate information, enact edits, and automate repetitive tasks:

#### Additional Resources

For more information about Red Hat Insights API, see the Red Hat Insights API reference guide: [API Catalog](#)

For more information about getting started with Red Hat Insights API, see the Red Hat Insights API cheat sheet: [Insights API cheat sheet](#)

For more information about the inventory API, see Managed Inventory: [Managed Inventory API](#)

### 2.2. REFINING YOUR VIEW OF SYSTEMS IN INVENTORY

There are several ways to refine your inventory view to help you focus on the issues and systems that matter the most. You can filter by **Name**, **Status**, **Operating System**, **Data Collector**, **remote host configuration status**, **Last seen**, **Inventory group**, or **Tags**. Follow the procedure below to filter your systems:

#### Prerequisites

- You have inventory Hosts Viewer access.

#### Procedure

1. Navigate to [Red Hat Insights > RHEL > Inventory](#) page.
2. Click the **Name** filter drop-down. Choose an option from the drop-down menu, such as **Name**, **Status**, **Operating System**, **Data Collector**, **RHC status**, **Last seen**, **Inventory group** or **Tags**.
3. Select additional filters within your query. For example, if you chose the **Operating System** filter, click **Filter by operating system** in the header to choose a specific version of RHEL.
4. Click the checkbox next to the RHEL version you want to filter.
5. **Optional:** To add multiple filters to your query, click an additional filter (such as **Data Collector**). A second drop-down appears to the right of the **Data Collector** filter, called **Filter by data collector**.

6. Choose the desired data collector. This first filter then appears just below the header. If desired, choose a second filter. You can apply all 8 available filters to your query.
7. Click **Reset filters** to clear your query.

### Additional Resources

For information about global filters, see the following:

[System filtering and groups](#)

## 2.3. DELETING SYSTEMS FROM INVENTORY

When a system is obsolete or decommissioned, you might choose to remove it from inventory. Use the following procedure to do so:

### Prerequisites

1. You have Inventory Hosts Administrator access.

### Procedure

1. Navigate to [Red Hat Insights > RHEL > Inventory](#) page.
2. Check the box to the left of the system(s) you want to remove.
3. Click the **Delete** button to the right of the filter. A **Delete from Inventory** confirmation dialog box appears.
4. Click **Delete** to confirm this action.

A message box appears in the upper right corner of the screen, stating that the delete operation initiated. When the deletion is complete, a message box confirms that deletion was successful.

### CAUTION

The selected system(s) **will be removed** from **ALL console.redhat.com applications and services**.



### NOTE

A system might reappear in inventory if data collectors are uploading data from systems that are still **registered** and **subscribed**. Refer to the documentation for the specific data collector(s) to determine how to permanently unregister or unsubscribe.

### Additional resources

[Unregistering from Red Hat Subscription Management Services](#)

## CHAPTER 3. USER ACCESS FOR RBAC IN SYSTEMS INVENTORY

### 3.1. USER ACCESS FOR INVENTORY

Red Hat uses role-based access control (RBAC) to manage User Access on the Red Hat Hybrid Cloud Console. You can use User Access to configure access and permissions in systems inventory.

Insights for Red Hat Enterprise Linux provides a set of predefined roles. Depending on the application, the predefined roles for each supported application can have different permissions that are tailored to that application.

#### 3.1.1. How User Access works

The User Access feature is based on managing roles, rather than on individually assigning permissions to specific users. In User Access, each role has a specific set of permissions. For example, a role might allow **read permission** for an application. Another role might allow **write permission** for an application.

You create groups that contain roles and, by extension, the permissions assigned to each role. You also assign users to those groups. This means that each user in a group is assigned the permissions of the roles in that group.

By creating different groups and adding or removing roles for that group, you control the permissions allowed for that group. When you add one or more users to a group, those users can perform all actions that are allowed for that group.

Insights for Red Hat Enterprise Linux provides two default access groups for User Access:

- **Default admin access** group. The **Default admin access** group is limited to Organization Administrator users in your organization. You cannot change or modify the roles in the **Default admin access** group.
- **Default access** group. The **Default access group** contains all authenticated users in your organization. These users automatically inherit a selection of predefined roles.



#### NOTE

You can make changes to the Default access group. However, when you do so, the group name automatically changes to **Custom default access**

#### 3.1.2. Inventory predefined roles and permissions

Role Name	Description	Permissions
Inventory Administrator	You can perform any available operation against any Inventory resource.	inventory:** (* denotes all permissions on all resources)
Inventory Groups Administrator	You can read and edit Inventory Groups data.	inventory: groups: write and inventory: groups: read

Role Name	Description	Permissions
Inventory Groups Viewer	You can read Inventory Groups data.	inventory: groups: read
Inventory Hosts Administrator	You can read and edit Inventory Hosts data.	inventory: hosts: write and inventory: hosts: read
Inventory Hosts Viewer	You can read Inventory Hosts data.	inventory: hosts: read

## Additional Resources

[Role Based Access Control](#)

## 3.2. USER ACCESS TO INVENTORY GROUPS

Inventory groups allow you to group systems in your inventory together into logical units, such as location, department, or purpose. Each system can belong to only one Inventory group.

Inventory groups also support role-based access control (RBAC). Using RBAC enables you to set custom permissions on Inventory groups according to user role.

The **Inventory group administrator** User Access role allows you to create Inventory groups. This role is automatically included in the Default Access group and cannot be removed from it. However, users with this role can modify any Inventory group. Provide this role *only* to those users who are entitled to access the entire system inventory.

For a user to be able to use Inventory groups and RBAC to restrict access to specific systems, that user must either be a member of the Default Access group, or have both the **Inventory group Administrator** and the **User Access Administrator** roles.

Inventory group users have **group-level** RBAC permissions. Custom permissions include the following:

- inventory:groups:read
  - View Inventory group details page
- inventory:groups:write
  - Rename the Inventory group
  - Add systems to the Inventory group
- Remove systems from the Inventory group



### NOTE

A user cannot view the systems inside the Inventory group without inventory:hosts:read permissions.

Systems users have **system-level** RBAC permissions. They can perform the following Inventory group operations:

- `inventory:hosts:read`
  - View all the systems in the Inventory group and their details, or view ungrouped systems
  - View information about the systems for other Insights services
- `inventory:hosts:write`
  - Rename the system
  - Delete the system

### 3.2.1. Managing user access to Inventory groups



#### NOTE

If you do not have access to Inventory groups, navigating to **Inventory > Inventory groups** shows the message **Inventory group access permissions needed**.

Be aware that you can still view the Inventory group name assigned to the system for which you have read access, even if you do not have access to the Inventory group itself. To view the Inventory group that contains the system, you need to have the Inventory groups Viewer role, or have Inventory group view permissions assigned.



#### IMPORTANT

Before making changes in the RBAC configuration, review the list of known limitations in the User Scenarios section.

For more information about managing user access, assigning roles, and adding members to user access groups, see [User Access Configuration Guide for Role-based Access Control \(RBAC\)](#) .

#### 3.2.1.1. Creating a custom User Access role

Use the User Access application to configure user access for your Inventory group.

To create a custom role:

1. Click the **Settings** icon (⚙️) in the top right corner, and then select **User Access** to navigate to the User Access application. The **Identity & Access Management** main page displays.
2. In the left navigation menu, click **Roles**.
3. Click **Create role**. The **Create Role** wizard displays.
4. Select whether you want to create a new role, or copy an existing role.
  - a. To create a new role, select **create a role from scratch**
  - b. To copy an existing role, select **Copy an existing role**. A list of roles appears. Select the role you want to copy, and then click **Next**.
5. Name the new role. If desired, add a description.
6. Click **Next**. The **Add permissions** page displays.

7. The Applications filter displays by default. Click the **Filter by application** drop-down and select **inventory** to display all the available inventory permissions.

