Red Hat Insights 1-latest

システムインベントリーの表示と管理

インベントリーを使用してインフラストラクチャーを簡単に追跡および管理する

Last Updated: 2024-09-08

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

インベントリーを使用してインフラストラクチャーを簡単に追跡および管理する

法律上の通知

概要

このドキュメントは、Insights for Red Hat Enterprise Linux 管理者がシステムインベントリーを論理グループ (ワークスペースと呼ばれる) 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 プロパティー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、用語の置き換えは、今後の複数のリリースにわたって段階的に実施されます。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

第1章 インベントリーの概要

インベントリーは組織内のすべてのシステムの包括的なビューを提供し、インフラストラクチャーを簡単に追跡および管理できるようにします。インベントリーにアクセスするには、次の 2 つの方法があります。

- Hybrid Cloud Console
- 管理インベントリー API

システムをインベントリーで表示するには、Red Hat に登録する必要があります。Red Hat に登録する方法は複数あります。Red Hat Insights へのシステムの登録の詳細は、以下を参照してください。

Red Hat Insights のクライアント設定ガイド。

登録アプリケーションはデータコレクターと呼ばれます。インベントリーにレポートする Red Hat データコレクターには以下が含まれます。

- Red Hat Insights
- Red Hat Subscription Manager (RHSM)
- リモートホスト設定 (rhc)
- Red Hat Discovery Tool
- Red Hat Satellite

Insights の分析

システムが Red Hat Insights に登録されると、Insights はシステムの初期分析を実行します。ステータス情報 (システムの状態やシステムがアクティブかどうかなど) はインベントリーに保存されます。Hybrid Cloud Console の **System Details** ページから、システムに関する追加の詳細にアクセスできます。最初の分析が完了すると、Insights は毎日分析を実行し、フィードバックを提供し、システムの状態をインベントリーに報告します。

Insights の分析結果には、システムの問題を特定するアラートや、それらの問題を解決する方法に関する推奨事項が含まれる場合があります。

Insights はシステムがどの程度古くなっているかも監視し、特定の基準を使用して、定期的にレポートされていないシステムにフラグを立てます。一定期間が経過してもシステムからの報告がない場合、Insights はそれらのシステムに削除のフラグを立てます。

関連情報

Red Hat Insights の使用

Staleness and culling

1.1. インベントリーのデータコレクター

インベントリーに登録されている各システムは、多数のデータコレクターの 1 つからデータを取得します。データコレクターは定期的に実行され、収集したデータを Red Hat Hybrid Cloud Console と同期します。

システムは 1 つ以上のコレクターによってレポートできます。複数のコレクターが同じシステムの情報を提供する場合、インベントリーは重複排除メカニズムを使用して情報を結合します。このプロセスにより、システムがインベントリーに 1 回だけ表示されるようになります。

以下のデータコレクターは、システム情報を Red Hat Hybrid Cloud Console にアップロードします。

- **Red Hat Insights**。Insights はシステムデータを登録し、集約します。デフォルトでは、各システムで毎日実行され、システムデータが Red Hat Hybrid Cloud Console にアップロードされて処理されます。Insights が収集するデータは、すべてのデータコレクターが提供するすべての調査結果と推奨事項に反映されます。

- **Red Hat Subscription Manager (RHSM)**subscription-manager ツールは毎日実行され、組織内で Red Hat に登録されているすべてのシステムのリストを提供します。Insights も有効と設定されていない限り、Subscription Manager で収集されるデータだけでは推奨事項が提供されない点に注意してください。

- **リモートホスト設定 (rhc)**。rhc クライアントを使用すると、システムを Insights および RHSM に登録し、組織内のすべての RHEL システムの Insights 接続を設定できます。さらに、rhc クライアントを使用すると、システムの問題を簡単に見つけ、Insights によって生成された修復 Playbook を使用して修正できます。

- **Red Hat Discovery ツール**。Discovery ツールは、システムをスキャンして Red Hat ソフトウェアのインストールを検出し、システムインベントリーに含めるためのレポートを Red Hat Hybrid Cloud Console に提供します。このツールは手動で実行します。

