



# Red Hat Insights 1-latest

## システムインベントリーの表示と管理

インベントリーグループを使用したシステムインベントリーの整理とユーザーアクセスの管理



## Red Hat Insights 1-latest システムインベントリーの表示と管理

---

インベントリーグループを使用したシステムインベントリーの整理とユーザーアクセスの管理

## 法律上の通知

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.

## 概要

このドキュメントは、Insights for Red Hat Enterprise Linux ユーザーのシステムインベントリーを論理グループに整理し、システムへのユーザーアクセスを制御するのに役立ちます。Red Hat では、コード、ドキュメント、Web プロパティにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージをご覧ください。

---

## 目次

<b>第1章 インベントリーグループ</b> .....	<b>3</b>
1.1. インベントリーグループへのユーザーアクセス	3
1.2. ユーザーシナリオ	4
1.3. インベントリーグループの作成	18
1.4. 新しく作成したインベントリーグループへのシステムの追加	18
1.5. グループからのシステムの削除	19
1.6. グループ名の変更	21
1.7. グループの削除	21
<b>第2章 RED HAT ENTERPRISE LINUX 向け RED HAT INSIGHTS によるシステムの古さや削除の管理</b> .....	<b>23</b>
2.1. INSIGHTS FOR RED HAT ENTERPRISE LINUX システムの失効および削除	23
2.2. INSIGHTS FOR RED HAT ENTERPRISE LINUX システムの失効および削除までの期限の変更	23
2.3. INSIGHTS FOR RED HAT ENTERPRISE LINUX システムの状態の表示	24
<b>RED HAT ドキュメントへのフィードバック (英語のみ)</b> .....	<b>25</b>



# 第1章 インベントリーグループ

インベントリーグループを使用すると、特定のシステムを選択してグループ化できます。個々のインベントリーグループと各グループのシステムメンバーシップを表示および管理できます。さらに、複数のアプリケーションを対象とするシステムリストをグループでフィルタリングできます。特定のインベントリーグループへのユーザーアクセスを管理して、セキュリティを強化することもできます。

インベントリーグループには次の特徴があります。

- インベントリーグループはシステム専用です。
- インベントリーグループを別のインベントリーグループの子として追加することはできません。
- 各システムは1つのインベントリーグループにのみ属することができます。
- インベントリーグループの使用は必須ではありません。特定のグループに割り当てられていないシステムは、未割り当てのままにすることができます。

## 1.1. インベントリーグループへのユーザーアクセス

インベントリーグループは、ロールベースのアクセス (RBAC) をサポートします。RBAC を使用すると、ユーザーロールに基づいてインベントリーグループにカスタム権限を設定できます。

インベントリーグループ管理者のロールを使用すると、インベントリーグループを作成できます。このロールは、デフォルト管理者アクセスグループに自動的に組み込まれており、グループから削除することはできません。ただし、このロールを持つユーザーは、任意のインベントリーグループを変更できます。このロールは、システムインベントリー全体にアクセスする資格のあるユーザーにのみ提供してください。

ユーザーがインベントリーグループと RBAC を使用して特定のシステムへのアクセスを制限するには、そのユーザーがデフォルト管理者アクセスグループのメンバーであるか、インベントリーグループ管理者と User Access 管理者の両方のロールを持っている必要があります。

インベントリーグループユーザーには、グループレベルの RBAC 権限が付与されます。カスタム権限には次のものが含まれます。

- `inventory: groups: read`
  - グループの詳細ページを表示します。
- `inventory: groups: write`
  - グループの名前を変更します。
  - システムをグループに追加します。
- グループからシステムを削除します。



### 注記

ユーザーは、`inventory:hosts:read` 権限がなければ、グループ内のシステムを表示できません。

システムユーザーには、システムレベルの RBAC 権限が付与されます。システムユーザーは次のインベントリーグループ操作を実行できます。

- Inventory hosts read
  - インベントリーグループ内のすべてのシステムとその詳細を表示するか、グループ化されていないシステムを表示します。
  - 他の Insights サービスのシステムに関する情報を表示します。
- Inventory hosts write
  - システムの名前を変更します。
  - システムを削除します。

### 1.1.1. インベントリーグループを使用したユーザーアクセスの管理



#### 注記

インベントリーグループへのアクセス権がない場合は、**Inventory > Groups**に移動すると、**Inventory group access permissions needed** というメッセージが表示されます。

