Red Hat Insights 2022

RHEL システムのセキュリティーポリシーコンプライアンスの評価および監視

Red Hat Enterprise Linux インフラストラクチャーのセキュリティーコンプライアンスステータスについて

Last Updated: 2022-06-20

Red Hat Insights 2022 RHEL システムのセキュリティーポリシーコンプライアンスの評価および監視

Red Hat Enterprise Linux インフラストラクチャーのセキュリティーコンプライアンスステータスについて

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

RHEL 環境の security-policy コンプライアンスステータスを評価し、追跡してコンプライアンスレベルを判断し、コンプライアンス問題を解決するためのアクションのコースをプランニングします。

目次

多様性を受け入れるオープンソースの強化

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、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。

RED HAT ドキュメントへのフィードバック

弊社のドキュメントに関するご意見やご感想をお寄せください。フィードバックを提供するには、ドキュメントのテキストを強調表示し、コメントを追加します。

前提条件

- Red Hat カスタマーポータルにログインしている。
- Red Hat カスタマーポータルでは、このドキュメントは **Multi-page HTML** 表示形式です。

手順

フィードバックを提供するには、以下の手順を実施します。

1. ドキュメントの右上隅にある **フィードバック** ボタンをクリックして、既存のフィードバックを確認します。

注記

フィードバック機能は、**マルチページ HTML** 形式でのみ有効です。

2. フィードバックを提供するドキュメントのセクションを強調表示します。
3. ハイライトされたテキスト近くに表示される **Add Feedback** ポップアップをクリックします。ページの右側のフィードバックセクションにテキストボックスが表示されます。
4. テキストボックスにフィードバックを入力し、**Submit** をクリックします。ドキュメントに関する問題が作成されます。
5. 問題を表示するには、フィードバックビューで問題リンクをクリックします。

第1章 RHEL コンプライアンスサービスの概要に関する洞察

Insights for Red Hat Enterprise Linux コンプライアンスサービスにより、IT セキュリティーおよびコンプライアンス管理者は、RHEL システムのセキュリティーポリシーコンプライアンスを評価、監視、およびレポートできます。

Compliance サービスには、シンプルながらも強力なユーザーインターフェースがあり、SCAP セキュリティーポリシーの作成、設定、管理が可能です。フィルタリング機能とコンテキスト追加機能が組み込まれているため、IT セキュリティー管理者は RHEL インフラストラクチャのセキュリティコンプライアンスの問題を簡単に特定し、管理することができます。

本書では、レポートの理解、問題の管理、Compliance サービスから最大限の価値を得られるように、このサービスの機能の一部を説明します。

また、Ansible Playbook を作成して、セキュリティーコンプライアンスの問題を解決し、ステークホルダーとレポートを共有して、コンプライアンスステータスの伝達が可能です。

関連情報

- Ansible Playbook を使用したセキュリティーポリシーコンプライアンスの問題修正
- Compliance サービスレポートの生成

1.1. 要件および前提条件

Compliance サービスは、Red Hat Enterprise Linux (RHEL)サブスクリプションに含まれる Red Hat Enterprise Linux の Insights の一部で、現在 Red Hat がサポートしているすべてのバージョンの RHEL で使用できます。Insights for RHEL および Compliance サービスを使用するのに、追加の Red Hat サブスクリプションは必要ありません。

1.2. サポートされる構成

Red Hat は、Red Hat Enterprise Linux (RHEL) のマイナーバージョンごとに特定のバージョンの SCAP セキュリティーガイド (SSG) をサポートしています。SSG バージョンのルールおよびポリシーは、1 つの RHEL マイナーバージョンに対してのみ正確です。正確なコンプライアンスレポートを受け取るには、システムにサポートされている SSG バージョンがインストールされている必要があります。

Red Hat Enterprise Linux のマイナーバージョンは、サポートされている SSG バージョンが含まれている状態で出荷およびアップグレードされます。ただし、一部の組織では、アップグレードする前に、以前のバージョンを一時的に使用し続けることを決定する場合があります。

ポリシーにサポート対象外の SSG バージョンを使用するシステムが含まれる場合、影響を受けるシステムの数の前に **サポートされない** 警告が、Red Hat Enterprise Linux > Compliance > Reports のポリシーの横に表示されます。

注記

RHEL でサポートされている SCAP セキュリティーガイドのバージョンの詳細については、Insights コンプライアンス - サポートされている構成 を参照してください。

サポートされていないバージョンの SSG を実行しているシステムのコンプライアンスポリシーの例

1.2.1. コンプライアンスサービスに関するよくある質問

SSG パッケージ名をどのように解釈しますか?