- **Red Hat Satellite**。Satellite は、Red Hat Hybrid Cloud Console と統合できます。設定すると、Satellite は登録済みシステムのインベントリーを毎日アップロードし、Systems インベントリーと同期します。これには、Satellite Server および Capsule Server に登録されているすべてのシステムが含まれます。Red Hat Insights も有効になっていない限り、Satellite で収集されたデータだけでは調査結果や推奨事項は提供されない点に注意してください。

関連情報

Red Hat Insights クライアント

Red Hat Satellite

Red Hat Subscription Manager (RHSM)

サブスクリプションサービスのスタートガイド

Red Hat Discovery ツール

リモートホストの設定と管理 (rhc クライアント)

1.2. インベントリー内のシステムのビュー調整

最も重要な問題やシステムに集中できるように、インベントリービューを改良する方法はいくつかあります。**Name**、**Status**、**Operating System**、**Data Collector**、**remote host configuration status**、**Last seen**、**Workspace**、または **Tags** でフィルタリングできます。

前提条件

- インベントリーの Hosts Viewer の権限がある。

手順

1. Red Hat Hybrid Cloud Console で、ウィンドウの左側にある **Red Hat Enterprise Linux** ウィジェットを見つけます。
2. ウィジェットの下部にある **Insights** for **RHEL** をクリックします。
3. **Inventory** > **Systems** をクリックします。
4. **Name** フィルターのドロップダウンをクリックします。ドロップダウンメニューから、**Name**、**Status**、**Operating System**、**Data Collector**、**RHC status**、**Last seen**、**Workspace**、**Tags** などのオプションを選択します。
5. クエリー内で追加のフィルターを選択します。たとえば、**Operating System** フィルターを選択した場合は、ヘッダーの **Filter by operating system** をクリックして、特定のバージョンの RHEL を選択します。
6. フィルタリングする RHEL バージョンの横にあるチェックボックスをクリックします。
7. **オプション:** クエリーに複数のフィルターを追加するには、追加のフィルター (**Data Collector** など) をクリックします。**Data Collector** フィルターの右側に、**Filter by data collector** という 2 番目のドロップダウンが表示されます。
8. 必要なデータコレクターを選択します。この最初のフィルターはヘッダーのすぐ下に表示されます。必要に応じて、2 番目のフィルターを選択します。利用可能な 8 つのフィルターすべてをクエリーに適用できます。
9. クエリーを初期ょするには、**Reset filters** をクリックします。

関連情報

グローバルフィルターの詳細は、以下を参照してください。

システムのフィルタリングとグループ

1.3. インベントリーからのシステムの削除

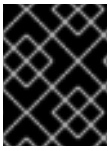
システムが古くなったり廃止されたりした場合は、インベントリーから削除できます。

前提条件

1. インベントリーの Hosts Administrator 権限がある。

手順

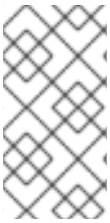
1. Red Hat Hybrid Cloud Console で、ウィンドウの左側にある **Red Hat Enterprise Linux** ウィジェットを見つけます。
2. ウィジェットの下部にある **Insights for Red Hat Enterprise Linux**をクリックします。
3. **Inventory > Systems**をクリックします。
4. 削除するシステムの左側にあるチェックボックスをオンにします。
5. フィルターの右側にある **Delete** ボタンをクリックします。**Delete from Inventory**の確認ダイアログボックスが表示されます。
6. Delete をクリックして、このアクションを確認します。



重要

選択したシステムは **すべての console.redhat.com アプリケーションおよびサービスから削除されます。**

画面の右上隅に、削除操作が開始されたことを示すメッセージボックスが表示されます。削除が完了すると、削除が成功したことを確認するメッセージボックスが表示されます。



注記

データコレクターが、**登録解除** または **購読解除していない** システムからデータをアップロードしている場合、システムがインベントリーに再表示される場合があります。システムを登録解除する手順/アクションについては、特定のデータコレクターのドキュメントを参照してください。

1.4. インベントリーのロールベースアクセス制御のユーザーアクセス

ユーザーアクセス機能は、Red Hat Hybrid Cloud Console 上のサービスへのユーザーアクセスを定義するロールベースアクセス制御 (RBAC) の実装です。ユーザーアクセスを使用して、システムインベントリーのアクセスと権限を設定できます。