グループ自体にアクセスできない場合でも、読み取りアクセス権を持つシステムに割り当てられたインベントリーグループ名を表示できるようにしてください。システムを含むインベントリーグループを表示するには、Inventory Group Viewer ロールまたはインベントリーグループの表示権限が割り当てられている必要があります。



#### 重要

RBAC 設定を変更する前に、「ユーザーシナリオ」セクションの既知の制限事項のリストを確認してください。

ユーザーアクセスの管理、ロールの割り当て、ユーザーアクセスグループへのメンバー追加に関する詳細は、[ロールベースアクセス制御 \(RBAC\) の User Access 設定ガイド](#)を参照してください。

## 1.2. ユーザーシナリオ

このセクションには、インベントリーグループの機能を示す 2 つのシナリオが記載されています。これらのシナリオは手順の形式で記述されています。必要に応じて必須のステップを実行してテストできます。

### 1.2.1. シナリオ 1: 2 つの異なる IT チームが Insights を使用してシステムを管理する必要がある場合

このシナリオでは、同じ会社で働く 2 つの異なる IT チームが、Red Hat アカウント内で同じ Insights 組織を共有します。

- 各 IT チームは Red Hat Hybrid Cloud Console で自チームのシステムを完全に制御する必要がありますが、他のチームに属するシステムを表示したり変更したりすることはできません。
- 同じチーム内のすべてのユーザーは、インベントリーグループとシステムの両方に対して同じレベルのアクセス権を持ちます。アクセスレベルは必要に応じて調整できます。
- 両方の IT チームに属する通常のユーザーは、どのインベントリーグループにも属していないシステムを表示したり変更したりすることはできません。

- 組織管理者、またはインベントリーグループ管理者およびインベントリーホスト管理者のロールを持つユーザーは、インベントリー全体にアクセスできます。これらのロールを持たない他のユーザーは、インベントリー全体にはアクセスできません。

### 1.2.1.1. 初期段階

デフォルトでは、Red Hat Hybrid Cloud Console の組織管理者 (デフォルト管理者アクセスグループのメンバー) は、常にすべてのインベントリーグループへの読み取り/書き込みアクセス権と、すべてのシステムへの読み取り/書き込みアクセス権を持ちます。これには、インベントリーグループのオブジェクトとそれらに割り当てられたシステムに対して権限がどのように定義されているかは関係ありません。

これらのユーザーは、インベントリーグループのユーザーアクセスを設定できる唯一のユーザーです。通常のユーザーがユーザーアクセスを管理する必要がある場合、管理者はそのユーザーにインベントリーグループ管理者ロールとインベントリーホスト管理者ロールを個別に付与できます。

デフォルトでは、組織管理者ではないユーザーには、Default access グループからインベントリーホスト管理者ロールが割り当てられます。Default access グループは、これらのユーザーにインベントリー全体に対する `inventory:hosts:read` アクセス権および `inventory:hosts:write` アクセス権を付与します。これらの権限は、すべてのシステムおよびすべてのインベントリーグループに対する読み取り権限と書き込み権限を付与するものです。



#### 注記

Default access グループの詳細は、[Default access グループ](#) を参照してください。

### 1.2.1.2. アクセスの制限

#### 前提条件

- デフォルト管理者アクセスグループのメンバーである。

#### ステップ 1: インベントリーグループの作成

まず、2つの個別のインベントリーグループを作成します。(この例では2つのグループを作成しますが、必要な数だけ作成できます。)