パッケージ名は **scap-security-guide-0.1.43-13.el7** のようになります。この場合、SSG バージョンは 0.1.43 です。リリースは 13 で、アーキテクチャーは el7 です。リリース番号は、表に記載されているバージョン番号と異なる場合があります。ただし、バージョン番号は、以下に示しているように、サポート対象の設定になるように一致させる必要があります。

使用中の RHEL マイナーバージョンで Red Hat がサポートする SSG が複数ある場合

RHEL 7.9 および RHEL 8.1 のように、RHEL マイナーバージョンで複数の SSG バージョンがサポートされる場合には、Compliance サービスは利用可能な最新バージョンを使用します。

以前のポリシーが SSG でサポートされなくなった理由:

RHEL マイナーバージョンが古くなると、サポート対象の SCAP プロファイルも少なくなります。サポートされている SCAP プロファイルを確認するには、Insights コンプライアンス - サポートされている構成 を参照してください。

サポート対象外の設定の制限事項

以下の条件が、サポート対象外の設定の結果に適用されます。

- Red Hat のサポート対象外の SSG バージョンを使用すると結果の精度が落ちる可能性があるため、ベストエフォートでの推測をもとにこれらの結果が出されます。

重要

サポート対象外のバージョンの SSG がインストールされているシステムの結果が依然として表示される可能性がありますが、コンプライアンスレポートの目的では、結果が正確ではないと見なされる可能性があります。

- サポート対象外の SSG バージョンを使用するシステムに関する結果は、ポリシーの全体的なコンプライアンスアセスメントには**含まれません**。
- サポート対象外の SSG バージョンがインストールされているシステムのルールでは、修正は利用できません。

1.3. ベストプラクティス

Red Hat では、ユーザーエクスペリエンスを最適化し、最も正確な結果を受け取るにはベストプラクティスに従うことを推奨します。

RHEL OS システムのマイナーバージョンが Insights クライアントに表示されるようにする

Compliance サービスで RHEL OS のマイナーバージョンが表示されない場合は、サポート対象の SCAP セキュリティーガイドのバージョンを検証できないので、レポートが正確でない可能性があります。Insights クライアントを使用すると、Red Hat Enterprise Linux OS マイナーバージョンなど、Insights for Red Hat Enterprise Linux にアップロードされるデータペイロードから 特定のデータを編集できます。そのため、Complaince サービスによる正確なレポーティングができなくなります。

データ整理の詳細は、以下のドキュメントを参照してください。Red Hat Insights クライアントリダクションの設定

Complaince サービス内でのセキュリティーポリシーの作成

Compliance サービス内に組織のセキュリティーポリシーを作成すると、複数システムとそのポリシーを関連付け、RHEL マイナーバージョンに適した、サポート対象の SCAP Security Guide (SSG) が使用されていることを確認し、組織の要件をもとに追加するルールを編集できます。

第2章 コンプライアンスサービスの使用を開始する

次の手順では、コンプライアンスデータを InsightsforRHEL アプリケーションに報告するように RHEL システムを設定する方法について説明します。これにより、コンプライアンススキャンの実行に使用される SCAP セキュリティーガイド (SSG) などの必要な追加コンポーネントがインストールされます。

前提条件

- Insights クライアントがシステムにデプロイされている。
- システムに対する root 権限がある。

手順

1. システム上の RHEL のバージョンを確認します。

```
[user@insights]$ cat /etc/redhat-release
```

2. Insights のコンプライアンス - サポートされている設定 の記事を確認し、システムでサポートされている RHEL マイナーバージョンの SSG バージョンをメモします。

注記

一部のマイナーバージョンの RHEL は、複数のバージョンの SSG をサポートしています。Insights コンプライアンスサービスは、サポートされている最新バージョンの結果を常に表示します。

3. サポートされているバージョンの SSG パッケージがシステムにインストールされているかどうかを確認します。
例: RHEL8.4 の実行の場合:

```
[root@insights]# dnf info scap-security-guide-0.1.57-3.el8_4
```

4. まだインストールされていない場合は、サポートされているバージョンの SSG をシステムにインストールします。
例: RHEL8.4 の実行の場合:

```
[root@insights]# dnf install scap-security-guide-0.1.57-3.el8_4
```

5. コンプライアンスサービス UI で、Red Hat EnterpriseLinux > コンプライアンス >SCAP ポリシー で、システムをポリシーに追加します。
   a. **新しいポリシーの作成** をクリックして、システムを新しいセキュリティーポリシーに追加します。
   b. または、既存のポリシーを選択し、**ポリシーの編集** をクリックしてシステムを追加します。
6. 各システムを目的のセキュリティーポリシーに追加した後、システムに戻り、以下を使用してコンプライアンススキャンを実行します。

```
[root@insights]# insights-client --compliance
```