The four inventory permissions include:

- `inventory:hosts:read` - Allows users to view systems (needed to view systems both inside and outside the Inventory group).
- `inventory:hosts:write` - Allows users to Rename or Delete systems.
- `inventory:groups:read` - Allows users to view Inventory groups, and general info (not including systems in it).
- `inventory:groups:write` - Allows users to edit Inventory group membership (add and remove systems from Inventory groups).

8. Select the inventory permissions that you need. Here are some examples:

- a. To give a user full access to the Inventory group and all systems in that Inventory group, select all four permissions.
- b. To give a user full access to the systems inside a Inventory group without granting Inventory group editing access, select `inventory:hosts:read`, `inventory:hosts:write`, and `inventory:groups:read`, but *do not* select `inventory:groups:write`.
- c. To give a user full access to ungrouped systems, select all four permissions (ungrouped systems are considered a Inventory group).

9. Click **Next**. The **Define Inventory group access** page displays.

10. Click the drop-down arrow next to each permission in the list, and then select the Inventory groups you want to apply to those permissions. You must select at least one Inventory group for each permission.

11. Click **Next**. The **Review details** page displays.

12. Review the permissions for the custom role and click **Submit**.

Repeat this process for each Inventory group or for each group of users that requires specific Inventory group access.

## Example scenarios

These examples describe the permissions you assign to users in specific custom roles.

- To allow users to only see systems in specific Inventory groups, but to *not* see systems that do not belong to any Inventory groups, select only those Inventory groups.
- To allow users to see systems in specific Inventory groups as well as any systems that do not belong to any Inventory groups, select those Inventory groups for all permissions and select **Ungrouped systems** for `inventory:hosts` permissions.
- To allow users to see everything in the inventory, you do not need to create a custom role.
- To give a group of system administrators the same access to Inventory groups A, B, and C, create a single custom role and assign permissions to those three Inventory groups. However, if you want to give different users access to different Inventory groups, create a separate custom role for each Inventory group.



### 3.2.1.2. Assigning custom roles

To assign custom roles to a user or group of users, create a User Access group. The users inside a group receive the roles assigned to that group.

1. At the top right of the screen, click the Settings icon (the **Settings** icon (⚙)), and then click **User Access**.
2. In the left navigation menu, click **User Access > Groups**
3. Click **Create group**. The Create group wizard displays the **Name and description** page.
4. Add a group name. If desired, add a description for the group.
5. Click **Next**. The **Add roles** page displays.
6. Select the custom role you created, and then click **Next**. The **Add members** page displays.
7. Select the users to whom you want to assign the custom role.
8. Click **Next**. The **Add service accounts** page appears.
9. **Optional**. If you want to assign a service account or accounts to the selected users, select one or more service accounts from the list.
10. Click **Next**. Review the details of your selections and click **Submit**.

Repeat this procedure for each custom role that you want to assign to one or more users.

### 3.2.1.3. Configuring user access

After you create and assign a custom role, all users in your organization still have full access to inventory because they still have the **Inventory Hosts Administrator** role assigned. This allows any user to view and edit all hosts. The Default Access workspace assigns this role to all users in your organization by default.

To limit organization users' access to only the Inventory groups/systems defined in your custom roles, edit the Default Access Inventory group to remove the **Inventory Hosts Administrator** role.

1. At the top right of the screen, click the Settings icon (the **Settings** icon (⚙)), and then click **User Access**.
2. In the left navigation menu, click **User Access > Groups** The list of User access groups displays.
3. Click the **Default access** group. The list of roles displays.
4. Select the checkbox for the **Inventory Hosts Administrator** role.
5. Click the options icon (⋮) at the far right of the row. The **Remove role** option appears.
6. Click **Remove role**. The **Remove role** dialog box appears.
7. Click the **Remove role** button. If you have never edited the Default Access Inventory group before, a warning message displays.
8. Select the **I understand, and I want to continue** checkbox, and then click **Continue**.

### 3.2.1.4. Configuring Inventory Hosts Administrator access

After you edit the Default Access Inventory group, you might want to create a new User Access group of users who should have **Inventory Hosts Administrator** permissions.

1. At the top right of the screen, click the Settings icon (the **Settings** icon (⚙)), and then click **User Access**.
2. In the left navigation menu, click **User Access > Groups**. The list of Inventory groups displays.
3. Click **Create group**. The Create Group wizard appears.
4. Add a name for the group. If desired, add a description.
5. Click **Next**. The **Add roles** page displays.
6. Select the **Inventory Hosts Administrator** role from the list of roles.
7. Click **Next**. The **Add members** page displays.
8. Select the users to whom you want to assign the role.
9. Click **Next**. The **Add service accounts** page appears.
10. **Optional.** If you want to assign a service account or accounts to the selected users, select one or more service accounts from the list.
11. Click **Next**. The **Review details** page displays.
12. Review the details of your selections, and click **Submit**.

After you have finished configuring access, specific users within your organization have full inventory access, and others have limited inventory access.

## 3.3. USER SCENARIOS

This section contains two example scenarios that illustrate the features of Inventory groups. These scenarios follow a procedure format, so that you can follow the required steps and test them, if desired.

### 3.3.1. Scenario 1: Two different IT teams must manage their systems with Insights

In this scenario, two different IT teams working for the same company share the same Insights organization within their Red Hat account.

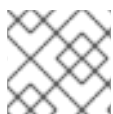
- Each IT team must have complete control of their systems in the Red Hat Hybrid Cloud Console, but should not be able to see or modify the systems belonging to the other team.
- All users within the same team have the same level of access on both their Inventory groups and their systems. Access levels can be adjusted as needed.
- Regular users of both IT teams will not be able to see or modify systems that are not part of any Inventory groups.
- Organization administrators, or anyone with Inventory group administrator and Inventory Hosts administrator roles, have access to the entire inventory. Any other users without those roles cannot access the entire inventory.

### 3.3.1.1. Initial phase

By default, organization administrators (who are members of the Default administrator access group) on the Red Hat Hybrid Cloud Console always have read/write access to all Inventory groups and read/write access to all systems, regardless of how permissions are defined for the Inventory group objects and systems assigned to them.

These users are the only ones who may configure user access for Inventory groups. If any regular users need to manage user access, the administrators can grant them Inventory group admin and Inventory Hosts admin roles separately.

By default, users who are not Organization administrators are assigned the Inventory Hosts Administrator role from the Default access group. The Default access group gives these users `inventory:hosts:read` and `inventory:hosts:write` access across the entire inventory. Those permissions grant read and write permissions on all systems and all Inventory groups.



#### NOTE

For more information about the Default access group, see [The Default access group](#).

### 3.3.1.2. Restricting access

#### Prerequisites

- You are a member of the Default administrator access group.

#### Step 1: Create the Inventory groups

First, create two separate Inventory groups. (This example shows two Inventory groups, but you may create as many as you need).

- Inventory group 1: IT team A - Systems
- Inventory group 2: IT team B - Systems

