Red Hat Insights 1-latest

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: 2024-03-27

Red Hat Insights 1-latest 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

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。 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。

目次

第1章 RED HAT INSIGHTS コンプライアンスサービスの概要

Red Hat 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および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ーのセキュリティー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

- コンプライアンス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 Insights for Red Hat Enterprise Linux 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 Red Hat Enterprise Linux およびコンプライアンスサービスを使用するために、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は、Security > Compliance > Reports のポリシーの横に、影響を受けるシステム数に続いて **サポート対象外** の警告が表示されます。

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、Compliance サービスは利用可能な最新バージョンを使用します。

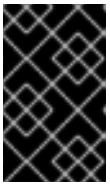
以前のポリシーが SSG でサポートされなくなった理由:

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ため、レポートが正確では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 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、Red Hat Enterprise Linux OS マイナーバージョンなどの特定のデータを編集できます。そのため、コンプライアンス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。

データ編集の詳細は、Red Hat Insights クライアントデータ編集 のドキュメントを参照してください。

Complaince サービス内でのセキュリティーポリシーの作成

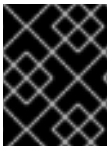
Complaince サービス内で組織のセキュリティーポリシーを作成すると、次のことが可能になります。

- 多くのシステムをポリシーに関連付けることができます。
- RHEL のマイナーバージョンで対応している SCAP Security Guide を使用できます。
- 組織の要件に基づいて、どのルールが含まれるかを編集できます。

1.4. USER ACCESS に関する考慮事項

アカウントの組織管理者は、User Access で設定を行い、Red Hat Insights for Red Hat Enterprise Linux 機能へのアクセスを制御します。アカウントのどのユーザーも、Insights for Red Hat Enterprise Linux のほとんどのデータにアクセスできます。ただし、一部のアクションを実行するには、ユーザーのアクセス権の昇格が必要です。

アクセスの付与は、Red Hat Hybrid Cloud Console の User Access で行います。アクセスを付与または変更するには、組織管理者または User Access 管理者は、Red Hat Hybrid Cloud Console > **Settings** アイコン (⚙) > Identity & Access Management > User Access > Users で必要なロールを持つ User Access グループにユーザーを追加する必要があります。



重要

このドキュメントでは、手順の前提条件で、その手順を実行するためにアクセス権の昇格が必要かどうかを示しています。

User Access を理解するうえで重要な事前定義済みグループおよびロールは次のとおりです。

- **デフォルトのアクセスグループ**
- **Default admin access グループ**
- **組織管理者ロール**

一部の事前定義済みグループおよびロールの概要

アクセスには、以下の事前定義済みのグループおよびロールが関連します。

- **デフォルトのアクセスグループ**: アカウント上のすべてのユーザーが、デフォルトアクセスグループのメンバーです。デフォルトのアクセスグループのメンバーには読み取り専用アクセス権があります。これにより、Insights for Red Hat Enterprise Linux のほとんどの情報を表示できます。
- **デフォルトの管理者アクセスグループ**: アカウント上の組織管理者であるすべてのユーザーは、このグループのメンバーです。ユーザーは、Red Hat が管理するデフォルト管理者アクセスグループのロールを変更できません。デフォルト管理者アクセスグループのメンバーには読み取り/書き込みアクセス権があります。これにより、Insights for Red Hat Enterprise Linux で他のアクションを表示および実行できます。
- **組織管理者ロール**: アカウント上の組織管理者であるすべてのユーザーは、User Access グループを作成および変更し、他のアカウントユーザーにアクセス権利を付与できます。組織管理者であるかどうかを確認するには、画面の右上にある Red Hat Hybrid Cloud Console ヘッダーで自分の名前をクリックして、“Org.Administrator” がユーザー名の下に表示されるかどうかを確認します。

重要

アクセス権の昇格のリクエスト 必要な機能にアクセスできない場合は、以下を実行できます。

- カスタマーサービス に連絡して、アカウントの組織管理者の詳細を取得します。
  - リクエストを送信する際に、アカウント番号を提供してください。
- 組織管理者に連絡し、次の情報を提供してアクセス権の付与を依頼します。
  - アクセスする必要があるロールの名前 (Remediations 管理者など)。
  - User Access に関するすべてのドキュメント へのリンク。アクセス権を付与する方法について組織管理者に知らせるのに役立ちます。

1.4.1. コンプライアンスサービスユーザーの User Access ロール

次のロールにより、Insights for Red Hat Enterprise Linux の修復機能への標準または拡張アクセスが有効になります。

- **Compliance viewer.**コンプライアンスリソースへのアクセス権限を付与するコンプライアンスサービスロール。
- **Compliance administrator.**コンプライアンスリソースへの読み取りアクセスを付与するコンプライアンスロール。コンプライアンス管理者ロールまたはその他の拡張パーミッションを付与されることが必要な手順の場合は、その手順の **前提条件** に記載されます。

第2章 コンプライアンスサービスの使用を開始する

このセクションでは、コンプライアンスデータを Insights for RHEL 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:

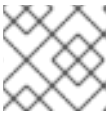
```
[root@insights]# dnf info scap-security-guide-0.1.57-3.el8_4
```

4. サポートされているバージョンの SSG がシステムにインストールされていない場合は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 の Security > Compliance > SCAP policies 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。

関連情報

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 Red Hat 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 Red Hat Enterprise Linux アプリケーションにアップロードするには、**insights-client --compliance** をオンデマンドで、または設定したスケジュールされたジョブで実行する必要があります。

関連情報

How do I set up recurring uploads for Insights services?