注記

スキャンが完了するまで 1-5 分かかる場合があります。

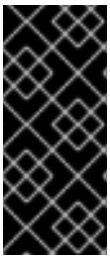
7. Generating Compliance Service Reports に移動し、結果を表示します。
8. 必要に応じて、コンプライアンスジョブを cron で実行するようにスケジュールします。

Resources

Red Hat Enterprise Linux マイナーバージョンでサポートされている SCAP セキュリティーガイドのバージョンについては、Insights コンプライアンス - サポートされている設定 を参照してください。

第3章 INSIGHTSFOR RHEL コンプライアンスサービスでの SCAP セキュリティーポリシーの管理

コンプライアンスサービス UI 内のみで SCAP セキュリティポリシーを作成して管理します。新しいポリシーを定義し、関連付けるルールおよびシステムを選択し、要件の変更に合わせて既存のポリシーを編集します。



重要

その他のほとんどの Insights for Red Hat Insights サービスとは異なり、コンプライアンスサービスはデフォルトのスケジュールで自動的に実行されません。OpenSCAP データを Insights for RHEL アプリケーションにアップロードするには、オンデマンドまたは設定したスケジュール済みジョブのいずれかで、**insights-client --compliance** を実行する必要があります。

1. 関連情報 コンプライアンススキャンのスケジュールの詳細については、**Insights サービスの定期的なアップロードを設定する方法** を参照してください。

3.1. 新しい SCAP ポリシーの作成

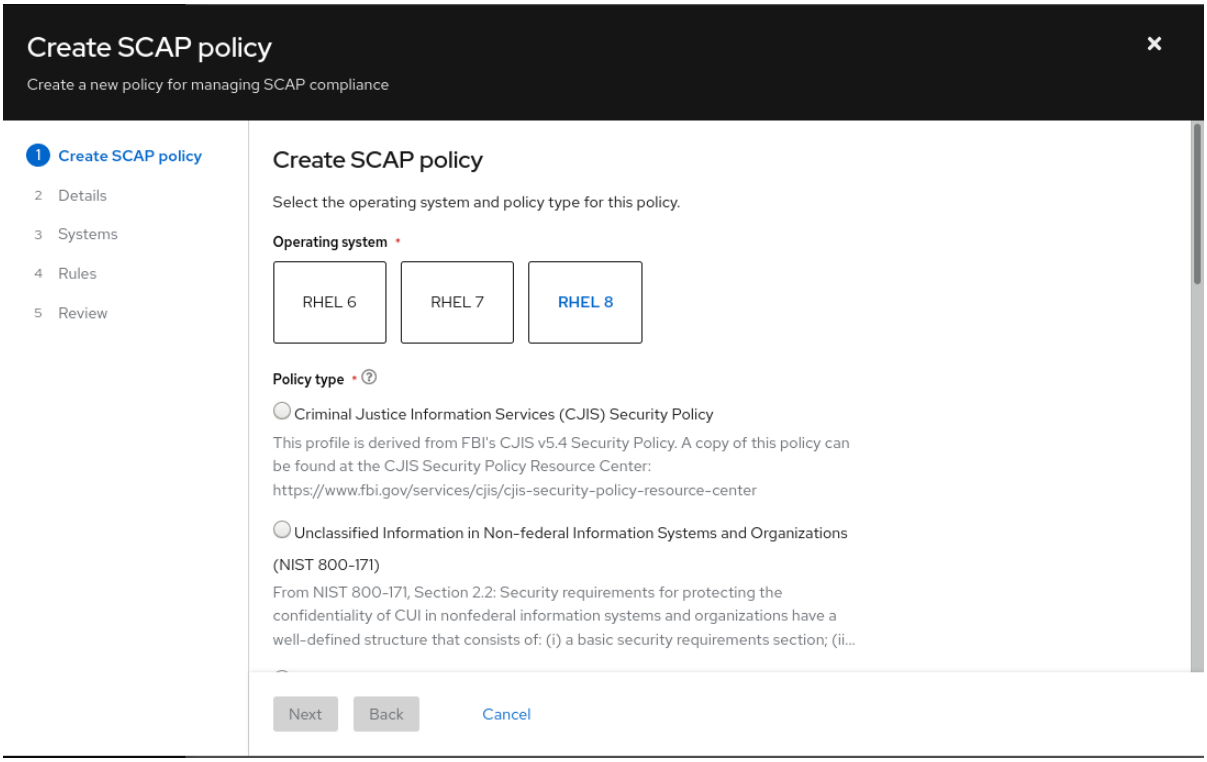
コンプライアンスサービス UI でスキャンを実行したり、そのスキャンの結果を確認したりする前に、RHEL に登録された各システムの Insights を 1 つ以上のセキュリティーポリシーに追加する必要があります。新しいポリシーを作成して、特定のシステムおよびルールを含めるには、以下の手順を実行します。