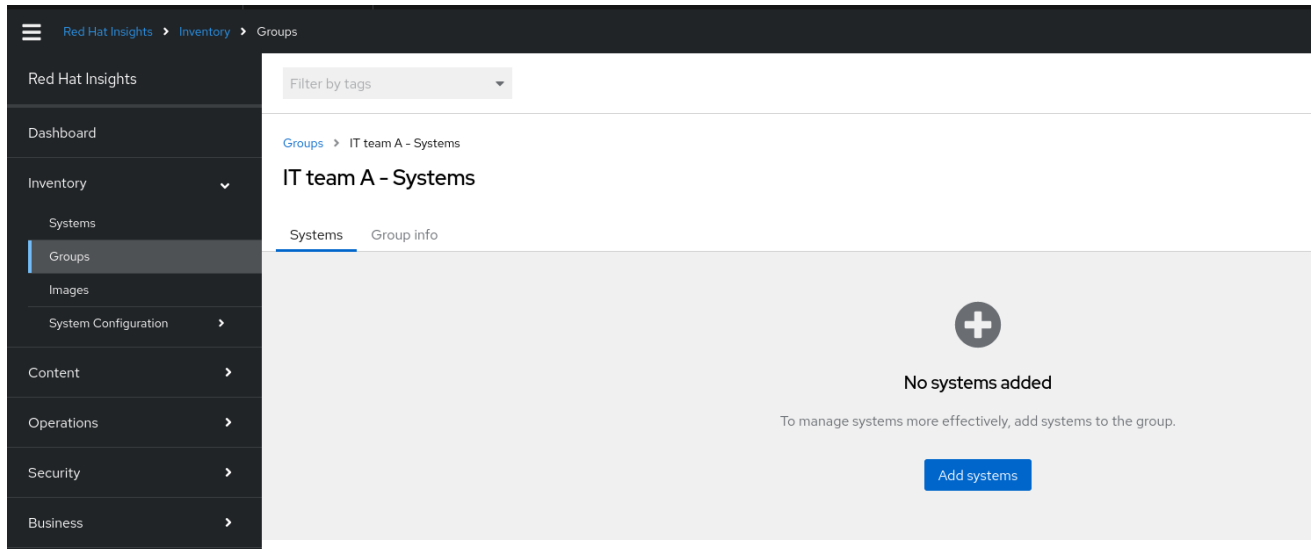
## Create group ×

**Group name** \*

Can only contain letters, numbers, spaces, hyphens ( - ), and underscores( \_ ).

#### Step 2: Add systems to Inventory groups

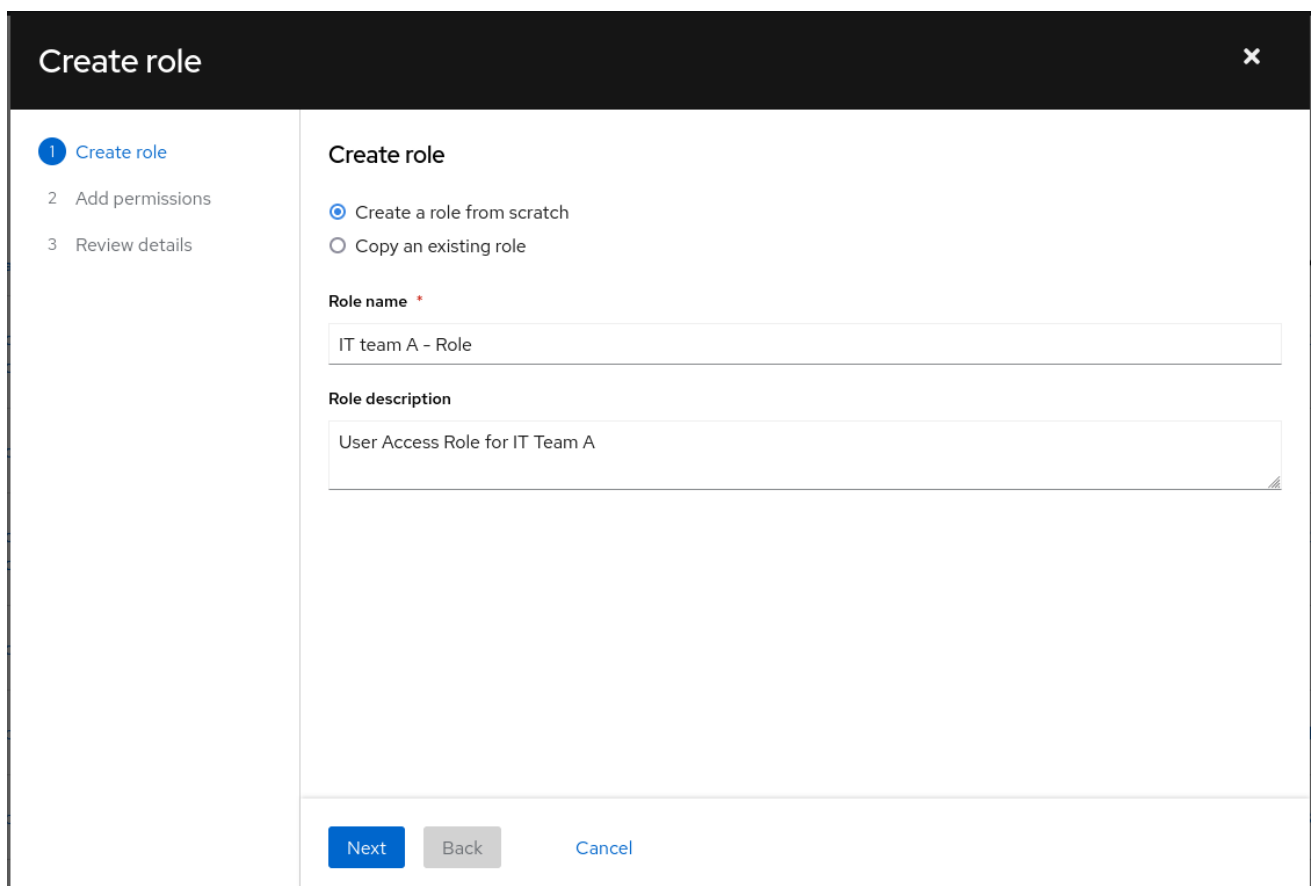
Now that the Inventory groups have been created, add systems to them. Click in each Inventory group and select **Add systems**.



At this stage, all the users still have access to all systems, regardless of the Inventory groups they are in. This is because they still have the Inventory hosts administrator role, which allows them to see all systems, whether or not they are grouped into Inventory groups.

### Step 3: Create custom roles

To customize access for different Inventory groups, create custom roles for those Inventory groups. To create a custom role, navigate to **User Access > Roles** and click **Create role**. A wizard opens. Name your role (For example, IT Team - A Role), and click **Next**.



### Step 3a: Select permissions to add to the custom role

The wizard displays the **Add permissions** step. This step contains four inventory permissions options. Select them depending on the level of access you want to grant.

For full access to the Inventory group and its systems, select:

- inventory:groups:read
- inventory:groups:write
- inventory:hosts:read
- inventory:hosts:write

**Create role** ✕

1 Create role  
 2 **Add permissions**  
 3 Review details

Selected permissions: inventory:groups:write ✕ inventory:groups:read ✕ inventory:hosts:write ✕ [1 more](#)

**Add permissions**  
 Select permissions to add to your role

4 selected Applications Filter by application 1 - 6 of 6

Applications: inventory ✕ [Clear filters](#)

Application	Resource type	Operation
<input type="checkbox"/> inventory	staleness	read
<input type="checkbox"/> inventory	staleness	write
<input checked="" type="checkbox"/> inventory	hosts	read
<input checked="" type="checkbox"/> inventory	hosts	write
<input checked="" type="checkbox"/> inventory	groups	read
<input checked="" type="checkbox"/> inventory	groups	write

1 - 6 of 6 1 of 1

[Next](#) [Back](#) [Cancel](#)

After selecting permissions, click **Next**. You can adjust the permissions as needed.

### Step 3b: Assign permissions to selected Inventory groups

In this step, choose the Inventory group(s) to which you want to grant permission. This example shows how to select the Inventory group that corresponds to the current role. For example, create the role **IT team A - Role**, and specify the Inventory group **IT team A - Systems** for each permission.

**Create role**
✕

- 1 Create role
- 2 Add permissions
- 3 Define Inventory group access
- 4 Review details

### Review details

Specify which inventory groups you'd like to give access for these permissions

Permissions	Group definition	
hosts:read *	Select groups <span style="background-color: #eee; border: 1px solid #ccc; border-radius: 3px; padding: 2px;">1</span> <span style="float: right;">✕ ▼</span>	<a href="#">Copy to all</a>
hosts:write *	Select groups <span style="background-color: #eee; border: 1px solid #ccc; border-radius: 3px; padding: 2px;">1</span> <span style="float: right;">✕ ▼</span>	
groups:read *	Select groups <span style="background-color: #eee; border: 1px solid #ccc; border-radius: 3px; padding: 2px;">Add permission to these groups.</span> <span style="float: right;">✕ ▼</span>	
groups:write *	Select groups <span style="background-color: #eee; border: 1px solid #ccc; border-radius: 3px; padding: 2px;">▼</span>	

[Select all \(2\)](#)

- IT team A - Systems
- IT team B - Systems

Next
Back
Cancel

Review the details and click **Submit**.