3.1. 新しい SCAP ポリシーの作成

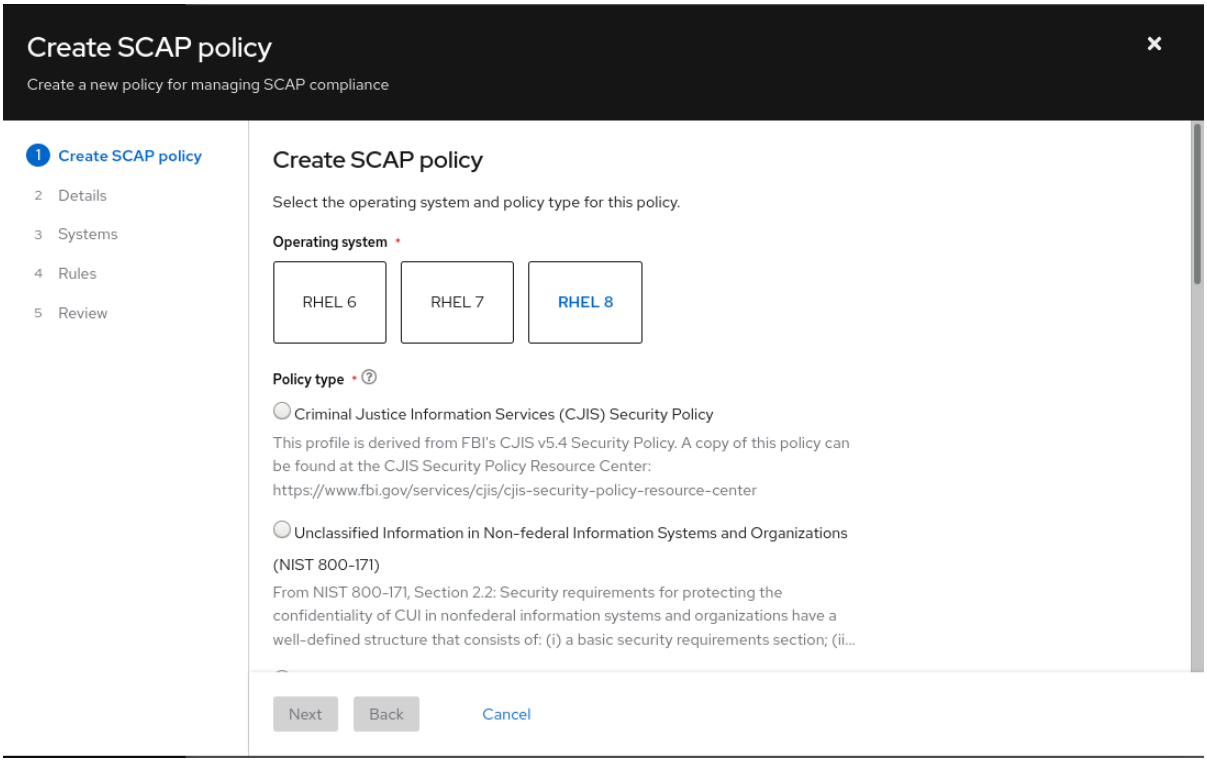
コンプライアンスサービス UI でスキャンを実行したり、そのスキャンの結果を確認したりする前に、Insights for Red Hat Enterprise Linux に登録された各システムを 1 つ以上のセキュリティーポリシーに追加する必要があります。新しいポリシーを作成して、特定のシステムおよびルールを含めるには、以下の手順を実行します。

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。

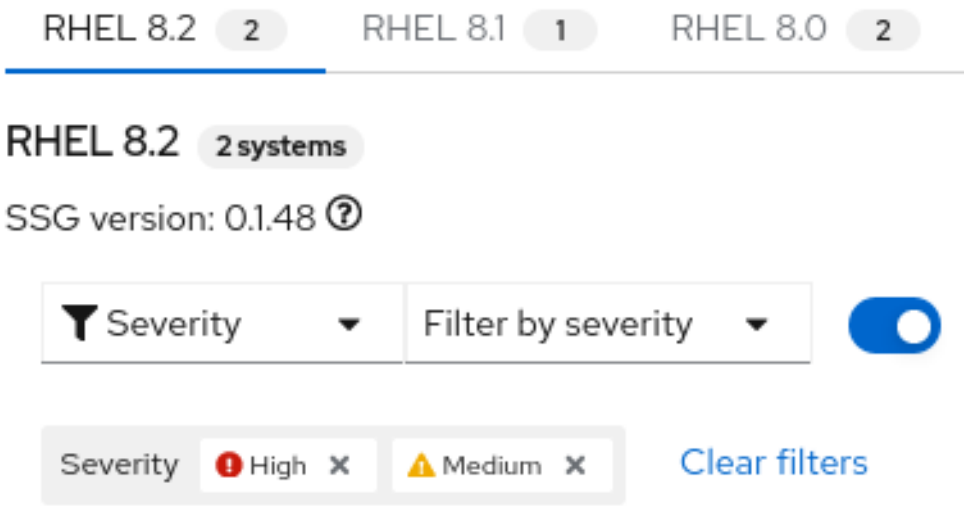
手順

1. **Security > 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 **コンプライアンスのしきい値** 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) を使用できるため、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、ルールのリストを絞り込みます。
   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. コンプライアンスポリシーの編集

コンプライアンスポリシーを作成したら、後でポリシーを編集してポリシーの詳細や、含まれるルールまたはシステムを変更できます。

以下の手順を使用して、組織のニーズに合わせてポリシーを編集します。

User Access Note

ポリシーに含まれるルールおよびシステムを編集する場合は、ユーザーが **コンプライアンス管理者** ロールを持つ User Access Group のメンバーである必要があります。コンプライアンス管理者ロールには、デフォルトですべての Insights for Red Hat Enterprise Linux ユーザーに付与されない拡張パーミッションが含まれます。

3.2.1. ポリシーの詳細の編集

前提条件

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

手順

1. Security > 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. ポリシー名をクリックします。これにより、ポリシー詳細ビューが開きます。
4. 鉛筆アイコンが表示されている場合は、アイコンをクリックしてそのフィールドの詳細を編集できます。編集可能なフィールドには以下が含まれます。
   - コンプライアンスのしきい値
   - ビジネスの目的
   - ポリシーの説明
5. フィールドを編集したら、フィールドの右側にある青いチェックマークをクリックし、入力を保存します。

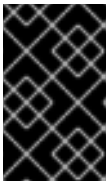
3.2.2. 含まれるルールの編集

前提条件

- Red Hat Hybrid Cloud Console にログインしている。
- **コンプライアンス管理者** の User Access 権限がある。

手順

1. Security > 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 ポップアップで **Rules** タブをクリックします。
5. RHEL マイナーバージョンをクリックします。



重要

RHEL のマイナーバージョンごとに異なる SCAP Style Guide (SSG) バージョンが存在するため、RHEL のマイナーバージョンごとにルールを編集する必要があります。

6. Name フィルターおよび search 関数を使用して、削除するルールを見つけます。

注記

Name プライマリーフィルターを選択した状態で、ルール名またはその識別子で検索できます。

7. 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。
   または、追加するルールの横にあるボックスにチェックを入れます。
8. 各 RHEL マイナーバージョンタブで、これらの手順を繰り返します。
9. **Save** をクリックします。

検証

1. Security > Compliance > SCAP policies ページに移動し、編集され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。

3.2.3. 含まれるシステムの編集

1. Security > 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 ポップアップで、**Systems** タブをクリックします。
   利用可能なシステムの一覧が表示されます。