ユーザーアクセスの使用方法

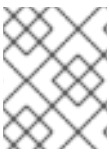
ユーザーアクセス機能は、特定のユーザーに個別に権限を割り当てるのではなく、ロールの管理に基づいています。ユーザーアクセスでは、各ロールに特定のパーミッションセットがあります。たとえば、ロールはアプリケーションの **読み取りパーミッション** を許可する場合があります。別のロールで、アプリケーションの **書き込みパーミッション** が許可される可能性があります。

ロールを含むグループを作成し、拡張で各ロールに割り当てられたパーミッションを作成します。ユーザーをグループに割り当てることもできます。つまり、グループ内の各ユーザーには、そのグループ内のロールの権限が割り当てられます。

異なるグループを作成し、そのグループのロールを追加または削除することで、そのグループに許可されるパーミッションを制御できます。グループにユーザーを追加すると、1 人以上のユーザーはそのグループに許可されたすべてのアクションを実行できます。

Red Hat は、ユーザーアクセス用に 2 つのデフォルトアクセスグループを提供します。

- **Default admin access** グループ。**Default admin access** グループは、組織内の組織管理者ユーザーに制限されています。**Default admin access** グループのロールを変更または修正することはできません。
- **Default access** グループ。**Default access** グループには、組織内の認証されたすべてのユーザーが含まれます。これらのユーザーは、事前定義されたロールの選択を自動的に継承します。



注記

Default access グループに変更を加えることができます。ただし、これを行うと、その名前が Custom default access グループに変更されます。

Red Hat は、事前に定義されたロールのセットを提供します。アプリケーションによっては、対応のアプリケーションごとに事前定義されたロールでは、アプリケーションに対してカスタマイズされるパーミッション異なる場合があります。

表1.1 インベントリーで事前定義されたロールおよびパーミッション

ロール名	設定	Permissions
inventory administrator	任意の Inventory リソースに対して利用可能な操作を実行できます。	インベントリー:*:* (* はすべてのリソースに対するすべての権限を示します。
Workspaces Administrator	ワークスペースデータの読み取りおよび編集が可能です。	inventory: groups: write および inventory: groups: read
Inventory Groups Viewer	ワークスペースデータを読み取ることができます。	inventory: groups: read
Inventory Hosts Administrator	Inventory Hosts データの読み取りと編集が可能です。	inventory: hosts: write および inventory: hosts: read
Inventory Hosts Viewer	Inventory Hosts データを読み取ることができます。	inventory: hosts: read

関連情報

ロールベースのアクセス制御

第2章 ワークスペース

ワークスペースを使用すると、特定のシステムを選択してグループ化することができます。個々のワークスペース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、ワークスペースごとにアプリケーション全体のシステムリストをフィルタリングできます。また、特定のワークスペースへのユーザーアクセスを管理し、セキュリティーを強化することもできます。

ワークスペースには次の特徴があります。

- ワークスペースはシステムのみを対象としています。
- ワークスペースを別のワークスペース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 のワークスペースにしか属することができません。
- ワークスペースの使用は必須ではありません。特定のワークスペース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しておくことができます。

2.1. ワークスペースへのユーザーアクセス

ワークスペース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、ユーザーロールに応じてワークスペースにカスタムパーミッションを設定できます。

Workspace administrator User Access ロールは、ワークスペースの作成を許可します。このロールは Default Access グループに自動的に組み込まれており、削除できません。ただし、このロールが割り当てられたユーザーはどのワークスペースでも変更できます。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。

ユーザーがワークスペースと RBAC を使用して特定のシステムへのアクセスを制限できるようにするには、そのユーザーがデフォルトのアクセスグループのメンバーであるか、**Workspace Administrator** と **User Access Administrator** の両方のロールを持っている必要があります。

ワークスペースユーザーには、グループレベルの RBAC 権限があります。カスタム権限には次のものが含まれます。

- inventory:groups:read
  - ワークスペースの詳細ページを表示する
- inventory:groups:write
  - ワークスペースの名前を変更する
  - ワークスペースにシステムを追加する
- ワークスペースからシステムを削除する

注記

ユーザーは、inventory:hosts:read 権限がないと、ワークスペース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。以下のワークスペース操作を実行できます。

- inventory:hosts:read

- ワークスペース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する
- 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。

2.1.1. ワークスペースへのユーザーアクセスの管理

注記

Workspace にアクセスできない場合は、**Inventory > Workspaces**に移動し、**Workspace access permissions needed** を表示します。