- インベントリーグループ 1: IT team A - Systems
- インベントリーグループ 2: IT team B - Systems

## Create group ×

**Group name \***

IT team A - Systems

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

Create
Cancel

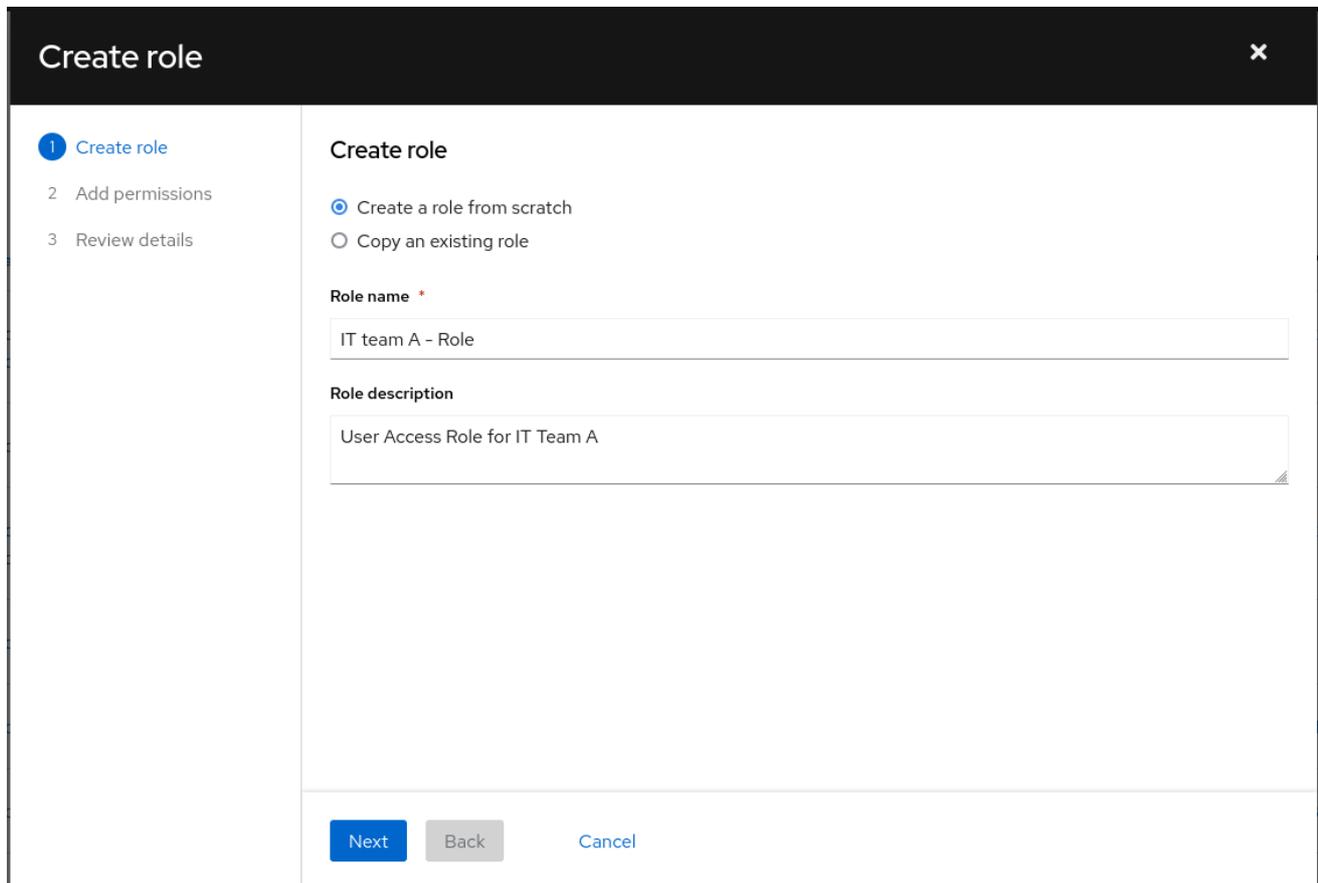
### ステップ 2: インベントリーグループへのシステムの追加

グループを作成したら、グループにシステムを追加します。各グループをクリックし、**Add systems** を選択します。

この段階では、ユーザーが所属するグループに関係なく、すべてのユーザーがすべてのシステムにアクセスできます。これは、ユーザーがグループ化されているかどうかに関係なく、すべてのシステムの表示を許可するインベントリーホスト管理者ロールが、ユーザーにまだ付与されているためです。

### ステップ 3: カスタムロールの作成

さまざまなインベントリーグループのアクセスをカスタマイズするには、それらのグループのカスタムロールを作成します。カスタムロールを作成するには、**User Access > Roles**に移動し、**Create role** をクリックします。ウィザードが開きます。ロールに名前を付け (例: IT Team - A Role)、**Next** をクリックします。



**Create role** ×

1 Create role  
2 Add permissions  
3 Review details

**Create role**

Create a role from scratch  
 Copy an existing role

**Role name \***

IT team A - Role

**Role description**

User Access Role for IT Team A

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

### ステップ 3a: カスタムロールに追加する権限の選択

ウィザードに **Add permissions** ステップが表示されます。このステップには 4 つのインベントリ権限オプションがあります。必要なアクセスレベルに応じて選択します。