   ポリシーにすでに含まれているシステムの場合は、システム名の左側のボックスにチェックマークが付いています。

   システム名の横にあるチェックマークのないシステムは、このポリシーには含まれません。
5. 名前でシステムを検索します。このシステムをポリシーに含めるには、システム名の横にあるチェックボックスにチェックを入れます。
   または、ポリシーからシステムを削除するには、システム名の横にあるチェックボックスの選択を解除します。
6. **Save** をクリックして変更を保存します。

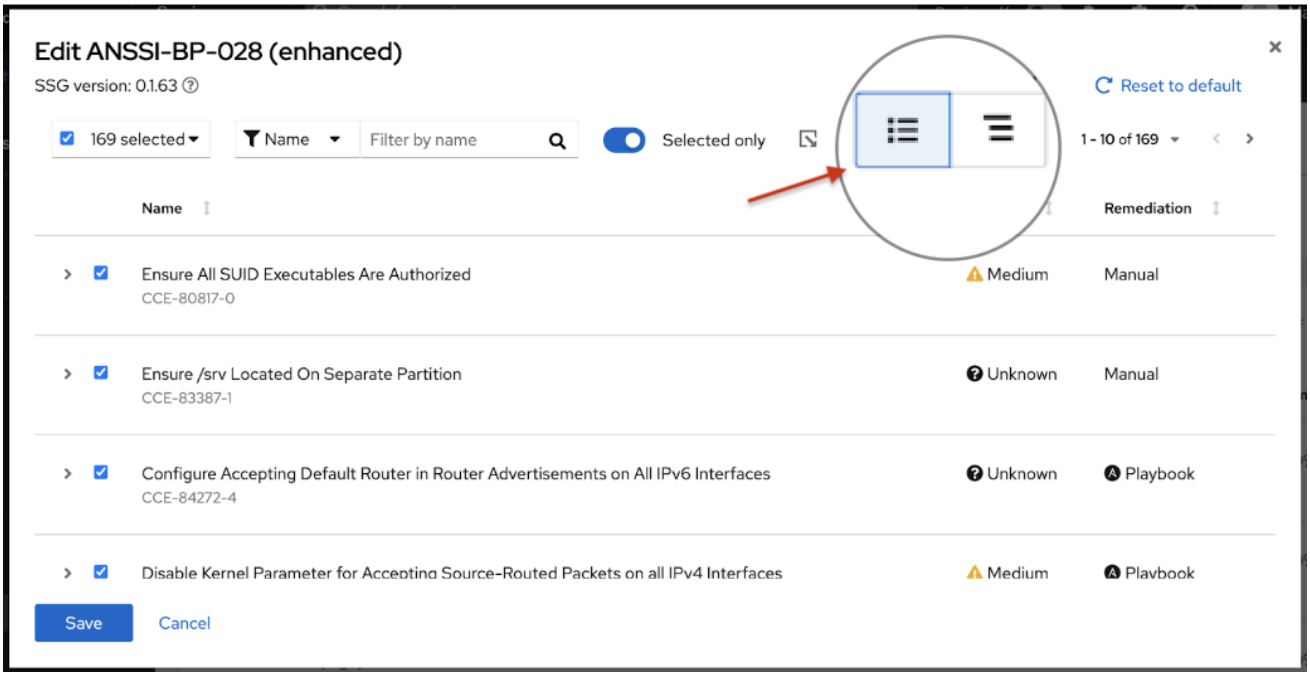
検証

1. Security > Compliance > SCAP policies ページに移動し、編集されたポリシーを見つけます。
2. ポリシーをクリックし、含まれているシステムが編集内容と一致していることを確認します。

3.3. ポリシールールの表示

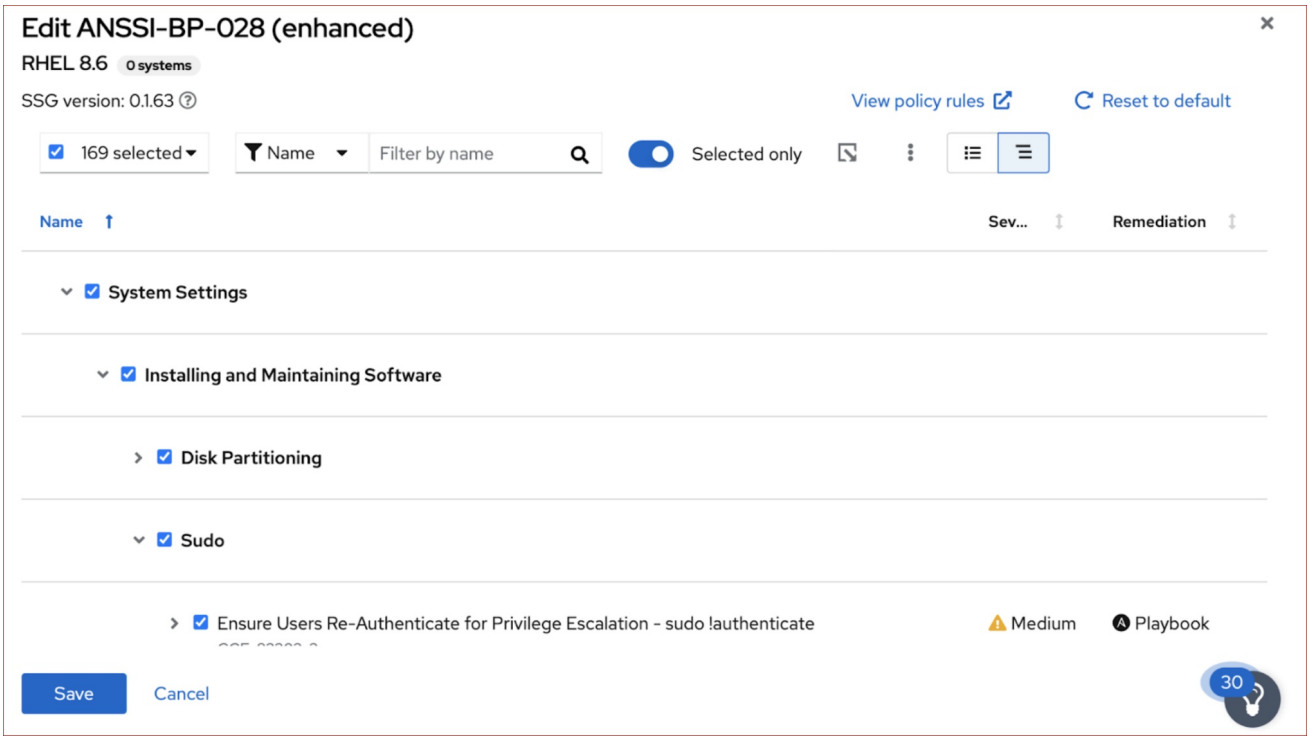
Insights Compliance では、類似したルールがまとまっているように、分類されたグループにルールを分けて表示します。ポリシーに対して実行されるコンプライアンスチェックのカテゴリーまたは分類に従ってグループ化されたルールを表示できます。ネストされたグループ構造 (またはツリービュー) がデフォルトのビューです。ツリービューには、ルールのカテゴリー、場合によってはポリシーの複数のルールを表示できる追加のコンテキスト情報が提供されます。ツリービューでは、編集可能な値を持つルールを表示することもできます (編集可能なルール値の詳細については、“ポリシールールの値の編集” を参照してください)。