**Create role**
✕

- 1 Create role
- 2 Add permissions
- 3 Define Inventory group access
- 4 Review details

### Review details

Review and confirm the details for your role, or click Back to revise.

**Name** IT team A - Role

**Description** User Access Role for IT Team A

Permissions	Application	Resource type	Operation
	inventory	hosts	read
	inventory	hosts	write
	inventory	groups	read
	inventory	groups	write

Resource definitions	Permission	Group definition
	inventory:hosts:read	IT team A - Systems
	inventory:hosts:write	IT team A - Systems
	inventory:groups:read	IT team A - Systems
	inventory:groups:write	IT team A - Systems

Submit
Back
Cancel

Repeat the steps in this section to create a second custom role called **IT team B - Role** and select the **IT team B - Systems** Inventory group.

Create role
✕

- 1 Create role
- 2 Add permissions
- 3 Define Inventory group access
- 4 Review details

### Review details

Review and confirm the details for your role, or click Back to revise.

**Name** IT team B - Role

**Description** User Access Role for IT Team B

Permissions	Application	Resource type	Operation
	inventory	groups	write
	inventory	hosts	write
	inventory	groups	read
	inventory	hosts	read

Resource definitions	Permission	Group definition
	inventory:groups:write	IT team B - Systems
	inventory:hosts:write	IT team B - Systems
	inventory:groups:read	IT team B - Systems
	inventory:hosts:read	IT team B - Systems

Submit
Back
Cancel



## NOTE

You can grant access to systems that are not part of any Inventory group to one or both IT teams. To add those systems, add the Ungrouped systems that appear in the Group definition of the host permissions to your custom role.

**Create role** ✕

- 1 Create role
- 2 Add permissions
- 3 Define Inventory group access
- 4
 Review details

### Review details

Review and confirm the details for your role, or click Back to revise.

**Name** IT team B - Role

**Description** User Access Role for IT Team B

Permissions	Application	Resource type	Operation
	inventory	groups	write
	inventory	hosts	write
	inventory	groups	read
	inventory	hosts	read

Resource definitions	Permission	Group definition
	inventory:groups:write	IT team B - Systems
	inventory:hosts:write	IT team B - Systems, Ungrouped systems
	inventory:groups:read	IT team B - Systems
	inventory:hosts:read	IT team B - Systems, Ungrouped systems

Submit
Back
Cancel

#### Step 4: Create User Access groups to assign custom roles to users

Now that the custom roles are created, create User Access groups to assign the custom roles to users.

To create a new group, navigate to **User Access > Groups** and click **Create group**. Name the group, select the newly created role, and select the users to whom you want to give the role.

For example, two IT groups have the following permissions:

- IT team A - user group
- IT team A - role
- IT team B - user group
- IT team B - role

The groups appear as follows:



## Create group ✕

- 1 Name and description
- 2 Add roles
- 3 Add members
- 4 Review details**

<b>Review details</b>	
<b>Group name</b>	IT team A - User group
<b>Group description</b>	User Access Group for IT Team A
<b>Roles</b>	IT team A - Role
<b>Members</b>	insights-test-day-01

[Cancel](#)

## Create group ✕

- 1 Name and description
- 2 Add roles
- 3 Add members
- 4 Review details**

<b>Review details</b>	
<b>Group name</b>	IT team B - User group
<b>Group description</b>	User Access Group for IT Team B
<b>Roles</b>	IT team B - Role
<b>Members</b>	insights-test-day-03


[Cancel](#)

### Step 5: Remove Inventory Hosts Admin role from the Default Access group

At this stage, despite all the steps taken above, all users still have access to all systems, regardless of the Inventory groups they are in. This is because they still have the Inventory Hosts Administrator role, which allows them to see all systems, whether or not they are grouped into Inventory groups.


To limit access to systems, navigate to **User Access > Groups** and select the Default Access group. Remove the Inventory Hosts Administrator role from this group.

1 selected		Name	Filter by name	Q	Add role	:
	Name	Description	Remove			
<input type="checkbox"/>	Approval User	An approval user role which grants permissions to create/read/cancel a request, and read workflows.				
<input type="checkbox"/>	Automation Analytics Editor	An Automation Analytics Editor role that grants read-write permissions.				
<input type="checkbox"/>	Automation Services Catalog user	A catalog user roles grants read and order permissions				
<input type="checkbox"/>	Compliance viewer	A Compliance role that grants read access to any Compliance resource.				
<input type="checkbox"/>	Drift viewer	Perform read only operation against Drift Analysis resources.				
<input checked="" type="checkbox"/>	Inventory Hosts Administrator	Be able to read and edit Inventory Hosts data.				

 **Remove role?** ✕

Members in the group will lose the permissions in the **Inventory Hosts Administrator** role

**Remove role**  **Cancel**

 **Warning** ✕

Once you edit the **Default access** group, the system will no longer update it with new default access roles. The group name will change to **Custom default access**.

I understand, and I want to continue.

**Continue**  **Cancel**

If the users are also members of additional User Access Groups, make sure to review and remove the Inventory Hosts Administrator role from those groups as needed.

Once the role has been removed, the User Access controls behave as expected: Users given custom roles to limit their views to certain Inventory groups and systems only see those Inventory groups and systems.

### 3.3.1.3. Adjustment considerations

- If you have more than two IT groups, you can create as many custom roles and user groups as you need.
- If you are trying to grant the same people the same access to multiple Inventory groups, you can select more than one Inventory group to grant permissions within the same custom role.
- You can grant access to systems that are not part of any Inventory group. Add the Ungrouped systems in the Group definition of the host permissions to the custom role.
- Remember that as long the Inventory hosts administrator role is still in the Default Access group, all users who have that role still have access to everything.
- If you do not select Ungrouped systems in your custom roles, users with those roles will not be able to see any ungrouped systems once you remove the inventory hosts administrator permission from the Default access group.

### 3.3.2. Scenario 2: Access to ungrouped systems

In this example, an admin wants to give a group of users access to ungrouped systems, but not to grouped systems.

#### Step 1: Create a custom role

1. Navigate to **User Access > Roles** and click **Create role**. The Create Role wizard displays.

**Create role** ✕

- 1 Create role
- 2 Add permissions
- 3 Review details

### Create role

Create a role from scratch  
 Copy an existing role

**Role name \***

**Role description**

Next
Back
Cancel

1. Set the role name and description and click **Next**.
2. Add the inventory:hosts permissions and click **Next**.

**Create role** ✕

- 1 Create role
- 2 Add permissions
- 3 Define Inventory group access
- 4 Review details

Selected permissions
inventory:hosts:write ✕
inventory:hosts:read ✕

### Add permissions

Select permissions to add to your role

2 selected ▾
Applications ▾
Filter by application ▾
1 - 6 of 6 ▾

Applications
inventory ✕
Clear filters

Application	Resource type	Operation
<input type="checkbox"/> inventory	staleness	read
<input type="checkbox"/> inventory	staleness	write
<input checked="" type="checkbox"/> inventory	hosts	read
<input checked="" type="checkbox"/> inventory	hosts	write
<input type="checkbox"/> inventory	groups	read
<input type="checkbox"/> inventory	groups	write

1 - 6 of 6 ▾
⏪ <
1
> ⏩
of 1

Next
Back
Cancel

Configure both of the permissions to apply to the Group definition named **Ungrouped systems**. Click **Next**.

**Create role** ✕

- 1 Create role
- 2 Add permissions
- 3 Define Inventory group access
- 4 Review details

### Review details

Specify which inventory groups you'd like to give access for these permissions

Permissions	Group definition	
hosts:read *	<div style="border: 1px solid #ccc; padding: 2px;">           Select groups <span style="float: right;">Add permission to these groups. <span style="font-size: 0.8em;">+</span> ▼</span> </div>	<a href="#">Copy to all</a>
hosts:write *	<div style="border: 1px solid #ccc; padding: 5px;">           Select groups <span style="float: right;">▼</span>  <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <input type="text" value="ung"/> </div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">           Select all (1)         </div> <div style="border: 1px solid #ccc; padding: 2px;"> <input type="checkbox"/> Ungrouped systems         </div> </div>	

Next
Back
Cancel

Review the details of the role and click **Submit**.