グループとそのシステムへのフルアクセスを追加するには、次を選択します。

- 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

権限を選択したら、**Next** をクリックします。必要に応じて権限を調整できます。

権限の詳細は、「インベントリーグループへのユーザーアクセス」を参照してください。

### ステップ 3b: 選択したインベントリーグループへの権限の割り当て

このステップでは、権限を付与するインベントリーグループを選択します。この例では、現在のロールに対応するインベントリーグループを選択する方法を示します。たとえば、ロール **IT team A - Role** を作成し、各権限にインベントリーグループ **IT team A - Systems** を指定します。

×

## 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 5px;">1</span> <span style="float: right; cursor: pointer;">✖</span> <span style="float: right; color: #007bff;">Copy to all</span>
hosts:write *	Select groups <span style="background-color: #eee; border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;">1</span> <span style="float: right; cursor: pointer;">✖</span>
groups:read *	Select groups <span style="background-color: #eee; border: 1px solid #ccc; border-radius: 3px; padding: 2px 5px;">Add permission to these groups.</span> <span style="float: right; cursor: pointer;">✖</span>
groups:write *	Select groups <span style="border: 1px solid #ccc; padding: 5px;"> <input style="width: 100%; border: none;" type="text" value="it"/> </span> <div style="border: 1px solid #ccc; margin-top: 5px; padding: 5px;"> <p style="margin: 0; color: #007bff;">Select all (2)</p> <p><input type="checkbox"/> IT team A - Systems</p> <p><input type="checkbox"/> IT team B - Systems</p> </div>

Next
Back
Cancel

詳細を確認し、Submit をクリックします。

×

## 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

このセクションの手順を繰り返して、IT team B - Role という 2 番目のカスタムロールを作成し、IT team B - Systems インベントリグループを選択します。

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



### 注記

インベントリグループに含まれていないシステムへのアクセス権を、一方または両方の IT チームに付与できます。このようなシステムを追加するには、ホスト権限のグループ定義に表示される、グループ化されていないシステムをカスタムロールに追加します。

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

#### ステップ 4: User Access グループを作成してユーザーにカスタムロールを割り当てる

カスタムロールを作成したら、User Access グループを作成してカスタムロールをユーザーに割り当てます。

新しいグループを作成するには、**User Access > Groups**に移動し、**Create group** をクリックします。グループに名前を付け、新しく作成したロールを選択し、ロールを付与するユーザーを選択します。

たとえば、2つのITグループが次の権限を持っているとします。

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

これらのグループは次のように表示されます。

## Create group ✕

- Name and description
- Add roles
- Add members
- 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

## Create group ✕

- Name and description
- Add roles
- Add members
- 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

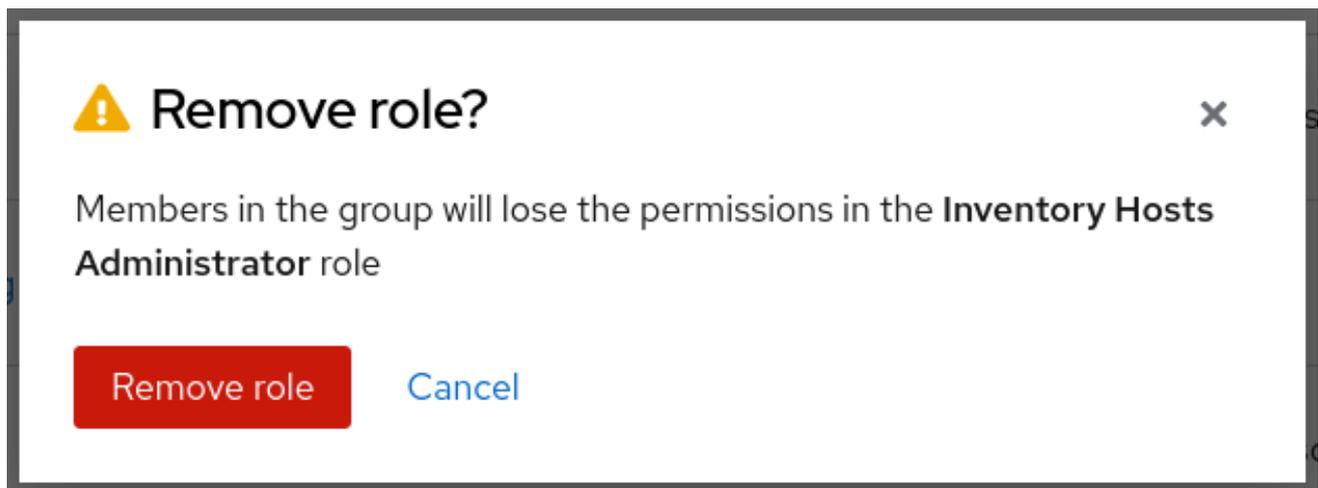
### ステップ 5: Default access グループからのインベントリーホスト管理者ロールの削除