重要

RHEL サーバーで RHEL のメジャーリリースを複数使用する場合は、メジャーリリースごとに個別のポリシーを作成する必要があります。たとえば、全 RHEL 7 サーバーが **Standard System Security Profile for RHEL** ポリシーを、全 RHEL 8 サーバーに別のポリシーを使用する場合などです。

手順

1. Red Hat Hybrid Cloud Console にログインし、Red Hat Enterprise Linux > Compliance > SCAP policies ページに移動します。
2. **Create new policy** ボタンをクリックします。
3. ウィザードの **Create SCAP policy** ページで、ポリシーに含まれるシステムの **RHEL メジャーバージョン** を選択します。



4. 対象の RHEL メジャーバージョンで利用可能な **ポリシータイプ** の中から 1 つ選択して、**Next** をクリックします。

5. **Details** ページで、すでに入力されている名前および説明を使用するか、わかりやすい名前や説明を入力します。

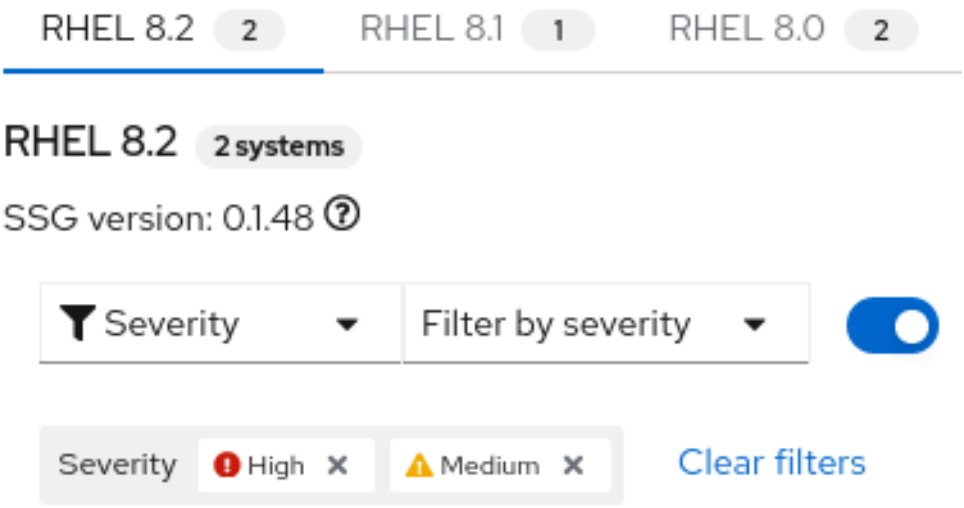
6. 必要に応じて、**ビジネスの目的** (例: CISO mandate) を追加して、コンテキストを追加します。

7. 要件に合った **コンプライアンスしきい値** を定義して、**Next** をクリックします。

8. このポリシーに含める **システム** を選択し、**Next** をクリックします。最初の手順で RHEL メジャーバージョンを選択すると、このポリシーに追加できるシステムが自動的に決定されます。

9. 各ポリシーで **使用するルール** を選択します。RHEL のマイナーバージョンごとに特定の SCAP Security Guide (SSG) バージョン (この場合は複数) を使用できるので、RHEL マイナーバージョンごとにルールセットは若干異なり、個別に選択する必要があります。

   a. 必要に応じて、フィルタリング機能および検索機能を使用して、ルールの一覧を絞り込みます。
   たとえば、重大度の最も高いルールのみを表示するには、主要なフィルターのドロップダウンメニューをクリックして、**Severity** を選択します。2 番目のフィルターで、**High** および **Medium** のチェックボックスを選択します。