ワークスペース自体へのアクセス権がない場合でも、読み取りアクセス権を持つシステムに割り当てられたワークスペース名は表示できることに注意してください。システムを含むワークスペースを表示するには、Workspaces Viewer ロールを割り当てるか、または Workspace view パーミッションを割り当てる必要があります。

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。

2.1.1.1. カスタムユーザーアクセスロールの作成

ユーザーアクセスアプリケーションを使用して、ワークスペースのユーザーアクセスを設定します。

カスタムロールを作成します。

1. 右上隅にある **Settings** アイコン (⚙) をクリックし、**User Access** を選択して、ユーザーアクセスアプリケーションに移動します。**Identity & Access Management**のメインページが表示されます。
2. 左側のナビゲーションメニューで、**Roles** をクリックします。
3. **Create role** をクリックします。**Create Role** ウィザードが表示されます。
4. 新しいロールを作成するか、既存のロールをコピーするかを選択します。
   a. 新しいロールを作成するには、**create a role from scratch**を選択します。
   b. 既存のロールをコピーするには、**Copy an existing role**を選択します。ロールのリストが表示されます。コピーするロールを選択し、**Next** をクリックします。
5. 新しいロールに名前を付けます。必要に応じて説明を追加します。
6. **Next** をクリックします。**Add permissions** ページが表示されます。

7. アプリケーションフィルターはデフォルトで表示されます。**Filter by application** ドロップダウンをクリックし、**Inventory** を選択して、利用可能なすべてのインベントリーパーミッションを表示します。
   4 つのインベントリーパーミッションには以下が含まれます。

   - inventory:hosts:read - ユーザーがシステムを表示できるようにします (ワークスペースの内外の両方でシステムを表示するために必要です)。
   - inventory:hosts:write - ユーザーがシステムの名前を変更または削除できるようにします。
   - inventory:groups:read - ユーザーがワークスペースと一般情報 (そこに含まれるシステムは含まない) を表示できるようにします。
   - inventory:groups:write - ユーザーがワークスペースのメンバーシップを編集できるようにします (ワークスペースへのシステムの追加と削除)。

8. 必要なインベントリー権限を選択します。以下に例を示します。

   a. ユーザーにワークスペースとそのワークスペース内のすべてのシステムに対する完全なアクセス権を付与するには、4 つの権限をすべて選択します。

   b. ワークスペースの編集アクセスを付与せずにワークスペース内のシステムへの完全なアクセスを付与するには、inventory:hosts:read、inventory:hosts:write、および inventory:groups:read を選択しますが、inventory:groups:write は **選択しない** でください。

   c. ユーザーにグループ化されていないシステムへのフルアクセスを付与するには、4 つの権限すべてを選択します (グループ化されていないシステムはワークスペースと見なされます)。

9. **Next** をクリックします。**Define Workspace access**ページが表示されます。

10. リスト内の各権限の横にあるドロップダウン矢印をクリックし、それらの権限に適用するワークスペースを選択します。各権限ごとに少なくとも 1 つのワークスペースを選択する必要があります。

11. **Next** をクリックします。**Review details** ページが表示されます。

12. カスタムロールのパーミッションを確認し、**Submit** をクリックします。

特定のワークスペースアクセスを必要とする各ワークスペースまたは各ユーザーグループに対して、このプロセスを繰り返します。

シナリオ例

これらの例では、特定のカスタムロールのユーザーに割り当てる権限を説明します。

- ユーザーが特定のワークスペース内のシステムのみを表示できるようにし、どのワークスペースにも属さないシステムを **表示しない** ようにするには、それらのワークスペースのみを選択します。
- ユーザーが特定のワークスペース内のシステムだけでなく、どのワークスペースにも属していないシステムも表示できるようにするには、すべての権限に対してそれらのワークスペースを選択し、inventory:hosts 権限に **Ungrouped systems** を選択します。
- ユーザーがインベントリー内のすべてを表示できるようにするために、カスタムロールを作成する必要はありません。
- システム管理者のグループにワークスペース A、B、C への同じアクセス権を付与するには、単

ーのカスタムロールを作成し、これら 3 つのワークスペースに権限を割り当てます。ただし、異なるユーザーに異なるワークスペースへのアクセス権を付与する場合は、ワークスペースごとに個別のカスタムロールを作成します。