上記のすべての手順を実行しても、この段階では、ユーザーが所属するグループに関係なく、すべてのユーザーがすべてのシステムにアクセスできます。これは、ユーザーがグループ化されているかどうかに関係なく、すべてのシステムの表示を許可するインベントリーホスト管理者ロールが、ユーザーにま

だ付与されているためです。

システムへのアクセスを制限するには、**User Access > Groups**に移動し、Default access グループを選択します。このグループからインベントリーホスト管理者のロールを削除します。

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



 **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.

ContinueCancel

ユーザーがその他の User Access グループのメンバーでもある場合は、必要に応じて、必ずそれらのグループからインベントリーホスト管理者ロールを確認して削除してください。

ロールを削除すると、User Access 制御が期待どおりに動作します。特定のグループおよびシステムに表示を制限するカスタムロールを付与したユーザーには、それらのグループおよびシステムのみが表示されます。

### 1.2.1.3. 調整に関する考慮事項

- 3つ以上の IT グループがある場合は、必要な数のカスタムロールとユーザーグループを作成できます。
- 同じユーザーに複数のインベントリーグループへの同じアクセス権を付与する場合は、複数のインベントリーグループを選択して、同じカスタムロール内で権限を付与できます。
- インベントリーグループに含まれていないシステムへのアクセス権を付与できます。ホスト権限のグループ定義のグループ化されていないシステムをカスタムロールに追加します。
- インベントリーホスト管理者ロールが Default access グループ内にある限り、そのロールを持つすべてのユーザーは引き続きすべてにアクセスできることに注意してください。
- カスタムロールでグループ化されていないシステムを選択しない場合、Default access グループからインベントリーホスト管理者権限を削除すると、そのカスタムロールを持つユーザーはグループ化されていないシステムを表示できなくなります。

### 1.2.2. シナリオ 2: グループ化されていないシステムへのアクセス

この例では、グループ化されたシステムではなく、グループ化されていないシステムへのアクセス権を、管理者がユーザーのグループに付与します。

#### ステップ 1: カスタムロールの作成

User Access > Roles に移動し、Create role をクリックします。Create Role ウィザードが表示されます。

**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

ロール名と説明を設定し、**Next** をクリックします。

inventory:hosts 権限を追加し、**Next** をクリックします。

**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
>
>>

Next
Back
Cancel

両方の権限を、**Ungrouped systems** という名前のグループ定義に適用するように設定します。Next をクリックします。

**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 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 style="width: 90%;" type="text" value="ung"/> </div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;"> <a href="#">Select all (1)</a> </div> <div style="border: 1px solid #ccc; padding: 2px;"> <input type="checkbox"/> Ungrouped systems         </div> </div>	

Next
Back
Cancel

ロールの詳細を確認し、**Submit** をクリックします。

**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

## ステップ 2: RBAC グループへのカスタムロールの追加

カスタムロールを作成したら、**User Access > Groups**に移動し、**Create Group**をクリックして User Access (RBAC) グループを作成します。グループに名前を付け、新しいカスタムロールを選択し、このロールを割り当てるユーザーを選択します。

**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



### 注記

上記の手順は、ユーザーが Default access グループから割り当てられるインベントリホスト管理者ロールを持っていない場合のみ機能します。これを確認するには、**User Access > Groups**に移動し、上部の Default access グループをクリックします。インベントリホスト管理者ロールがグループ内にある場合は、これを削除します。このロールにより、グループ化されていないシステムとグループ化されているシステムの両方を含むインベントリ全体へのアクセスがユーザーに付与されるためです。

ロールを削除すると、選択した一連のユーザーが、インベントリ内のグループ化されていないシステムにのみアクセスできるようになります。

### 1.2.3. 既知の制限

- 組織管理者 (デフォルト管理者アクセスグループのメンバー) であるユーザーは、常にシステムおよびインベントリグループへのフルアクセス権を持ちます。
- システムに対する権限のないユーザーは、システムを修復に追加できません。ただし、アクティブなシステムを使用した既存の修復が過去に作成されている場合は、そのシステムで現在のユーザーに対して権限が削除されていても、ユーザーは引き続きそれを実行できます。



## 注記

組織でインベントリーグループを有効にする前に、通知設定を確認して、適切なユーザーグループのみがメール通知を受信するように設定されていることを確認してください。通知設定を確認しないと、ユーザーのインベントリーグループからはアクセスできないシステムによってトリガーされたアラートをユーザーが受信する可能性があります。