**Create role** ✕

- 1 Create role
- 2 Add permissions
- 3 Define Inventory group access
- 4 Review details

### Review details

Review and confirm the details for your role, or click Back to revise.

**Name** Support Team

**Description** User Access Role for the Support Team

Permissions	Application	Resource type	Operation
	inventory	hosts	read
	inventory	hosts	write

Resource definitions	Permission	Group definition
	inventory:hosts:read	Ungrouped systems
	inventory:hosts:write	Ungrouped systems

Submit
Back
Cancel

## Step 2: Add the custom role to an RBAC group

1. Once you create the custom role, navigate to **User Access > Groups** and click **Create Group** to create a User Access (RBAC) group.
2. Name the group, select the new custom role, and select the users to whom you want to assign this role.

**Create group**
✕

- 1 Name and description
- 2 Add roles
- 3 Add members
- 4 Review details

### Review details

<b>Group name</b>	Support Team - User group
<b>Group description</b>	User Access Group for the Support Team
<b>Roles</b>	Support Team
<b>Members</b>	insights-test-day-03

Submit
Back
Cancel



### NOTE

These steps only work when the users do *not* have the inventory hosts admin role assigned from the Default Access group. To check this, navigate to **User Access > Groups** and click on the Default Access group at the top. If that role is in the group, remove it, because that role gives users access to the whole inventory - including both ungrouped and grouped systems.

After you remove the role, the selected set of users only has access to ungrouped systems in your inventory.

### 3.3.3. Known limitations

- Users who are Organization Administrators (members of the Default admin access group) will always have full access to systems and Inventory groups.
- A user without permission on the system will not be able to add it to a Remediation. However, if an existing Remediation with active systems was created in the past, the user will still be able to run it, even if the permissions have been removed on that system for the current user.

**NOTE**

Before enabling Inventory groups in your organization, review your Notifications configuration to ensure that only appropriate groups of users are configured to receive Email notifications. If you do not review your Notifications configuration, users might receive alerts triggered by systems outside of their Inventory group permission scope.

**Additional Resources**

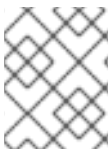
- For more information about user access, refer to [User Access Guide for Role-based Access Control \(RBAC\)](#).

## CHAPTER 4. EXPORTING INVENTORY DATA

You can use the export service for inventory to export a list of systems and their data from your Insights inventory. You can specify CSV or JSON as the output format. The export process takes place asynchronously, so it runs in the background. The service is available in both the Insights UI and through the export service API.

The exported content includes the following information about each system in your inventory:

- **host\_id**
- **fqdn** (Fully Qualified Domain Name)
- **display\_name**
- **group\_id**
- **group\_name**
- **state**
- **os\_release**
- **updated**
- **subscription\_manager\_id**
- **satellite\_id**
- **tags**
- **host\_type**



### NOTE

The export service currently exports information about all systems in your inventory. Support for filters will be available in a future release.

The Inventory export service works differently from the export function in other services, such as Advisor. Some of the differences are:

- Inventory export operates asynchronously
- Exports the entire inventory to one continuous file (no pagination in the export file)
- Retains generated files for 7 days
- Uses token-based service accounts for authorization if using the export service API



### IMPORTANT

Your RBAC permissions affect the system information you can export. You must have **inventory:hosts:read** permission for a system to export system information.

### 4.1. INVENTORY DATA FILES



The inventory export process creates and downloads a zip file. The zip file contains the following files:

- **id.suffix** – the export data file, with the file name format of **id.json** for JSON files, or **id.csv** for CSV files. For example: **f26a57ac-1efc-4831-9c26-c818b6060ddf.json**
- **README.md** – the export manifest for the JSON/CSV file, which lists the downloaded files, any errors, and instructions for obtaining help
- **meta.json** – describes the export operation – requestor, date, Organization ID, and file metadata (such as the filename of the JSON/CSV file)

## 4.2. EXPORTING SYSTEM INVENTORY FROM THE INSIGHTS UI

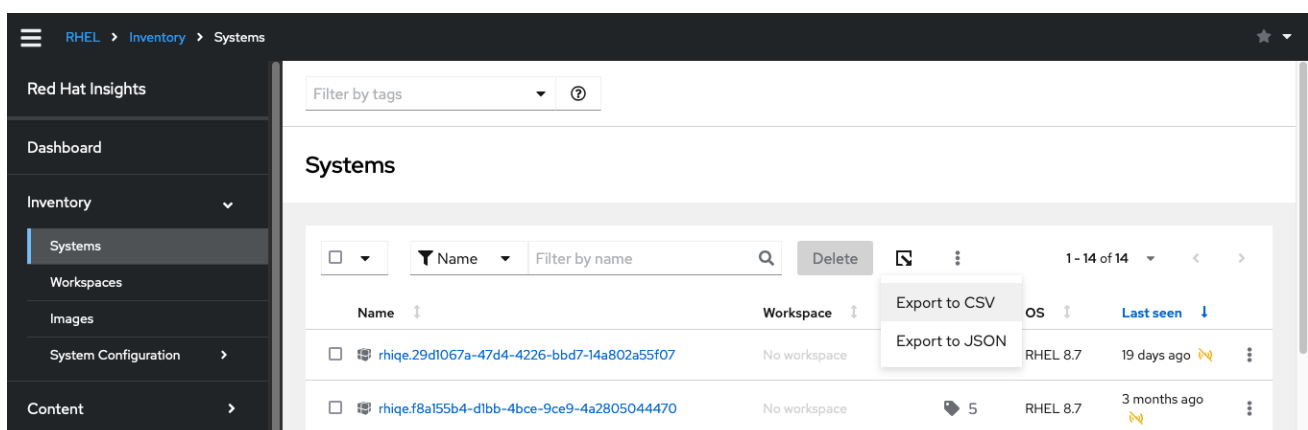
You can export inventory data from the Insights UI. The inventory data export service works differently from the export service for other Insights services, such as Advisor.

### Prerequisites

- RBAC permissions for the systems you want to view and export
  - `Inventory:hosts:read` (`inventory:hosts:read *` for all systems in inventory)
- A User Access role for workspaces. For more information about User Access roles, see [User access to workspaces](#).

### Procedure

1. Navigate to `Inventory > Systems`. The list of systems displays.
2. Click the Export icon next to the options icon ( `:` ). The drop-down menu displays.
3. Select CSV or JSON as the export format. A status message displays: **Preparing export. Once complete, your download will start automatically.**



When the download completes, a browser window automatically opens to display the results.

If you remain on the Systems page after requesting the download, status messages from Insights appear with updates on the progress of the export operation.

## 4.3. EXPORTING SYSTEM INVENTORY USING THE EXPORT API

You can use the Export API to export your inventory data. Use the REST API entry point: [console.redhat.com/api/export/v1](https://console.redhat.com/api/export/v1).

The Export Service API supports the GET, POST, and DELETE HTTP methods. The API offers the following services:

- POST /exports
- GET /exports
- GET /exports/*id*
- DELETE /exports/*id*
- GET /exports/*id*/status

The API works asynchronously. You can submit the POST /exports request for export from the Export API and receive a reply with an ID for that export. You can then use that ID to monitor the progress of the export operation with the GET /exports/*id*/status request. When the generated export is complete, you can download it (GET /exports/*id*) or delete it (DELETE /exports/*id*).

Successful requests return the following responses:

- 200 – Success
- 202 – Successfully deleted (for the DELETE method)

For more information about the operations, schemas, and objects, see [Consoledot Export Service](#).