ルールはツリービューまたはクラシックビューで表示できます。クラシックビューでは、ルールはリニアリストに表示されます。

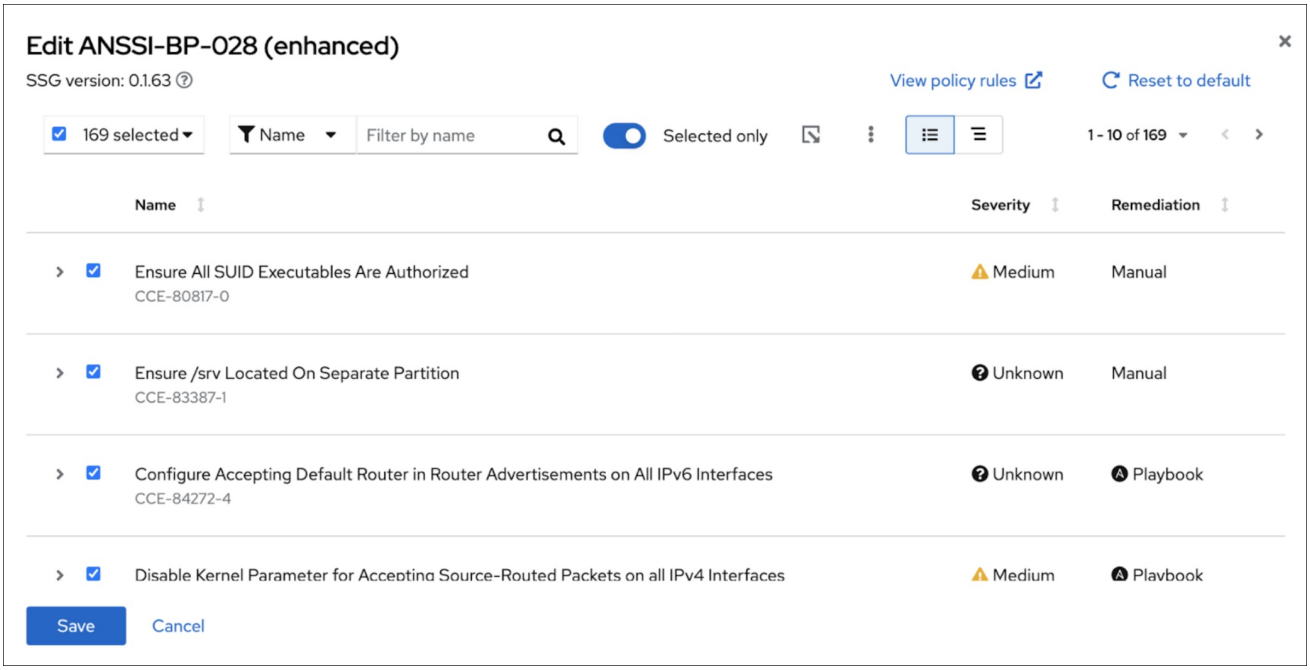


View policy rules の下にある 2 つのボタンを切り替えることで、ツリービューからクラシックビューに切り替えることができます。

ツリービュー形式でルールを表示するには、ツリービューアイコン( ) をクリックします。



クラシックビュー形式でリストされたルールを表示するには、クラシックビューアーイコン ( ) をクリックします。



注記

- フィルター機能を使用して特定のルールを検索すると、ビューは自動的にクラシックビューに切り替わります。
- ルールを展開して追加情報を表示すると、別のビューに切り替えても、ルールは展開ビューのままとなります。

次の場合にビューを切り替えることができます。

- 既存のポリシーの編集
- 新しい SCAP ポリシーの作成
- コンプライアンスサービスレポートの生成 ("レポートのエクスポート" トピックを参照)

3.4. ポリシールールの値の編集

組織では、セキュリティー要件に基づいて規制順守ポリシーをある程度カスタマイズする必要がある場合があります。カスタマイズの 1 つのレベルは、組織のニーズに適用されないルールを追加または削除することです。ポリシー内のルールの値を編集することで、コンプライアンスサービスの SCAP ポリシーをカスタマイズできます。特定の値を編集すると、より詳細な制御が可能になり、組織のセキュリティーニーズを満たす正確な追跡が可能になります。特定のニーズに合わせてポリシーを編集することで、セキュリティー体制に関連し、意味のあるコンプライアンスフレームワークを作成できます。

ルール値について

ルールは、特定の SCAP Security Guide (SSG) バージョンに対して複数回表示される可能性があるため、同じ SSG バージョン内の複数のルールに同じ値を使用することができます。このような場合、SSG バージョンで特定のポリシーのルールの値を更新しても、他のポリシーのルールは更新されません。現在のポリシーと更新している SSG バージョンのルールのみが更新されます。

さらに、ルールは RHEL のマイナーバージョンごとに異なる可能性があり、異なることになります。たとえば、RHEL 8.5 と RHEL 8.7 を使用している場合、RHEL 8.5 ルールのルールの値を変更しても、RHEL 8.7 の値は自動的に編集されません。必要に応じて、リストされている RHEL バージョンごとに

値を個別に変更する必要があります。また、あるバージョンのルールが別のバージョンでは同じではないこともわかります。

ルールの値を編集するには、次の手順を使用します。

前提条件

- Red Hat Hybrid Cloud Console にログインしている。
- コンプライアンス管理者のロールまたは "ポリシーの編集" 権限を持つユーザーでログインしています。Insights コンプライアンスのロールベースアクセス制御 (RBAC) の詳細は、コンプライアンスサービスユーザーの User Access ロール を参照してください。