## 1.3. インベントリーグループの作成

### 前提条件

- 組織管理者 (デフォルト管理者アクセスグループのメンバー) であるか、インベントリーグループ管理者ロールを持っている。

### 手順

1. Red Hat Hybrid Cloud Console で **Inventory** に移動します。
2. Inventory ドロップダウンメニューをクリックし、**Groups** を選択します。
3. **Create Group** をクリックします。 **Create group** ダイアログボックスが表示されます。
4. **Group name** フィールドにグループの名前を入力します。名前には、小文字、数字、スペース、ハイフン (-)、およびアンダースコア (\_) を使用できます。
5. **Create** をクリックします。 **Group Created** というメッセージが表示され、新しいグループがインベントリーグループのリストに表示されます。

## 1.4. 新しく作成したインベントリーグループへのシステムの追加



## 注記

各システムは1つのインベントリーグループにのみ属することができます。インベントリーグループの現在のリリースでは、1つのステップでシステムを別のグループに割り当て直すことはできません。まず現在のグループからシステムを削除してから、新しいグループに割り当てる必要があります。

### 前提条件

- Insights for Red Hat Enterprise Linux への組織管理者アクセス権、またはグループへのインベントリーグループ管理者権限、またはグループへの `inventory:groups:write` 権限と `inventory:groups:read` 権限の両方

### 手順

1. Red Hat Hybrid Cloud Console で **Inventory > Groups** に移動します。
2. システムを追加するグループの名前をクリックします。 **Inventory group** ページが表示され、グループの名前と2つのタブ **Systems** と **Group Details** が表示されます。
3. **Systems** タブで、 **Add systems** をクリックします。 **Add systems** ダイアログボックスが表示され、インベントリーで表示できるシステムが表示されます。

4. グループに追加するシステムを選択します。



### 注記

すでに別のグループに属しているシステムを選択すると、次の警告メッセージが表示されます。**One or more of the selected systems already belong to a group. Make sure that all the systems you have selected are ungrouped, or you will not be able to proceed.**

5. システムの選択が完了したら、**Add systems** をクリックします。**Inventory group** ページが表示され、グループに追加したシステムが含まれます。

## 1.4.1. インベントリーシステムページからのシステムの追加とグループの作成

### 前提条件

- Insights for Red Hat Enterprise Linux への組織管理者アクセス権、またはグループへのインベントリーグループ管理者権限、またはグループへの `inventory:groups:write` 権限と `inventory:groups:read` 権限の両方

### 手順

1. Red Hat Hybrid Cloud Console で **Inventory** に移動します。インベントリー内のシステムのリストが表示されます。
2. 追加するシステムを見つけます。
3. システムリストの右端にある **More options** アイコン (⋮) をクリックします。
4. ポップアップメニューから **Add to group** を選択します。**Add to group** ダイアログボックスが表示されます。
5. **Create a new group** をクリックします。**Create group** ダイアログボックスが表示されます。
6. **Name** フィールドに新しいグループの名前を入力し、**Create** をクリックします。

**Inventory** ページが表示され、ステータス (成功または失敗) メッセージが表示されます。

## 1.5. グループからのシステムの削除

Red Hat Hybrid Cloud Console の **Groups** ページと **Systems** ページで、インベントリーグループからシステムを削除できます。

### 1.5.1. Groups ページを使用したグループからのシステムの削除

#### 前提条件

- 組織管理者 (デフォルト管理者アクセスグループのメンバー) であるか、インベントリーグループ管理者ロールを持っているか、または特定のインベントリーグループに対する `inventory:group:write` 権限を持っている。

#### 手順

1. Red Hat Hybrid Cloud Console で、**Inventory** に移動します。
2. **Inventory** ドロップダウンメニューをクリックし、**Groups** を選択します。**Groups** ページが表示されます。
3. 削除するシステムが含まれるグループを選択します。
4. グループから削除するシステムを見つけます。
5. システムリストの右端にある **More options** アイコン (⋮) をクリックします。
6. ポップアップメニューから **Remove from group** を選択します。**Remove from group?** ダイアログボックスが表示されます。
7. **オプション**: グループから複数のシステムを一度に削除するには、削除する各システムを選択し、ツールバーの **More options** メニュー (⋮) から **Remove from group** を選択します。
8. **Remove** をクリックします。