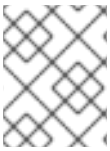
b. デフォルトで表示されるルールは、SSG の対象のポリシータイプおよびバージョンに指定されたものです。デフォルトでは、フィルターボックスの横にある **Selected only** のトグルを有効にします。必要に応じて、このトグルを削除できます。

c. 必要に応じて、**各 RHEL マイナーバージョンタブ** でこのプロセスを繰り返します。

d. 各 Red Hat Enterprise Linux マイナーバージョンの SSG ルールを選択したら、**Next** をクリックします。

10. **Review** ページで、表示される情報が正しいことを確認してから、**Finish** をクリックします。

11. アプリにポリシーを作成する時間を与えてから、**Return to application** ボタンをクリックして新しいポリシーを表示します。



注記

結果がコンプライアンスサービス UI に表示される前に、システムに移動してコンプライアンススキャンを実行する必要があります。

3.2. 既存のポリシーの編集

ルールやシステムが要件に該当しなくなる場合があるので、セキュリティーポリシーの作成後に、追加するルール (またはシステム) を変更できます。以下の手順に従い、既存のポリシーを編集して、特定のルールを追加または削除します。

手順

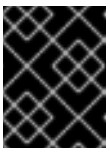
1. Red Hat Hybrid Cloud Console にログインし、Red Hat Enterprise Linux > Compliance > SCAP policies ページに移動します。

2. 編集するポリシーを見つけます。

3. ポリシー行の右側にある More Actions アイコン ( ) をクリックし、**Edit policy** をクリックします。

4. **Edit <Policy name>** カードで、**Rules** タブをクリックします。

a. フィルターまたは検索機能を使用して、削除するルールを見つけます。



重要

デフォルトでは、検索ボックスの右側にある **Selected only** トグルが有効になっています。必要に応じてトグルを削除できます。

b. 削除するルールの横にあるチェックボックスの選択を解除します。

c. 必要に応じて、RHEL マイナーバージョンの SSG タブごとに、このプロセスを繰り返します。

5. **Save** をクリックします。

検証

1. Red Hat Enterprise Linux > Compliance > SCAP policies ページに移動し、編集したポリシーを見つけます。

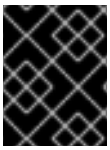
2. ポリシーをクリックし、追加したルールが編集した内容と一致していることを確認します。

第4章 コンプライアンスレポートの分析およびトリアージ

コンプライアンスサービスは、サービスに登録されている各ポリシーとシステムのデータ (およびレポートデータ) を表示します。これは大量のデータである可能性があり、そのほとんどは当面の目標に関連していない可能性があります。

次のセクションでは、レポート、SCAP ポリシー、およびシステムのコンプライアンスサービスデータの大部分を改良して、最も重要なシステムまたはポリシーに焦点を当てる方法について説明します。

コンプライアンスサービスを使用すると、ユーザーはシステム、ルール、およびポリシーのリストにフィルターを設定できます。他の Insights for RHEL サービスと同様に、コンプライアンスサービスでもシステムグループタグによるフィルターリングが可能です。ただし、コンプライアンスに登録されたシステムは異なるレポートメカニズムを使用するため、タグフィルターは、Insights アプリケーションの他の場所で使用されるグローバルな **Filter by status** ドロップダウンからではなく、コンプライアンス UI ビューのシステムのリストに直接設定する必要があります。



重要

システムの正確なデータを表示するには、UI で結果を表示する前に、常に各システムで **insights-client --compliance** を実行してください。

4.1. レポート

Red Hat Enterprise Linux > Compliance > Reports

Reports ページで、次のプライマリーフィルターとセカンダリフィルターを使用して、特定のレポートまたは狭いレポートセットに焦点を合わせます。

- **ポリシー名。** 名前でポリシーを検索します。
- **ポリシータイプ。** コンプライアンスサービスでインフラストラクチャーに設定されているポリシータイプから選択します。
- **Operating system**1 つ以上の RHEL OS メジャーバージョンを選択します。
- **コンプライアンスを満たすシステム。** 含まれているシステムのパーセンテージ (範囲) が準拠しているポリシーを表示します。

4.2. SCAP ポリシー

Red Hat Enterprise Linux > Compliance > SCAP policies

Filter by name 検索ボックスを使用して、名前で特定のポリシーを見つけます。次に、ポリシー名をクリックして、以下の情報を含むポリシーカードを表示します。

- **Details.**コンプライアンスのしきい値、ビジネス目標、OS、SSG バージョンなどの詳細を表示します。
- **Rules.**利用可能な名前 (Name)、重大度 (Severity)、および修復 (Remediation) を使用して、ポリシーの特定 SSG バージョンに含まれるルールを表示してフィルタリングします。次に、ルール名 (Rule name)、重大度 (Severity)、または Ansible Playbook サポート (Ansible Playbook Support) 別に結果を並べ替えます。

- **Systems**システム名で検索して、ポリシーに関連付けられた特定のシステムを見つけてから、システム名をクリックして、そのシステムおよび影響を受ける可能性のある問題の詳細を表示します。