手順

1. Security > Compliance > SCAP policies に移動します。
2. 編集するポリシーを見つけます。
3. 編集するルールが含まれるポリシーをクリックします。
4. **Rules** タブをクリックします。**Filter by name** フィールドに、編集するルールの最初の数文字を入力します。この例では、 **ANSSI** と入力します。
5. 編集するルールを見つけて、ルールの横にあるキャレットをクリックし、コンテンツを展開します。
6. 展開したテキスト内で **Depends on values** フィールドを見つけて、値の編集アイコン ( ) をクリックして値を変更します。(**Depends on values** が表示されない場合、値は編集できません。)
7. 値を編集します。デフォルト値に戻すには、元に戻すアイコン ( ) をクリックします。編集された値は入力された値をチェックまたは検証しないため、編集を慎重に確認してください。たとえば、数値が必要な値フィールドに記号を入力しても、エラーメッセージは表示されません。
8. 保存アイコン ( ) をクリックして、新しい値を保存します。**Rule value updated** を示すアラートが画面に表示されます。
9. (オプション) 編集した値をデフォルト値に戻すには、元に戻すアイコン ( ) をクリックします。**Rule values reset to default.** という警告メッセージが表示されます。編集の進行中または編集を保存した後に、デフォルト値に戻すことができます。元に戻すアイコンの存在は、値がデフォルト値と異なることを示します。

重要

現在、コンプライアンスサービスは、50 文字を超えるルール値、または複数の値を持つルールをサポートしていません。

注記

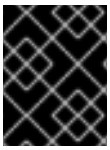
コンプライアンスサービスの SCAP ポリシーセクション内のルールのルール値のみを編集できます。編集内容は、Security > Compliance > Reports セクションで確認できますが、レポートセクションでは編集できません。

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ならびにシステムのデータ (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 Red Hat Enterprise Linux サービスと同様に、コンプライアンスサービスもシステムグループタグによるフィルタリングを有効にします。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. コンプライアンスレポート

Security > Compliance > Reports から、以下のプライマリーフィルターおよびセカンダリーフィルターを使用して、特定または限定された範囲のレポートセットにフォーカスします。

- **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。** 追加さ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

Security > Compliance > SCAP policies から、**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。

- **詳細。** 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。
- **ルール。** 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。
- **システム。** 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、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

Security > Compliance > Systems のデフォルトの機能は、システム名で検索することです。

- **タグ。**システムグループまたはタグ名で検索します。
- **名前。**システム名で検索します。
- **ポリシー。**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で検索して、RHEL 7 または RHEL 8 システムのみを表示します。

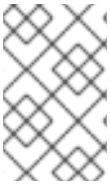
4.4. 検索

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 ポリシー。**名前で特定のポリシーを検索します。
- **システム。**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。

第5章 システムタグとグループ

Red Hat Insights for Red Hat Enterprise Linux を使用すると、管理者はグループタグを使用して、インベントリー内のシステムや個々のサービスでシステムのグループをフィルターできます。グループは、Insights for Red Hat Enterprise Linux へのシステムデータの取り込み方法によって識別されます。Insights for RHEL を使用すると、SAP ワークロードを実行しているシステム、Satellite ホストグループ、Microsoft SQL Server ワークロード、およびルートアクセス権を持つシステム管理者がシステムで Insights クライアントを設定するために定義したカスタムタグによって、システムのグループをフィルタリングできます。



注記

2022 年 春の時点で、インベントリー、アドバイザー、コンプライアンス、脆弱性、パッチ、ドリフト、およびポリシーで、グループとタグによるフィルタリングが有効になります。その他のサービスは後から続きます。

重要

タグ付けを有効にする他のサービスとは異なり、コンプライアンスサービスは、コンプライアンスサービス UI のシステムのリスト内にタグを設定します。詳細は、次のセクション **コンプライアンスサービスのグループフィルターとタグフィルター** を参照してください。

グローバルな **フィルター結果** ボックスを使用して、SAP ワークロード、Satellite ホストグループ、MS SQL Server ワークロード、または Insights クライアント設定ファイルに追加されたカスタムタグでフィルター処理します。

前提条件

Red Hat Insights for Red Hat Enterprise Linux のタグ付け機能を使用するには、以下の前提条件および条件を満たしている必要があります。

- Red Hat Insights クライアントが各システムにインストールされている。
- カスタムタグを作成したり、**/etc/insights-client/tags.yaml** ファイルを変更したりするには、ルート権限、または同等の権限が必要です。

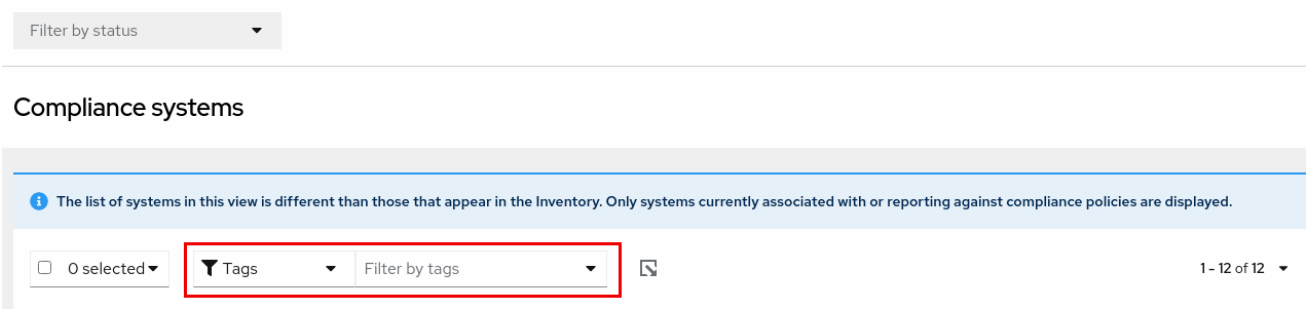
5.1. コンプライアンスサービスのグループおよびタグフィルター

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 Red Hat Enterprise Linux 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



5.2. SAP ワークロード

2025 年に Linux は SAP ERP ワークロードの必須オペレーティングシステムになるため、Red Hat Enterprise Linux および Red Hat Insights for Red Hat Enterprise Linux では、Insights for RHEL が SAP 管理者に選ばれる管理ツールとなるように取り組んでいます。

この継続的な取り組みの一環として、Insights for Red Hat Enterprise Linux は、管理者によるカスタマイズを必要とせずに、SAP ワークロードを実行しているシステムに SAP ID (SID) によって自動的にタグを付けます。ユーザーは、グローバル **Filter by tags** ドロップダウンメニューを使用して、Insights for Red Hat Enterprise Linux アプリケーション全体でこれらのワークロードを簡単にフィルター処理できます。

5.3. SATELLITE ホストグループ

Satellite ホストグループは Satellite で設定され、Insights for Red Hat Enterprise Linux で自動的に認識されます。

5.4. MICROSOFT SQL SERVER のワークロード

タグによるグローバルフィルター 機能を使用して、Red Hat Insights for Red Hat Enterprise Linux ユーザーは、Microsoft SQL Server ワークロードを実行しているシステムのグループを選択できます。