2.1.1.2. カスタムロールの割り当て

カスタムロールをユーザーまたはグループに割り当てるには、ユーザーアクセスグループを作成します。グループ内のユーザーは、そのグループに割り当てられたロールを受け取ります。

1. 画面の右上にある設定アイコン (**設定** アイコン (⚙)) をクリックし、次に **User Access** をクリックします。
2. 左側のナビゲーションメニューで、**User Access > Groups**をクリックします。
3. **Create group** をクリックします。Create group ウィザードには、 **Name and description**ページが表示されます。
4. グループ名を追加します。必要に応じて、グループの説明を追加します。
5. **Next** をクリックします。**Add roles** ページが表示されます。
6. 作成したカスタムロールを選択し、**Next** をクリックします。**Add members** ページが表示されます。
7. カスタムロールを割り当てるユーザーを選択します。
8. **Next** をクリックします。**Add service accounts** ページが表示されます。
9. **オプション:**選択したユーザーにサービスアカウントを割り当てる場合は、リストから 1 つ以上のサービスアカウントを選択します。
10. **Next** をクリックします。選択内容の詳細を確認し、**Submit** をクリックします。

1 つ以上のユーザーに割り当てる場合は、カスタムロールごとに、この手順を繰り返します。

2.1.1.3. ユーザーアクセスの設定

カスタムロールを作成して割り当てた後も、組織内の全ユーザーには **Inventory Hosts Administrator** ロールが割り当てられているため、インベントリーへのフルアクセス権が保持されます。これにより、すべてのユーザーがすべてのホストを表示および編集できるようになります。Default Access ワークスペースでは、このロールが組織内のすべてのユーザーにデフォルトで割り当てられます。

組織ユーザーのアクセスをカスタムロールで定義されたワークスペース/システムのみに制限するには、デフォルトのアクセスワークスペースを編集して、**Inventory Hosts Administrator** ロールを削除します。

1. 画面の右上にある設定アイコン (**設定** アイコン (⚙)) をクリックし、次に **User Access** をクリックします。
2. 左側のナビゲーションメニューで、**User Access > Groups**をクリックします。ユーザーアクセスグループのリストが表示されます。
3. **Default access** グループをクリックします。ロールのリストが表示されます。
4. **Inventory Hosts Administrator** ロールのチェックボックスを選択します。

5. 行の右端にあるオプションアイコン (⋮) をクリックします。**Remove role** オプションが表示されます。
6. **Remove role** をクリックします。**Remove role** ダイアログボックスが表示されます。
7. **Remove role** ボタンをクリックします。これまでに Default Access ワークスペースを編集したことがない場合は、警告メッセージが表示されます。
8. **I understand, and I want to continue**チェックボックスを選択して、**Continue** をクリックします。

2.1.1.4. インベントリーホストの管理者アクセスの設定

Default Access ワークスペースを編集した後、**Inventory Hosts Administrator** 権限を持つユーザーの新しいユーザーアクセスグループを作成する必要があります。

1. 画面の右上にある設定アイコン (**設定** アイコン (⚙)) をクリックし、次に **User Access** をクリックします。
2. 左側のナビゲーションメニューで、**User Access > Groups**をクリックします。ワークスペースのリストが表示されます。
3. **Create group** をクリックします。Create Group ウィザードが表示されます。
4. グループの名前を追加します。必要に応じて説明を追加します。
5. **Next** をクリックします。**Add roles** ページが表示されます。
6. ロールのリストから **Inventory Hosts Administrator** ロールを選択します。
7. **Next** をクリックします。**Add members** ページが表示されます。
8. ロールを割り当てるユーザーを選択します。
9. **Next** をクリックします。**Add service accounts** ページが表示されます。
10. **オプション:**選択したユーザーにサービスアカウントを割り当てる場合は、リストから 1 つ以上のサービスアカウントを選択します。
11. **Next** をクリックします。**Review details** ページが表示されます。
12. 選択した内容の詳細を確認し、**Submit** をクリックします。

アクセスの設定が完了すると、組織内の特定のユーザーには完全なインベントリーアクセスが許可され、他のユーザーには制限付きのインベントリーアクセスが許可されます。

2.2. ユーザーシナリオ

このセクションには、ワークスペースの機能を説明する 2 つのサンプルシナリオが含まれています。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。