Groups ページが表示され、更新されたグループがステータス (成功または失敗) メッセージとともに表示されます。

## 1.5.2. Systems ページを使用したグループからのシステムの削除

### 前提条件

- Insights for Red Hat Enterprise Linux への組織管理者アクセス権、またはグループへのインベントリグループ管理者権限、またはグループへの `inventory:groups:write` 権限と `inventory:groups:read` 権限の両方

### 手順

1. Red Hat Hybrid Cloud Console で **Inventory** に移動します。
2. **Inventory** ドロップダウンメニューをクリックし、**Systems** を選択します。**Systems** ページが表示されます。
3. グループから削除するシステムを見つけます。
4. システムリストの右端にある **More options** アイコン (⋮) をクリックします。
5. ポップアップメニューから **Remove from group** を選択します。**Remove from group?** ダイアログボックスが表示されます。



### 注記

選択したシステムがどのグループにも属していない場合、**Remove from group** オプションは無効のままです。グループに属するシステムのみを選択してください。

6. **オプション**: グループから複数のシステムを削除するには、削除する各システムを選択し、**More options** (⋮) メニューから **Remove from group** を選択します。
7. **Remove** をクリックします。

Systems ページが表示され、ステータス (成功または失敗) メッセージが表示されます。

## 1.6. グループ名の変更

### 前提条件

- 組織管理者 (デフォルト管理者アクセスグループのメンバー) であるか、インベントリーグループ管理者ロールを持っているか、または特定のインベントリーグループに対する `inventory:group:write` 権限を持っている。

### 手順

1. Red Hat Hybrid Cloud Console で、**Inventory** に移動します。
2. **Inventory** ドロップダウンメニューをクリックし、**Groups** を選択します。**Groups** ページが表示されます。
3. **Group** ページの右上隅にある **Group actions** ドロップダウンメニューをクリックします。
4. ドロップダウンメニューから **Rename** を選択します。**Rename group** ダイアログボックスが表示されます。
5. **Name** フィールドに新しい名前を入力し、**Save** をクリックします。
6. **Groups** ページのグループのリストに名前が変更されたグループが表示されます。

## 1.7. グループの削除



### 注記

グループを削除する前に、グループにシステムが含まれていないことを確認してください。削除できるのは空のグループのみです。システムがまだ含まれているグループを削除しようとする、Insights によって警告メッセージが返されます。

### 前提条件

- 組織管理者 (デフォルト管理者アクセスグループのメンバー) であるか、インベントリーグループ管理者ロールを持っているか、または特定のインベントリーグループに対する `inventory:group:write` 権限を持っている。

### 手順

1. Red Hat Hybrid Cloud Console で、**Inventory** に移動します。
2. **Inventory** ドロップダウンメニューをクリックし、**Groups** を選択します。**Groups** ページが表示されます。
3. 削除するグループのリストの右端にある **More options** アイコン (⋮) をクリックします。
4. ポップアップメニューから **Delete** を選択します。**Delete group** ダイアログボックスが表示されます。
5. チェックボックスを選択して、削除操作を元に戻すことができないことを承認します。**Delete** をクリックします。

**Groups** ページには、グループの更新されたリストとステータス (成功または失敗) メッセージが表示されます。



#### 注記

グループのページ内からグループを削除することもできます。グループに移動し、**Group Actions** ドロップダウンメニューをクリックし、ドロップダウンメニューから **Delete** を選択します。

## 第2章 RED HAT ENTERPRISE LINUX 向け RED HAT INSIGHTS によるシステムの古さや削除の管理

システム管理者は、Insights for Red Hat Enterprise Linux が管理するシステムが古いとみなされるタイミングと、システムがどの程度非アクティブであればインベントリから削除されるかなどを指定できます。

### 2.1. INSIGHTS FOR RED HAT ENTERPRISE LINUX システムの失効および削除

システムは、Red Hat Hybrid Cloud Console の Red Hat Insights Inventory 機能を通じて管理される Red Hat Enterprise Linux (RHEL) 環境です。システムアクティビティは、Red Hat によって自動的に監視されます。システムが指定された期間非アクティブである場合、そのシステムは古いものとしてラベル付けされます。システムが指定された期間使われていない場合は、システムの古さに関する警告が発行され、さらに指定された期間が経過すると、システムは Insights for Red Hat Enterprise Linux インベントリから削除されます。システムを削除した後は、再登録してインベントリに再度追加する必要があります。