### 4.3.1. Requesting the system inventory export

Before you can request the exported data file, you need to obtain a unique ID for the download. To obtain the ID, issue a POST request. The server returns a response that includes the ID. Use the ID in any request that requires the *id* parameter, such as GET /exports/*id*.

#### Prerequisites

- Token-based service account with the appropriate permissions for your systems
- RBAC permissions for the systems you want to view and export
  - Inventory:hosts:read (inventory:hosts:read \* for all systems in inventory)
- A User Access role for workspaces. For more information about User Access roles, see [User access to workspaces](#).

#### Procedure

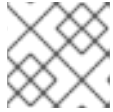
1. Create a request for the export service, or use this sample request code:

```
{
  "name": "Inventory Export",
  "format": "json",
  "sources": [
    {
      "application": "urn:redhat:application:inventory",
```

```

    "resource": "urn:redhat:application:inventory:export:systems",
  }
]
}

```

**NOTE**

You can request CSV or JSON as your export format.

- In the Hybrid Cloud Console, navigate to the API documentation:  
<https://console.redhat.com/docs/api/export>.

**NOTE**

You can use the API documentation to experiment and run queries against the API before writing your own custom client and/or use the APIs in your automation.

- Select POST /export.
- Remove the existing sample code in the **Request Body** window and paste the request code into the window.
- Click **Execute**. This request initiates the export process. The curl request and server response appear, along with the result codes for the POST operation.
- Look for the *id* field in the server response. Copy and save the string value for *id*. Use this value for *id* in your requests.
- Optional.** Issue the GET /exports request. The server returns the curl request, request URL, and response codes.
- Optional.** To request the status of the export request, issue the GET /exports/ *id*/status request.
- When the export has completed, issue the GET /exports/*id* request, with the ID string that you copied in place of *id*. The server returns a link to download the export file (the payload).
- Click **Download File**. When the download completes, a notification message appears in your browser.
- Click the browser notification to locate the downloaded zip file.

**NOTE**

The server retains export files for 7 days.

### 4.3.2. Deleting export files

To delete exported files, issue the DELETE /exports/*id* request.

#### Additional resources

- Export service API for multiple sources: <https://developers.redhat.com/api-catalog/api/export-service>
- Export service API doc within the console: <https://console.redhat.com/docs/api/export>
- For the latest OpenAPI specifications, see <https://swagger.io/specification/>

### 4.3.3. Automating inventory export using Ansible playbooks

You can use an Ansible playbook to automate the inventory export process. The playbook is a generic playbook for the export service that uses token-based service accounts for authentication.

#### Procedure

1. Navigate to <https://github.com/jeromemarc/insights-inventory-export>.
2. Download the `inventory-export.yml` playbook.
3. Run the playbook. The playbook does everything from requesting the export `id`, to requesting download status, to requesting the downloaded payload.

#### Additional resources

For more information about service accounts, refer to the KB article: [Transition of Red Hat Hybrid Cloud Console APIs from basic authentication to token-based authentication via service accounts](#).

### 4.3.4. Using the inventory export service for multiple Insights services

You can use the inventory export service for multiple services, such as inventory and notifications. To request multiple services, include source information for each service that you want to request in your POST `/exports` request. For example:

```
{
  "name": "Inventory Export multiple sources",
  "format": "json",
  "sources": [
    {
      "application": "urn:redhat:application:inventory",
      "resource": "urn:redhat:application:inventory:export:systems",
      "filters": {}
    },
    {
      "application": "urn:redhat:application:notifications",
      "resource": "urn:redhat:application:notifications:export:events",
      "filters": {}
    }
  ]
}
```

The POST `/exports` request returns a unique `id` for each export.

The GET `/exports` request returns a zip file that includes multiple JSON or CSV files, one for each service that you request.

## CHAPTER 5. SYSTEMS LIFECYCLE IN THE INVENTORY APPLICATION

A system is a Red Hat Enterprise Linux (RHEL) host that is managed by the Red Hat Insights inventory in the Red Hat Hybrid Cloud Console. System activity is automatically monitored by Red Hat. All systems registered with inventory follow a lifecycle that includes the following states: **fresh**, **stale**, and **stale warning**. The state that a system resides in depends on the last time it was reported by a data collector to the inventory application. Systems are automatically deleted from inventory if they do not report within a given time frame. The goal of the deletion mechanism is to maintain an up-to-date, accurate view of your inventory.

Here is a description of each state:

### Fresh

The default configuration requires systems to communicate with Red Hat daily. A system with the status of fresh, is active and is regularly reported to the inventory application. It will be reported by one of the data collectors described in section 1.2. Most systems are in this state during typical operations.

### Stale

A system with the status of stale, has *NOT* been reported to the inventory application in the last day, which is equivalent to the last 26 hours.

### Stale warning

A system with the status of stale warning, has *NOT* been reported to the inventory application in the last 14 days. When reaching this state, a system is flagged for automatic deletion. Once a system is removed from inventory it will no longer appear in the inventory application and Insights data analysis results will no longer be available.

## 5.1. DETERMINING SYSTEM STATE IN INVENTORY

There are two ways to determine which state a system is currently in. Use this procedure to identify system state on the **Systems** page:

### Prerequisites

- You have Inventory Hosts Viewer access.

### Procedure

1. Navigate to the [Red Hat Insights > RHEL > Inventory](#) page.
2. Click the **Filter** drop down list, select **Status**.
3. Click the **Filter by status** dropdown and select the state(s) you want to include in your query.
4. Click **Reset filters** to clear your query.

Alternatively, you can discover system(s) state(s) on the **Dashboard**:

### Prerequisites

- You have Inventory Hosts Administrator access.

## Procedure

1. Navigate to the [Red Hat Insights for Red Hat Enterprise Linux dashboard](#) page.
2. Look at the top left of the screen and you will see the total number of Systems registered with Insights for Red Hat Enterprise Linux.
3. Look to the right of the total number and you will see the number of **stale systems** and the number of **systems to be removed**
4. Click the blue **stale systems** link or the **systems to be removed** link, if applicable, to navigate to the inventory page and view more granular details.

### 5.1.1. Modifying system staleness and deletion time limits in inventory

By default, system states have the following time limits:

- Systems are labeled **stale** if they are not reported in 1 day. A warning icon appears of the top of the **Systems** page in the **Last seen:** field.
- Systems are labeled **stale warning** if they are not reported within 7 days. In this case the **Last seen:** field turns red.
- Systems that are not reported in 14 days are deleted. `git st`

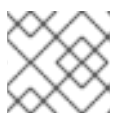
There are situations where a system is offline for an extended period of time, but is still being used. For example, test environments are often kept offline except when testing. Edge devices, submarines or Internet of Things (IoT) devices, can be out of range of communication for extended periods of time. You can modify the system staleness and deletion time limits (for both conventional and immutable systems), to accommodate these unique situations. Do this so that systems that are offline but still active are not deleted. Note that any changes that you make to these limits affect all of your conventional or immutable systems.

## Prerequisites

- You are logged into the Red Hat Hybrid Cloud Console as a user with the Organization Staleness and Deletion Administrator role.

## Procedure

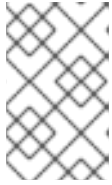
1. On the Red Hat Hybrid Cloud Console main page, click **RHEL** in the **Red Hat Insights** tile.
2. In the left navigation bar, click **Inventory** > **System Configuration** > **Staleness and Deletion**. The **Staleness and Deletion** page displays the current settings for system staleness, system stale warning, and system deletion for conventional systems.
3. Optional: To manage the staleness and configuration settings for edge (immutable) systems, select the **Immutable (OSTree)** tab.
4. To change these values, click **Edit**. The drop-down arrows next to each value are now enabled.
5. Click the arrow next to the value that you want to change and then select a new value.



### NOTE

The system stale warning value must be less than the system deletion value.

6. Optional: To revert to the default values for the organization, click **Reset**.
7. Click **Save** to save your changes.

**NOTE**

If you set the system deletion maximum time to less than the current maximum time, systems that have been stale for longer than then new maximum time will be deleted.