4.3. SYSTEMS

Red Hat Enterprise Linux > Compliance > Systems

このページのデフォルトの機能は、システム名で検索します。

- **Tags.**システムグループまたはタグ名で検索します。
- **Name.**システム名で検索します。
- **Policy.**ポリシー名で検索し、そのポリシーに含まれるシステムを確認します。
- **Operating system.**RHEL OS メジャーバージョンが検索して、RHEL 7 または RHEL 8 システムのみを表示します。

4.4. 検索

Compliance サービスの検索機能は、表示中ページのコンテキストで機能します。

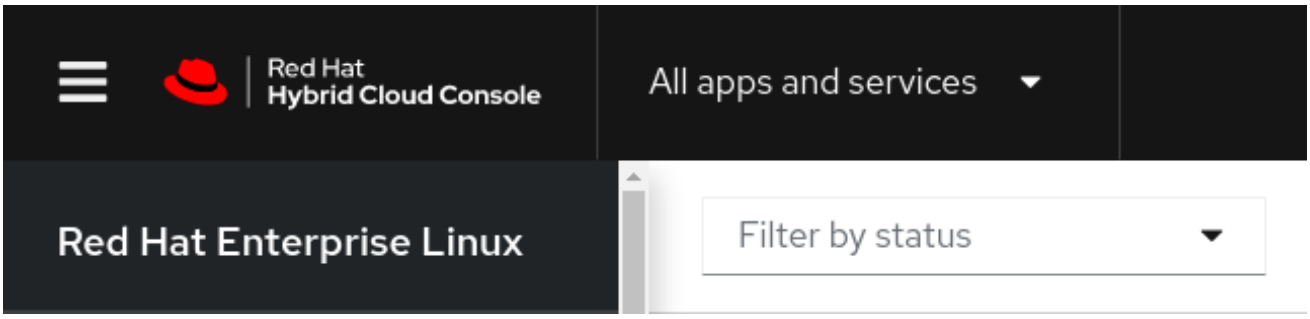
- **SCAP Policies**名前で特定のポリシーを検索します。
- **Systems**システム名、ポリシー、または Red Hat Enterprise Linux オペレーティングシステムのメジャーバージョンで検索します。
- **ルールリスト (単一システム)**ルールリスト検索機能では、ルール名または識別子で検索することができます。識別子はルール名の下に直接表示されます。

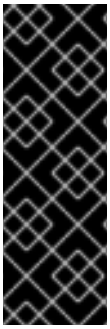
4.5. INSIGHTS FOR RHEL のシステムグループとタグ

Insights for RHEL アプリケーションを使用すると、ユーザーはデータをフィルター処理して、選択したシステムのグループのみを表示できます。**Filter by status** ドロップダウンを使用して 1 つ以上のグループを選択すると、そのグループフィルターは、コンプライアンスサービスのシステムリストを除いて、UI 全体の各サービスで引き続き適用されます。

システムのグループでフィルタリングする機能は、表示しているサービスに関係なく、結果に焦点を合わせ、それらのシステムのレポートを作成したいユーザーを支援します。

Insights for RHEL グローバルグループおよびタグフィルター





重要

コンプライアンスサービス UI では、グループおよびタグフィルターは、コンプライアンスデータを報告するシステム専用に設定されます。**Filter by status** を使用して設定されたタグおよびグループフィルターは、コンプライアンスサービス UI のシステムリストには適用されません。代わりに、ユーザーはシステムのリストの上に **Tags** プライマリーフィルターを設定してから、セカンダリフィルターで特定のグループまたはタグを選択します。詳細については、以下の **コンプライアンスサービスのグループおよびタグフィルター** セクションを参照してください。

システムにタグを付けたり、グループに割り当てたりする方法

システムは、次の 2 つの方法でグループに追加されます。

- **自動的に、Insights のデータ取り込み方法により。**管理者がアクションを実行する必要がないため、Insights クライアントは、SAP ワークロードを実行しているシステムを SAP ID で、Satellite ホストグループに属するシステムをホストコレクション名で自動的にタグ付けします。
- **カスタムタグの設定。**ルートアクセス権を持つユーザーは、/etc/insights-client/tags.yaml で特定のシステムのカスタムタグを設定できます。その後、ユーザーは Insights for RHEL UI のカスタムグループタグでフィルタリングし、そのタグで設定されたシステムのみを表示できます。