デフォルト設定では、システムは毎日 Red Hat と通信する必要があります。システムが1日以内に Red Hat と通信しない場合は、自動的に **stale** とラベルがつけられ、システムページの上部にある **Last seen:** フィールドに警告アイコンが表示されます。7日以内に通信しない場合は、**stale warning** のラベルが付けられ、**Last seen:** フィールドが赤になります。Red Hat と14日以内に通信しない場合には、削除されます。ただし、システムが長期間オフラインであっても、引き続き使用されている状況があります。たとえば、テスト環境は、テストに使用される時以外はオフラインに保たれることがよくあります。潜水艦やモノのインターネット (IoT) デバイスなどのエッジデバイスは、長期間にわたって通信範囲外になることがあります。このような状況に対応するために、システムの古さや削除の値を変更できます。

### 2.2. INSIGHTS FOR RED HAT ENTERPRISE LINUX システムの失効および削除までの期限の変更

Insights for Red Hat Enterprise Linux によって管理される従来型システムとエッジ (不変) システムの両方について、システムの古さや削除の時間制限を変更できます。オフラインであるものの、まだアクティブなシステムが削除されないように、これを実行します。このような制限に対して加えた変更は、すべて従来のシステムまたはエッジシステムに影響することに注意してください。

#### 前提条件

- Organization Staleness and Deletion Administrator ロールを持つユーザーとして Red Hat Hybrid Cloud Console にログインしている。

#### 手順

1. Red Hat Hybrid Cloud Console メインページで、**Red Hat Insights** タイルで **RHEL** をクリックします。
2. 左側のナビゲーションバーで **Inventory > System Configuration > Staleness and Deletion** をクリックします。**Staleness and Deletion** ページには、従来のシステムのシステムの古さ、システムの古さの警告、およびシステムの削除の現在の設定が表示されます。
3. オプション: エッジ (不変) システムの古さや設定を管理するには、**Immutable (OSTree)** タブを選択します。

4. これらの値を変更するには、**Edit** をクリックします。各値の横にあるドロップダウン矢印が有効になります。
5. 変更する値の横にある矢印をクリックして、新しい値を選択します。



#### 注記

システムの古い警告値は、システムの削除値よりも小さくする必要があります。

6. オプション: 組織のデフォルト値に戻すには、**Reset** をクリックします。
7. **Save** をクリックして変更を保存します。



#### 注記

システムの削除までの最大時間を、現在の最大時間よりも少なく設定すると、新しく指定した最大時間と比較して、それ以上使用されていないシステムは削除されます。

## 2.3. INSIGHTS FOR RED HAT ENTERPRISE LINUX システムの状態の表示

システムの状態を表示して、システムが使用されていない期間や、今後予定されている可能性のある削除を確認できます。

### 前提条件

- Red Hat Hybrid Cloud Console にログインしている。

### 手順

1. Red Hat Hybrid Cloud Console メインページで、**Red Hat Insights** タイルで **RHEL** をクリックします。
2. 左側のナビゲーションバーで **Inventory > Systems** をクリックします。**Systems** ページには、Insights for Red Hat Enterprise Linux によって管理されるシステムがリスト表示されます。
3. システムの状態を表示するには、システム名をクリックしてページの下部までスクロールします。状態は **System status** ボックスに表示されます。**Active** または **Stale** のいずれかです。
  - 状態が **Stale** の場合は、システムページの最上部に警告アイコンが表示され、**Last seen:** フィールドに警告アイコンが表示されます。
  - 状態が指定の期間 **Stale** の場合、システムには **stale warning** のラベルが付けられ、**Last seen:** フィールドは赤になります。
4. システムの **Last seen:** フィールドに **stale warning** のアイコンがある場合は、アイコンをクリックすると、システムがインベントリーから削除される時期が表示されます。たとえば、システムは 11 日後に削除される予定です。

## RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するフィードバックをお寄せください。いただいたご要望に迅速に対応できるよう、できるだけ詳細にご記入ください。

### 前提条件

- Red Hat カスタマーポータルにログインしている。

### 手順

フィードバックを送信するには、以下の手順を実施します。

1. [Create Issue](#) にアクセスします。
2. **Summary** テキストボックスに、問題または機能拡張に関する説明を入力します。
3. **Description** テキストボックスに、問題または機能拡張のご要望に関する詳細を入力します。
4. **Reporter** テキストボックスに、お客様のお名前を入力します。
5. **Create** ボタンをクリックします。

これによりドキュメントに関するチケットが作成され、適切なドキュメントチームに転送されます。フィードバックの提供にご協力いただきありがとうございました。