## CHAPTER 6. INVENTORY GROUPS

Inventory groups allow you to select specific systems and group them together. You can view and manage the individual Inventory groups and the system membership of each group. In addition, you can filter your system lists across applications by Inventory groups. You can also manage user access to specific Inventory groups to enhance security.

Inventory groups have the following characteristics:

- Inventory groups are only for systems.
- You cannot add Inventory groups as children of another Inventory group.
- Each system can belong to only *one* Inventory group.
- Using Inventory groups is not mandatory; systems that are not assigned to specific Inventory groups can remain unassigned.

### Additional resources

- For more information about user access, refer to [User Access Guide for Role-based Access Control \(RBAC\)](#).
- For more information about user access to Inventory groups, refer to [User access for RBAC in system inventory](#).

## 6.1. CREATING INVENTORY GROUPS

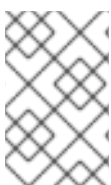
### Prerequisites

- You must be an Organization administrator (member of the Default administrator access group) or have the Inventory group Administrator role.

### Procedure

1. On the Red Hat Hybrid Cloud Console, navigate to **Inventory**.
2. Click the Inventory drop-down menu and select **Inventory groups**.
3. Click **Create Inventory group**. The **Create Inventory group** dialog box displays.
4. Type a name for the Inventory group in the **Inventory group name** field. Names can consist of lowercase letters, numbers, spaces, hyphens (-), and underscores (\_).
5. Click **Create**. A **Inventory group created** message displays, and the new group appears in the list of Inventory groups.

## 6.2. ADDING SYSTEMS TO A NEWLY CREATED INVENTORY GROUP



### NOTE

Each system can belong to only one Inventory group. In the current release of Inventory groups, a system cannot be reassigned to a different group in a single step. You must first remove the system from its current group, and then assign it to a new group.



## Prerequisites

- Organization Administrator access to Insights for Red Hat Enterprise Linux, or Inventory groups administrator permissions to the group, or both `inventory:groups:write` and `inventory:groups:read` permissions to the group

## Procedure

1. On the Red Hat Hybrid Cloud Console, navigate to **Inventory**.
2. Select **Inventory groups**.
3. Click the name of the group to which you want to add systems. A page for **Inventory groups** displays with the name of the Inventory group and two tabs, **Systems** and **Group Details**.
4. On the **Systems** tab, click **Add systems**. The **Add systems** dialog box displays and shows the systems available for you to view in inventory.
5. Select the systems you want to add to the Inventory group.



### NOTE

If you select a system that already belongs to another Inventory group, a warning message displays: *One or more of the selected systems already belong to {a workspace}. Make sure that all the systems you have selected are ungrouped, or you will not be able to proceed.*

6. When you have finished selecting systems, click **Add systems**. The **Inventory groups** page displays and includes the systems you added to the group.

## 6.2.1. Adding a system and creating a group from the Inventory systems page

### Prerequisites

- Organization Administrator access to Insights for Red Hat Enterprise Linux, or Inventory group administrator permissions to the group, or both `inventory:groups:write` and `inventory:groups:read` permissions to the group

### Procedure

1. On the Red Hat Hybrid Cloud Console, navigate to **Inventory**. The list of systems in your inventory appears.
2. Locate the system that you want to add.
3. Click the **More options** icon ( `:` ) on the far right side of the system listing.
4. Select **Add to Inventory group** from the pop-up menu. The **Add to Inventory group** dialog box displays.
5. Click **Create a new Inventory group**. The **Create Inventory group** dialog box displays.
6. Type a name for the new group in the **Name** field and click **Create**.

The **Inventory** page appears and displays a status (success or failure) message.

## 6.3. REMOVING SYSTEMS FROM THE INVENTORY GROUP

You can remove systems from the Inventory group from two pages in the Red Hat Hybrid Cloud Console: the Inventory groups page and the Systems page.

### 6.3.1. Removing systems from the Inventory group using the Inventory groups page

#### Prerequisites

- You must be an Organization administrator (member of the Default admin access group), or have the **Inventory group Administrator** role, or have the `inventory:group:write` permissions for that particular Inventory group.

#### Procedure

1. On the Red Hat Hybrid Cloud Console, navigate to **Inventory**.
2. Click the **Inventory** drop-down menu and select **Inventory groups**. The **Inventory groups** page displays.
3. Select the Inventory group that contains the systems that you want to remove.
4. Locate the system that you want to remove from the Inventory group.
5. Click the **More options** icon ( `:` ) on the far right side of the system listing.
6. Select **Remove from Inventory group** from the pop-up menu. The **Remove from Inventory group?** dialog box displays.
7. **Optional:** To remove multiple systems from the Inventory group at once, select each system you want to remove, and then select **Remove from Inventory group** from the **More options** menu (the options icon ( `:` )) in the toolbar.
8. Click **Remove**.

The Inventory group page displays and shows the updated Inventory group with a status (success or failure) message.

### 6.3.2. Removing systems from the Inventory group using the Systems page

#### Prerequisites

- Organization Administrator access to Insights for Red Hat Enterprise Linux, or **Inventory group administrator** permissions to the Inventory group, or both `inventory:groups:write` and `inventory:groups:read` permissions to the Inventory group

#### Procedure

1. On the Red Hat Hybrid Cloud Console, navigate to **Inventory**.
2. Click the **Inventory** drop-down menu and select **Systems**. The **Systems** page displays.
3. Locate the system that you want to remove from the Inventory group.
4. Click the **More options** icon ( `:` ) on the far right side of the system listing.

5. Select **Remove from Inventory group** from the pop-up menu. The **Remove from Inventory group?** dialog box displays.



#### NOTE

If any of the systems you selected do not belong to any Inventory group, the **Remove from Inventory group** option remains disabled. Make sure that you select only systems that belong to the Inventory group.

6. **Optional:** To remove multiple systems from the Inventory group, select each system you want to remove, and then select **Remove from Inventory group** from the **More options** (the options icon ( : )) menu.
7. Click **Remove**.

The Systems page displays and shows a status (success or failure) message.

## 6.4. RENAMING THE INVENTORY GROUP

### Prerequisites

- You must be an Organization administrator (member of the Default Administrator access group), or have the Inventory group Administrator role, or have the inventory:group:write permissions for that particular Inventory group.

### Procedure

1. On the Red Hat Hybrid Cloud Console, navigate to **Inventory**.
2. Click the **Inventory** drop-down menu and select **Inventory groups**. The **Inventory groups** page displays.
3. Click the **Inventory group actions** drop-down menu in the upper right corner of the **Inventory groups** page.
4. Select **Rename** from the drop-down menu. The **Rename Inventory group** dialog box displays.
5. Type the new name into the **Name** field, and click **Save**.
6. The **Inventory groups** page shows the renamed Inventory group in the list of Inventory groups.

## 6.5. DELETING THE INVENTORY GROUP



#### NOTE

Before you delete a Inventory group, make sure that the Inventory group does not contain any systems. You can only delete empty Inventory groups. If you attempt to delete a Inventory group that still contains systems, Insights returns a warning message.

### Prerequisites

- You must be an Organization administrator (member of the Default admin access group), or have the Inventory group Administrator role, or have the inventory:group:write permissions for that particular Inventory group.

### Procedure

1. On the Red Hat Hybrid Cloud Console, navigate to **Inventory**.
2. Click the **Inventory** drop-down menu and select **Inventory groups**. The **Inventory groups** page displays.
3. Click the options icon ( **:** ) on the far right side of the listing for the group you want to delete.
4. Select **Delete** from the pop-up menu. The **Delete Inventory group** dialog box displays.
5. Select the checkbox to acknowledge that the delete operation cannot be undone. Click **Delete**.

The **Inventory groups** page shows an updated list of Inventory groups and a status (success or failure) message.



### NOTE

You can also delete the Inventory group from within the page for the Inventory group itself. Navigate to the Inventory group and click the **Actions** drop-down menu, and then select **Delete**.