2019 年 5 月、Red Hat Insights チームは、Red Hat Enterprise Linux (RHEL) で実行されている Microsoft SQL Server 向けの RHEL 推奨事項の新しい一連の Insights を導入しました。これらのルールは、オペレーティングシステムレベルの設定が Microsoft および Red Hat から文書化された推奨事項に準拠していないことを管理者に警告します。

これらのルールの制限は、データベース自体ではなく、主にオペレーティングシステムを分析することでした。Insights for Red Hat Enterprise Linux および RHEL 8.5 の最新リリースでは、Microsoft SQL Assessment API が導入されています。SQL Assessment API は、MS SQL Server のデータベース設定のベストプラクティスを評価するメカニズムを提供します。API には、Microsoft SQL Server チームが提案するベストプラクティスルールを含むルールセットが付属しています。このルールセットは新しいバージョンのリリースで拡張されていますが、API は高度にカスタマイズ可能で拡張可能なソリューションを提供することを目的として構築されており、ユーザーはデフォルトのルールを調整して独自のルールを作成できます。

SQL Assessment API は PowerShell for Linux (Microsoft から入手可能) でサポートされており、Microsoft は、API を呼び出してその結果を JSON 形式のファイルとして保存するために使用できる PowerShell スクリプトを開発しました。RHEL 8.5 では、Insights クライアントがこの JSON ファイルをアップロードし、結果を Insights for Red Hat Enterprise Linux UI にわかりやすい形式で表示するようになりました。

Insights for Red Hat Enterprise Linux での SQL Server 評価の詳細については、Red Hat Insights で利用できるようになった SQL Server データベースのベストプラクティス を参照してください。

5.4.1. SQL Server 評価の設定

Red Hat Insights に情報を提供するように Microsoft SQL Assessment API を設定するには、データベース管理者は以下の手順を実行する必要があります。

手順

1. 評価するデータベースで、SQL 認証を使用して SQL Server 評価用のログインを作成します。次の Transact-SQL は、ログインを作成します。**<*PASSWORD*>** を強力なパスワードに置き換えます。

```
USE [master]
GO
CREATE LOGIN [assessmentLogin] with PASSWORD= N'<*PASSWORD*>'
ALTER SERVER ROLE [sysadmin] ADD MEMBER [assessmentLogin]
GO
```

2. システムにログインするための認証情報を次のように保存します。ここでも <*PASSWORD*> をステップ 1 で使用したパスワードに置き換えます。

```
# echo "assessmentLogin" > /var/opt/mssql/secrets/assessment
# echo "<*PASSWORD*>" >> /var/opt/mssql/secrets/assessment
```

3. mssql ユーザーのみが資格情報にアクセスできるようにして、評価ツールで使用される資格情報を保護します。

```
# chmod 0600 /var/opt/mssql/secrets/assessment
# chown mssql:mssql /var/opt/mssql/secrets/assessment
```

4. microsoft-tools リポジトリーから PowerShell をダウンロードします。これは、SQL Server インストールの一部として **mssql-tools** および **mssqlodbc17** パッケージをインストールしたときに設定したものと同じリポジトリーです。

```
# yum -y  install powershell
```

5. PowerShell 用の SQLServer モジュールをインストールします。このモジュールには、評価 API が含まれています。

```
# su mssql -c "/usr/bin/pwsh -Command Install-Module SqlServer"
```

6. Microsoft のサンプル GitHub リポジトリーから runassessment スクリプトをダウンロードします。mssql によって所有され、実行可能であることを確認してください。

```
# /bin/curl -LJ0 -o /opt/mssql/bin/runassessment.ps1
https://raw.githubusercontent.com/microsoft/sql-server-samples/master/samples/manage/sql-assessment-api/RHEL/runassessment.ps1
# chown mssql:mssql /opt/mssql/bin/runassessment.ps1
# chmod 0700 /opt/mssql/bin/runassessment.ps1
```

7. Red Hat Insights が使用するログファイルを保存するディレクトリーを作成します。繰り返しますが、mssql によって所有され、実行可能であることを確認してください。

```
# mkdir /var/opt/mssql/log/assessments/
# chown mssql:mssql /var/opt/mssql/log/assessments/
# chmod 0700 /var/opt/mssql/log/assessments/
```

8. 最初の評価を作成できるようになりましたが、mssql ユーザーとしてより安全に cron または systemd を介して後続の評価を自動的に実行できるように、必ずユーザー mssql として作成してください。

```
# su mssql -c "pwsh -File /opt/mssql/bin/runassessment.ps1"
```

9. Insights for Red Hat Enterprise Linux は、次回の実行時に評価を自動的に含めます。または、次のコマンドを実行して Insights クライアントを開始することもできます。

```
# insights-client
```

5.4.1.1. タイマーでの SQL 評価の設定

SQL Server の評価は完了するまでに 10 分以上かかる場合があるため、評価プロセスを毎日自動的に実行することが理にかなっている場合とそうでない場合があります。それらを自動的に実行したい場合は、Red Hat SQL Server コミュニティーが評価ツールで使用する systemd サービスとタイマーファイルを作成しています。

手順

1. Red Hat public SQL Server Community of Practice GitHub サイト から次のファイルをダウンロードします。
   - **mssql-runassessment.service**
   - **mssql-runassessment.timer**
2. 両方のファイルをディレクトリー **/etc/systemd/system/** にインストールします。

```
# cp mssql-runassessment.service /etc/systemd/system/
# cp mssql-runassessment.timer /etc/systemd/system/
# chmod 644 /etc/systemd/system/
```

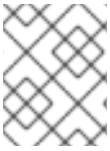
3. 次のコマンドでタイマーを有効にします。

```
# systemctl enable --now mssql-runassessment.timer
```

5.5. システムタグ付けのカスタム

システムにカスタムグルーピングとタグ付けを適用して、個別のシステムにコンテキストマーカーを追加したり、Insights for Red Hat Enterprise Linux アプリケーションでこれらのタグ別にフィルタリングしたり、より簡単に関連システムに焦点を当てたりすることができます。この機能は、何百または何千ものシステムが管理されている環境で、Red Hat Enterprise Linux の Insights を大規模にデプロイメントする場合に特に価値があります。

複数の Insights for Red Hat Enterprise Linux サービスにカスタムタグを追加する機能に加えて、定義済みタグを追加できます。advisor サービスは、これらのタグを使用して、より高いレベルのセキュリティーを必要とするシステムなど、より注意が必要なシステムに的を絞った推奨事項を作成できます。



注記

カスタムタグと定義済みタグを作成するには、**/etc/insights-client/tags.yaml** ファイルに追加または変更するための root 権限、またはそれと同等の権限が必要です。