2.2.1. 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。
- 同じチーム内のユーザーはすべて、ワークスペースとシステムの両方へのアクセス権のレベルは同じです。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、どのワークスペース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、ワークスペース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。

2.2.1.1. 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、常にすべてのワークスペースへの読み取り/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、ワークスペース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、ワークスペース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ワークスペース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ワークスペース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。

2.2.1.2. 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: ワークスペースを作成する

まず、2 つの個別のワークスペースを作成します。(この例では 2 つのワークスペースを作成しますが、必要な数だけ作成できます。)

- ワークスペース 1: IT チーム A - システム
- ワークスペース 2: IT チーム B - システム

ステップ 2: ワークスペースにシステムを追加する

ワークスペースが作成されたので、そこにシステムを追加します。各ワークスペースをクリックし、**Add systems** を選択します。

この段階では、ユーザーが所属するワークスペースに関係なく、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 Inventory Hosts Administrator 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

さまざまなワークスペースへのアクセスをカスタマイズするには、それらのワークスペース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。

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 つのインベントリー権限オプションがあります。付与するアクセスのレベルに応じて選択します。

ワークスペースとそのシステムに完全にアクセスするには、以下を選択します。

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

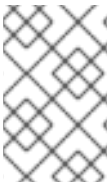
権限を選択したら、**Next** をクリックします。必要に応じて権限を調整できます。

ステップ 3b: 選択したワークスペースに権限を割り当てる

このステップでは、権限を付与するワークスペースを選択します。この例では、現在のロールに対応するワークスペース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、各権限にワークスペース **IT team A - Systems** を指定します。

詳細を確認し、**Submit** をクリックします。

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** ワークスペースを選択します。



注記

いずれのワークスペースにも属さないシステムへのアクセスを、一方または両方の IT チームに許可できます。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。

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

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を削除する

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ワークスペースに関係なく、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 Inventory Hosts Administrator 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。

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。

ロールが削除されると、ユーザーアクセスの制御は想定どおりに動作します。つまり、特定のワークスペースとシステムへの表示を制限するカスタムロールが付与されているユーザーには、それらのワークスペースとシステムのみが表示されます。

2.2.1.3. 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ワークスペースへの同じアクセス権を付与する場合は、複数のワークスペースを選択して、同じカスタムロール内で権限を付与できます。
- ワークスペースの一部ではないシステムへのアクセスを許可できます。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。

2.2.2. 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

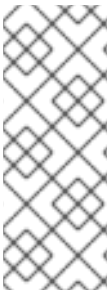
1. **User Access > Roles**に移動し、**Create role** をクリックします。Create Role ウィザードが表示されます。
2. ロール名と説明を設定し、**Next** をクリックします。
3. inventory:hosts 権限を追加し、**Next** をクリックします。

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。

ロールの詳細を確認し、**Submit** をクリックします。

ステップ 2: RBAC グループへのカスタムロールの追加

1. 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。
2. 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。



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ーホスト管理者ロールを **持っていない** 場合にのみ機能します。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。インベントリー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ー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、インベントリー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。

2.2.3. 既知の制限

- Organization Administrator (デフォルトの管理者アクセスグループのメンバー) であるユーザーは、常にシステムとワークスペース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

組織でワークスペースを有効にする前に、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、ユーザーのワークスペース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。

2.3. ワークスペースの作成

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、ワークスペース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、**Workspaces** を選択します。
3. **Create Workspace** をクリックします。**Create Workspace** ダイアログボックスが表示されます。

4. **Workspace name** フィールドにワークスペース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。**Workspace created** メッセージが表示され、新しいグループがワークスペースの一覧に表示されます。

2.4. 新規作成されたワークスペースへのシステムの追加

注記

各システムは、1 つのワークスペースにしか属することができません。現在の Workspaces リリースでは、システムを 1 回の手順で別のグループに再割り当てすることはできません。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ワークエウペース管理者権限、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

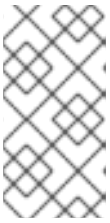
1. Red Hat Hybrid Cloud Console で **Inventory** に移動します。

2. **Workspaces** を選択します。

3. システムを追加するグループの名前をクリックします。ワークスペースの名前と、**Systems** と **Group Details** の 2 つのタブを含む **Workspaces** のページが表示されます。