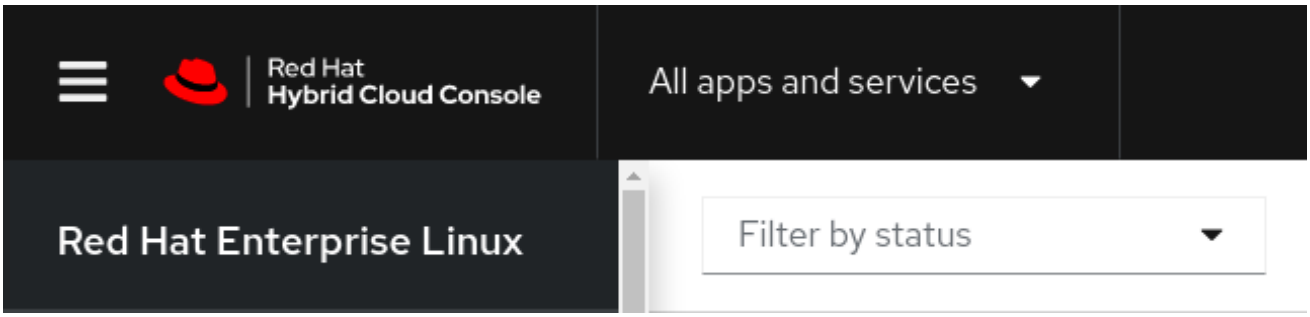
Insights クライアントにシステムタグを追加する方法など、グループとタグの詳細については、Insights for RHEL アドバイザーサービスの 第 8 章。システムのフィルターリングとグループ を参照してください。

4.6. INSIGHTS FOR RHEL のシステムグループとタグ

Insights for RHEL アプリケーションを使用すると、ユーザーはデータをフィルター処理して、選択したシステムのグループのみを表示できます。**Filter by status** ドロップダウンを使用して 1 つ以上のグループを選択すると、そのグループフィルターは、コンプライアンスサービスのシステムリストを除いて、UI 全体の各サービスで引き続き適用されます。

システムのグループでフィルタリングする機能は、表示しているサービスに関係なく、結果に焦点を合わせ、それらのシステムのレポートを作成したいユーザーを支援します。

Insights for RHEL グローバルグループおよびタグフィルター



重要

コンプライアンスサービス UI では、グループおよびタグフィルターは、コンプライアンスデータを報告するシステム専用に設定されます。**Filter by status** を使用して設定されたタグおよびグループフィルターは、コンプライアンスサービス UI のシステムリストには適用されません。代わりに、ユーザーはシステムのリストの上に **Tags** プライマリーフィルターを設定してから、セカンダリフィルターで特定のグループまたはタグを選択します。詳細については、以下の **コンプライアンスサービスのグループおよびタグフィルター** セクションを参照してください。

システムにタグを付けたり、グループに割り当てたりする方法

システムは、次の 2 つの方法でグループに追加されます。

- **自動的に、Insights のデータ取り込み方法により。**管理者がアクションを実行する必要がないため、Insights クライアントは、SAP ワークロードを実行しているシステムを SAP ID で、Satellite ホストグループに属するシステムをホストコレクション名で自動的にタグ付けします。

- **カスタムタグの設定。**ルートアクセス権を持つユーザーは、/etc/insights-client/tags.yaml で特定のシステムのカスタムタグを設定できます。その後、ユーザーは Insights for RHEL UI のカスタムグループタグでフィルタリングし、そのタグで設定されたシステムのみを表示できます。

Insights クライアントにシステムタグを追加する方法など、グループとタグの詳細については、Insights for RHEL アドバイザーサービスの 第 8 章。システムのフィルターリングとグループ を参照してください。

4.6.1. コンプライアンスサービスのグループおよびタグフィルター

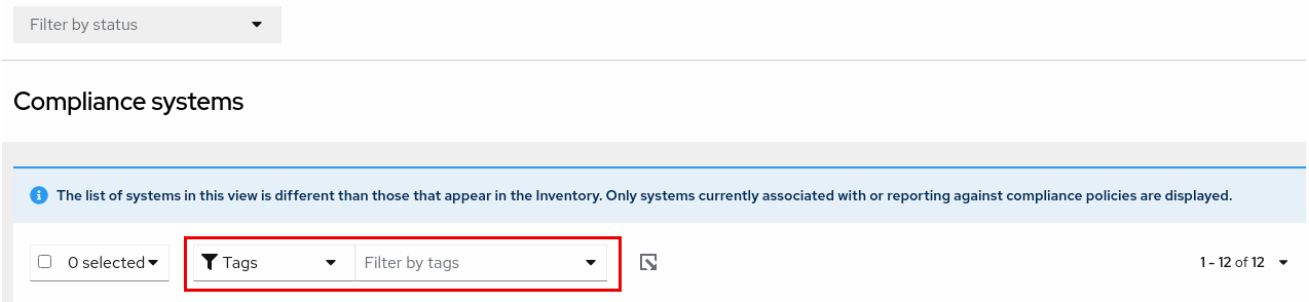
コンプライアンスサービスを使用すると、ユーザーは、コンプライアンスデータを報告するシステムにタグおよびグループフィルターを適用できます。ただし、**Filter by status** ドロップダウンを使用して設定することはできません。Insights for RHEL アプリケーションの他のほとんどのサービスとは異なり、コンプライアンスサービスは、次の条件下でのシステムのデータのみを表示します。