5.5.1. タグ構造

タグは、**namespace/key=value** のペアの構造を使用します。

- **名前空間。**名前空間は、インジェストポイントである **insights-client** の名前であり、変更することはできません。**tags.yaml** ファイルは名前空間から抽象化され、アップロード前に Insights クライアントによって挿入されます。
- **キー。**キーは、ユーザーが選択したキーまたはシステムの定義済みのキーにすることができます。大文字、文字、数字、記号、および空白文字の組み合わせを使用できます。
- **値。**独自の記述文字列値を定義します。大文字、文字、数字、記号、および空白文字の組み合わせを使用できます。

注記

advisor サービスには、Red Hat がサポートする定義済みタグが含まれています。

5.5.2. tags.yaml ファイルの作成とカスタムグループの追加

insights-client --group=<name-you-choose> を使用してタグ作成し、**/etc/insights-client/tags.yaml** に追加します。これは、以下を実行します。

- **etc/insights-client/tags.yaml** ファイルを作成します。
- **group=** キーおよび **<name-you-choose>** の値を **tags.yaml** に追加します。
- システムから Insights for Red Hat Enterprise Linux アプリケーションに新規アーカイブをアップロードすることで、最新の結果とともに新しいタグがすぐに表示されます。

初期 **グループ** タグを作成したら、必要に応じて **/etc/insights-client/tags.yaml** ファイルを編集し、タグを追加します。

次の手順は、**/etc/insights-client/tags.yaml** ファイルと初期グループを作成し、そのタグが Insights for Red Hat Enterprise Linux インベントリーに存在することを確認する方法を示しています。

グループの新規作成手順

1. **--group=** の後にカスタムグループ名を追加して、root で以下のコマンドを実行します。

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

tags.yaml 形式の例

次の **tags.yaml** ファイルの例は、新しいグループに追加されたファイル形式と追加のタグの例を示しています。

```
# tags
---
group: eastern-sap
```

```
name: Jane Example
contact: jexample@corporate.com
Zone: eastern time zone
Location:
- gray_rack
- basement
Application: SAP
```

カスタムグループが作成されたことを確認する手順

1. 必要に応じて Red Hat Insights > RHEL > Inventory に移動し、ログインします。
2. **Filter results** ドロップダウンメニューをクリックします。
3. リストをスクロールするか、検索機能を使用してタグを見つけます。
4. タグをクリックしてフィルター処理を行います。
5. システムが、アドバイザーシステムリストの結果に含まれていることを確認します。

システムがタグ付けされていることを確認する手順

1. 必要に応じて Red Hat Insights > RHEL > Inventory に移動し、ログインします。
2. **Name** フィルターをアクティブにし、システムが表示されるまでシステム名を入力してから選択します。
3. システム名の横にタグシンボルがグレイになり、適用されるタグの正確な数を表す数字が表示されることを確認します。

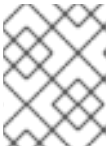
5.5.3. タグの追加または変更を行うための tags.yaml の編集

グループフィルターを作成したら、必要に応じて **/etc/insights-client/tags.yaml** の内容を編集して、タグの追加または変更を行います。

手順

1. コマンドラインで、編集するタグ設定ファイルを開きます。
   [root@server ~]# vi /etc/insights-client/tags.yaml
2. 必要に応じてコンテンツを編集するか、追加値を追加します。以下の例は、システムに複数のタグを追加する際の **tags.yaml** の管理方法を示しています。

```
# tags
---
group: eastern-sap
location: Boston
description:
- RHEL8
- SAP
key 4: value
```



注記

必要な数の key=value ペアを追加します。大文字、文字、数字、記号、および空白文字の組み合わせを使用します。

3. 変更を保存してエディターを閉じます。

4. オプションで、Red Hat Enterprise Linux の Insights へのアップロードを生成します。

```
# insights-client
```

5.5.4. 定義済みのシステムタグを使用した Red Hat Insights advisor サービスの推奨事項の精度とセキュリティーの向上

Red Hat Insights advisor サービスの推奨事項は、すべてのシステムを同等に扱います。ただし、システムによっては、他のシステムよりも高いレベルのセキュリティーが必要な場合や、異なるネットワークパフォーマンスレベルが必要な場合があります。カスタムタグを追加する機能に加えて、Red Hat Insights for Red Hat Enterprise Linux は定義済みタグを提供します。advisor サービスはこれを使用して、より注意が必要な可能性のあるシステムに的を絞った推奨事項を作成できます。

定義済みタグによって提供される拡張されたセキュリティー強化と強化された検出および修復機能をオプトインして取得するには、タグを設定する必要があります。設定後、advisor サービスは、調整された重大度レベルと、システムに適用されるネットワークパフォーマンス設定に基づいて推奨事項を提供します。

タグを設定するには、**/etc/insights-client/tags.yaml** ファイルを使用して、インベントリーサービスでシステムにタグを付ける場合と同様の方法で、定義済みタグを使用してシステムにタグを付けます。定義済みタグは、カスタムタグの作成に使用されるのと同じ **key=value** 構造を使用して設定されます。Red Hat の定義済みタグの詳細を次の表に示します。

表5.1 サポートされている定義済みタグのリスト

キー	値	注記
security	**normal** (デフォルト) / **strict**	**default** を使用すると、advisor サービスは、システムのリスクプロファイルを、RHEL の最新バージョンのデフォルト設定および頻繁に使用される使用パターンから導出されたベースラインと比較します。これにより、推奨事項の焦点があっており、アクション可能で、数を減らすことができます。**strict** 値を使用すると、advisor サービスはセキュリティーが重要なシステムであると見なし、特定の推奨事項でより厳密なベースラインが使用されるようになり、新しい最新の RHEL インストールでも推奨事項が表示される可能性があります。

キー	値	注記
network_performance	**null** (デフォルト) / **latency** / **throughput**	ネットワークパフォーマンス設定 (ビジネス要件に応じたレイテンシーまたはスループット) は、システムに対する advisor サービスの推奨事項の重大度に影響します。

注記

定義済みタグのキー名は予約されています。定義済みの値とは異なる値を持つキー **security** をすでに使用している場合、推奨事項に変更は加えられません。既存の **key=value** がいずれかの定義済みのキーと同じ場合にのみ、推奨事項に変更が加えられます。たとえば、**key=value** が **security: high** の場合、Red Hat の定義済みタグが原因で、推奨事項は変更されません。**key=value** ペアが **security: strict** である場合は、システムの推奨事項に変更が加えられます。

関連情報

- システムタグを使用して、拡張セキュリティー強化の推奨事項を有効にする
- タグを活用して Red Hat Insights Advisor の推奨機能の環境認識を向上させる
- システムタグ付けのカスタム