4. **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。

5. ワークスペースに追加するシステムを選択します。



注記

すでに別のワークスペースに属しているシステムを選択すると、**One or more of the selected systems already belong to {a workspace} 警告メッセージが表示されます。Make sure that all the systems you have selected are ungrouped, or you will not be able to proceed.** の警告メッセージが表示されます。

6. システムの選択が完了したら、**Add systems** をクリックします。**Workspaces** ページには、グループに追加したシステムが表示されます。

2.4.1. 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ワークスペース管理者権限、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 Workspace** を選択します。**Add to Workspace** ダイアログボックスが表示されます。
5. **Create a new Workspace** をクリックします。**Create Workspace** 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。

2.5. ワークスペースからのシステムの削除

Red Hat Hybrid Cloud Console の 2 つのページ (ワークスペースページとシステムページ) から、ワークスペースからシステムを削除できます。

2.5.1. ワークスペースページを使用したワークスペースからのシステムの削除

前提条件

- 組織管理者 (Default 管理者アクセスグループのメンバー) であるか、**Workspace Administrator** ロールを持っているか、特定のワークスペースに対する inventory:group:write 権限を持っている必要があります。

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、**Workspaces** を選択します。**Workspaces** ページが表示されます。
3. 削除するシステムが含まれるワークスペースを選択します。
4. ワークスペース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 Workspace** を選択します。**Remove from Workspace?** ダイアログボックスが表示されます。
7. **オプション:** ワークスペース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 (オプションアイコン (⋮)) から **Remove from Workspace** を選択します。
8. **Remove** をクリックします。

ワークスペースページが表示され、更新されたワークスペースとステータス (成功または失敗) メッセージが表示されます。

2.5.2. システムページを使用したワークスペースからのシステムの削除

前提条件

- 組織管理者のワークスペースへの Insights for Red Hat Enterprise Linux または **Workspace administrator** 権限、またはワークスペースへの inventory:groups:write および inventory:groups:read パーミッションの両方へのアクセス

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. ワークスペース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 Workspace** を選択します。**Remove from Workspace?** 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ワークスペースに属していないと、**Remove from Workspace** オプションは引き続き無効になります。ワークスペースに属するシステムのみを選択するようにしてください。

6. **オプション:** ワークスペース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、ツールバーの **More options** メニュー (オプションアイコン (⋮)) から **Remove from Workspace** 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。

2.6. ワークスペース名の変更

前提条件

- 組織管理者 (Default 管理者アクセスグループのメンバー) であるか、Workspace Administrator ロールを持っているか、特定のワークスペースに対する inventory:group:write 権限を持っている必要があります。

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、**Workspaces** を選択します。**Workspaces** ページが表示されます。
3. **Workspaces** ページの右上にある **Workspace 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 Workspace** 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. **Workspaces** ページのワークスペースのリストに、名前を変更したワークスペースが表示されます。

2.7. ワークスペースの削除

注記

ワークスペースを削除する前に、ワークスペースにシステムが含まれていないことを確認してください。空のワークスペースのみを削除できます。システムがまだ含まれているワークスペースを削除しようとすると、Insights によって警告メッセージが返されます。

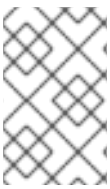
前提条件

- 組織管理者 (Default 管理者アクセスグループのメンバー) であるか、Workspace Administrator ロールを持っているか、特定のワークスペースに対する inventory:group:write 権限を持っている必要があります。

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、**Workspaces** を選択します。**Workspaces** 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オプションアイコン (⋮) 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 Workspace** 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。

Workspaces ページには、更新されたワークスペースの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

ワークスペース自体のページ内からワークスペースを削除することもできます。ワークスペースに移動し、**Actions** ドロップダウンメニューをクリックして、**Delete** を選択します。

第3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ーから削除されるかなどを指定できます。

3.1. 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ーは、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 インベントリーから削除されます。システムを削除した後は、再登録してインベントリー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とき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。

3.2. 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。

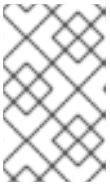
5. 変更する値の横にある矢印をクリックして、新しい値を選択します。

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。

3.3. 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」などです。

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。フィードバックをご提供いただきありがとうございました。