- システムは、コンプライアンスサービスのセキュリティーポリシーに関連付けられています。

- システムは、**insights-client --compliance** コマンドを使用して、コンプライアンスデータをインサイトに報告しています。

これらの条件のため、コンプライアンスサービスのユーザーは、コンプライアンスサービス UI のシステムのリストの上にあるプライマリーフィルターとセカンダリフィルターを使用して、タグフィルターとグループフィルターを設定する必要があります。

コンプライアンスサービスのシステムリスト上のタグおよびグループフィルター



4.6.2. グループまたはタグによるコンプライアンスサービスシステムリストのフィルタリング

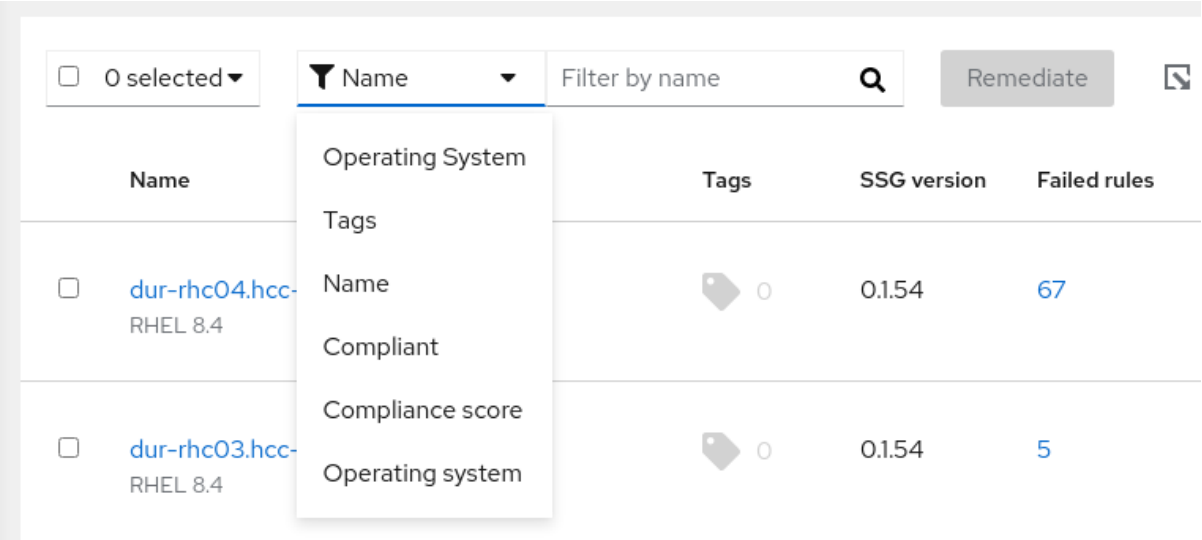
次の手順を使用して、コンプライアンスサービスのシステムの特定のグループにフィルターを設定します。この手順は、グループフィルターを設定するための 1 つのパスを示しています。ただし、一度設定すると、フィルターはコンプライアンスサービス UI 全体のシステムリストに保持されます。

前提条件

- ユーザーは Red Hat Hybrid Cloud Console にログインしています。

手順

1. Red Hat Enterprise Linux > Compliance > Reports に移動します。
2. レポート名をクリックします。
3. システムリストの上で、プライマリーフィルターのドロップダウンをクリックし、**Tags** を選択します。



4. セカンダリーフィルターで、グループまたはタグの名前を入力するか、リストをスクロールして複数の選択を行います。

5. システムリストで選択したグループのシステムを表示します。

第5章 参考資料

Compliance サービスの詳細は、以下の資料を参照してください。

- **Ansible Playbook を使用したセキュリティーポリシーコンプライアンスの問題修正**
- **Compliance サービスレポートの生成**
- Insights for Red Hat Enterprise Linux ドキュメント
- Insights for Red Hat Enterprise Linux 製品サポートページ