5.5.5. 定義済みタグの設定

Red Hat Insights for Red Hat Enterprise Linux advisor サービスの定義済みタグを使用すると、システムの推奨事項の動作を調整し、拡張されたセキュリティー強化と強化された検出および修復機能を得ることができます。以下の手順に従って、事前定義されたタグを設定できます。

前提条件

- システムへのルートレベルのアクセスがある。
- Insights クライアントがインストールされている。
- Insights クライアント内にシステムが登録されている。
- すでに **tags.yaml** ファイルを作成している。tags.yaml ファイルの作成とカスタムグループの追加 を参照してください。

手順

1. コマンドラインと任意のエディターを使用して、**/etc/insights-client/tags.yaml** を開きます。(次の例では Vim を使用しています。)

```
[root@server ~]# vi /etc/insights-client/tags.yaml
```

2. **/etc/insights-client/tags.yaml** ファイルを編集して、タグの定義済みの **key=value** ペアを追加します。この例は、**security: strict** および **network_performance: latency** タグを追加する方法を示しています。

```
# cat /etc/insights-client/tags.yaml
group: redhat
location: Brisbane/Australia
description:
- RHEL8
- SAP
security: strict
network_performance: latency
```

3. 変更を保存します。
4. エディターを終了します。
5. **オプション: Insights-client** コマンドを実行して、Red Hat Insights for Red Hat Enterprise Linux へのアップロードを生成するか、次のスケジュールされた Red Hat Insights アップロードまで待ちます。

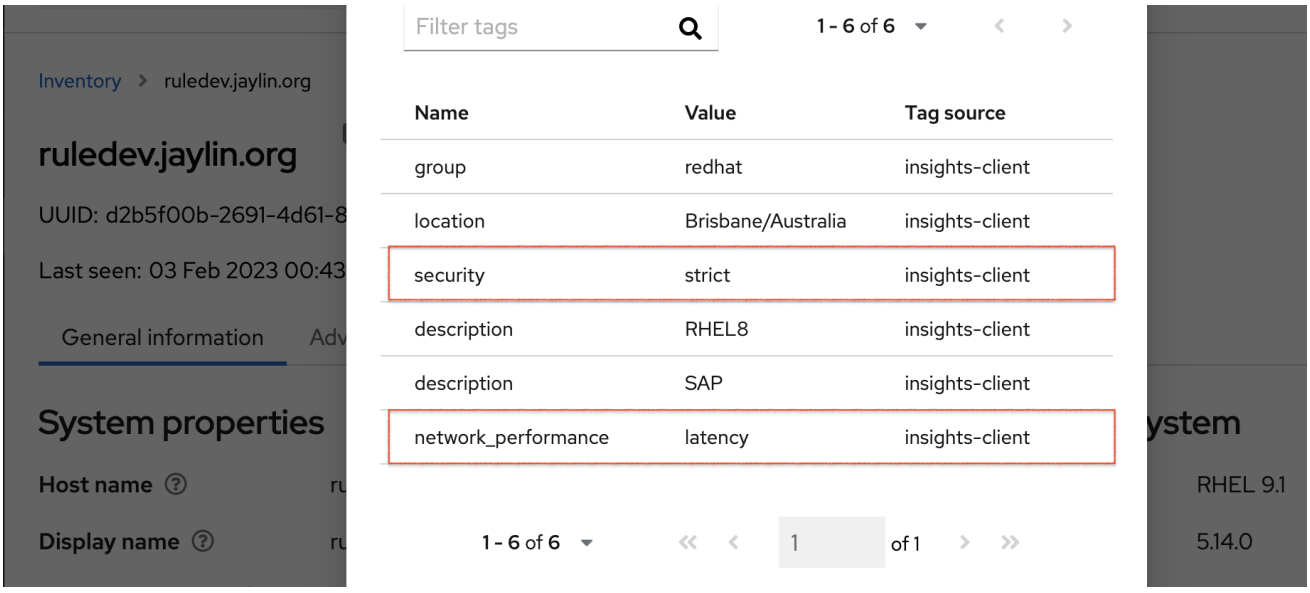
```
[root@server ~]# insights-client
```

定義済みタグが実稼働環境にあることの確認

Red Hat Insights へのアップロードを生成した後 (または、次の Insights アップロードのスケジュールを待った後)、Red Hat Insights > RHEL > Inventory にアクセスして、タグが実稼働環境にあるかどうかを確認できます。システムを見つけて、新たに作成されたタグを探します。次のことを示す表が表示されます。

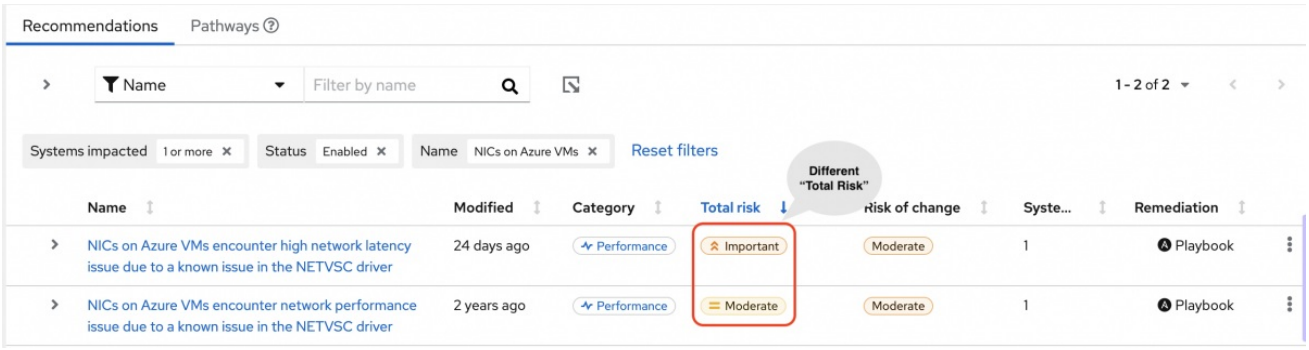
- 名前
- 値
- タグソース (例: insights-client)。

次のイメージは、タグを作成した後にインベントリーに表示される内容の例を示しています。



定義済みタグを適用した後の推奨事項の例

次の図では、advisor サービスは **network_performance: latency** タグが設定されたシステムを示しています。



システムは、総リスク (重要に分類) が高い推奨事項を表示します。**network_performance: latency** タグのないシステムの場合、総リスクは中程度に分類されます。総リスクの高さに基づいて、システムの優先順位付けに関する決定を行うことができます。

第6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。

- **コンプライアンスサービスレポートの生成**
- Red Hat Insights for Red Hat Enterprise Linux ドキュメント
- Red Hat Insights for Red Hat Enterprise Linux 製品サポートページ

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。