## CHAPTER 7. CONFIGURING NOTIFICATIONS FOR INVENTORY EVENTS

The Inventory service triggers three types of events:

- New system registered
- System deleted
- Validation error

The **New system registered** and **System deleted** events trigger when you register a new system in inventory, or when a system is removed from inventory (either manually or when it becomes stale and Insights automatically removes it).

**Validation error** events trigger when data in a payload from **insights-client** is not valid (corrupted data, incorrect values, or other issues). The validation process follows these steps:

- **insights-client** runs on the system and generates a payload.
- **insights-client** uploads the payload to the Hybrid Cloud Console.
- The Hybrid Cloud Console receives the payload and validates it. The validation event triggers at this step. A validation error means that the payload cannot be processed, and that the console and Insights services cannot use its data.

You can configure notifications for these events using the Notifications service in the Red Hat Hybrid Cloud Console. The Notifications service enables you to configure responses to these events for your account. You can send email notifications to groups of users, or you can forward events to third-party applications, such as Splunk, ServiceNow, Event-Driven Ansible, Slack, Microsoft Teams, or Google Chat. You can also forward notifications, using a generic webhook with the Integrations service.



### NOTE

To receive Notifications emails, users must subscribe to email notifications in their user preferences. Users may choose to receive each email notification individually, or they may subscribe to a daily digest email. For more information, refer to [Configuring user preferences for email notifications](#).

The **New system registered** and **System deleted** events are particularly useful for driving automation, and for integrating Red Hat Insights into your operational workflows. For example, you can configure these events to automatically launch compliance or malware checks, validate systems assignments to Workspaces, update external CMDB records, or continuously monitor your RHEL environment.

### 7.1. SETTING UP ORGANIZATION NOTIFICATIONS FOR INVENTORY EVENTS



### NOTE

Make sure that you configure third-party system integrations in the Hybrid Cloud Console, as well as any behavior groups that should receive inventory notifications. For more information about third-party system integrations, refer to [Integrating the Red Hat Hybrid Cloud Console with third-party applications](#).

## Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console as a Notifications Administrator.

## Procedure

- Navigate to **Settings > Notifications > Configure Events**

The screenshot shows the 'Configure Events' interface in the Red Hat Hybrid Cloud Console. The left sidebar contains navigation options: Settings, Integrations, Notifications (with a dropdown arrow), Overview, Configure Events (highlighted), Notification Preferences, and Learning Resources. The main content area is titled 'Configure Events' and includes a sub-header 'Configure which event notifications different users within your organization are entitled to receive.' Below this, there are tabs for 'Red Hat Enterprise Linux', 'Console', and 'OpenShift'. The 'Configuration' tab is active, showing a table of event types. The table has columns for 'Event Type', 'Service', and 'Configuration'. The 'Service' column is filtered to 'Inventory'. A dropdown menu is open for the 'New system registered' event type, showing a list of behavior groups with checkboxes. The 'SPLUNK\_AUTOMATION\_GROUP' checkbox is checked. The table lists the following event types: 'Validation error', 'New system registered', and 'System deleted'. The 'New system registered' event type has a description: 'A new system was registered in Inventory'.

- In the **Configuration** tab, select the **Service** filter.
- Click **Filter by service**, and then select **Inventory** from the drop-down list. The inventory events appear in the list of events.
- Select the event type you want to configure (for example, **New system registered**).
- To configure the event type, click the **Edit** (pencil) icon at the far right of the event type. A drop-down list displays with the list of available behavior groups configured in your organization.
- Select the checkboxes next to the behavior groups you want to configure for the Inventory event type.
- When you have finished selecting behavior groups, click the checkmark next to the list of behavior groups to save your selections.

## Additional resources

For more information about behavior groups, refer to [Configuring notifications on the Red Hat Hybrid Cloud Console](#).

## 7.2. SETTING UP USER EMAIL NOTIFICATIONS FOR INVENTORY EVENTS



### NOTE

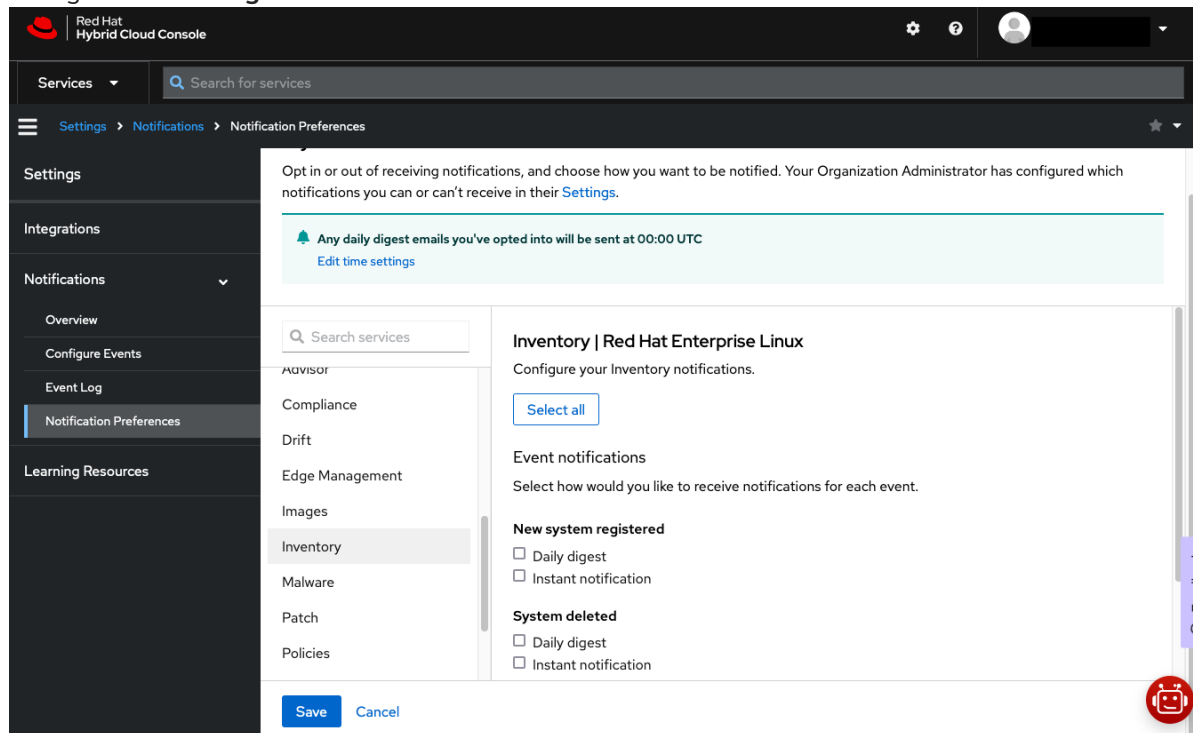
Make sure to configure email preferences for each user to receive email notifications. For more information about how to set up user preferences, refer to [Configuring user preferences for email notifications](#).

## Prerequisites

- You are a member of a user group that receives email notifications as part of a behavior group.
- The behavior group is configured to trigger email notifications for your systems and to send those notifications to the user group to which you belong.

## Procedure

1. Navigate to **Settings > Notifications > Notification Preferences**



2. Select **Inventory** from the list of services. The list of available notifications for Inventory displays.
3. Click the checkbox next to each type of notification you want to receive, or click **Select All** to receive all notifications for all Inventory events.
4. Click **Save**.



### NOTE

Configuring instant notifications might result in a large volume of email messages.

## PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate and prioritize your feedback regarding our documentation. Provide as much detail as possible, so that your request can be quickly addressed.

### Prerequisites

- You are logged in to the Red Hat Customer Portal.

### Procedure

To provide feedback, perform the following steps:

1. Click the following link: [Create Issue](#)
2. Describe the issue or enhancement in the **Summary** text box.
3. Provide details about the issue or requested enhancement in the **Description** text box.
4. Type your name in the **Reporter** text box.
5. Click the **Create** button.

This action creates a documentation ticket and routes it to the appropriate documentation team. Thank you for taking the time to provide feedback.