



Red Hat Insights 2023

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

Red Hat Insights 2023 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

Copyright © 2023 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[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] 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[®] 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

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	3
1.1. 要件および前提条件	3
1.2. サポートされる構成	3
1.3. ベストプラクティス	4
1.4. ユーザーアクセスに関する考慮事項	5
第2章 コンプライアンスサービスの使用を開始する	6
第3章 INSIGHTSFOR RHEL コンプライアンスサービスでの SCAP セキュリティポリシーの管理	8
3.1. 新しい SCAP ポリシーの作成	8
3.2. 既存のポリシーの編集	10
第4章 コンプライアンスレポートの分析およびトリージ	12
4.1. コンプライアンスレポート	12
4.2. SCAP ポリシー	12
4.3. SYSTEMS	13
4.4. 検索	13
第5章 システムタグとグループ	14
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	14
5.2. SAP ワークロード	15
5.3. SATELLITE ホストグループ	15
5.4. MICROSOFT SQL SERVER のワークロード	15
5.5. システムタグ付けのカスタム	17
第6章 参考資料	24
RED HAT ドキュメントへのフィードバック (英語のみ)	25

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

- [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 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、[Red Hat Enterprise Linux > Compliance > Reports](#) のポリシーの横で、サポートされない警告と、影響を受けるシステムが続いて表示されます。



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

DISA STIG for Red Hat Enterprise Linux 7 ⓘ
DISA STIG for Red Hat Enterprise Linux 7

RHEL 7

0%
0 of 0 systems ▲ 1 unsupported

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、Compliance サービスによる正確なレポート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。

Compliance 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。

1.4. ユーザーアクセスに関する考慮事項

Red Hat Enterprise Linux 機能の Red Hat Insights へのアクセスは、アカウントの組織管理者がユーザーアクセスで設定した設定によって制御されます。アカウントのすべてのユーザーは、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、ユーザーに昇格されたアクセス権が必要なアクションがいくつかあります。

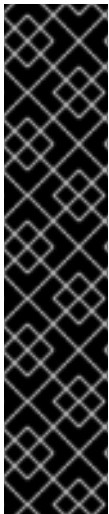


重要

このドキュメントでは、手順の前提条件で、手順を実行するために昇格したアクセス権が必要かどうかを宣言しています。

次の事前定義されたロールは、アクセスに特に関連しています。

- **デフォルトのアクセスグループ。** アカウントのすべての人は、デフォルトアクセスグループのメンバーです。Default アクセスグループのメンバーとして、すでに Insights for Red Hat Enterprise Linux のほとんどの情報を表示できます。
- **組織管理者。** アカウントの組織管理者は、ユーザーアクセス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を付与できます。画面の右上にある Red Hat Hybrid Cloud Console のヘッダーで自分の名前をクリックすると、自分が組織管理者であるかどうかを確認できます。管理者は、ユーザー名のすぐ下にあります。



重要

拡張アクセスのリクエスト 必要だと思われる機能を利用できない場合、以下のことが必要な場合があります。

- 組織管理者の詳細については、[カスタマーサービス](#) にお問い合わせください。
 - 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。
- その個人に連絡してアクセスを依頼し、次の情報を提供します。
 - アクセスする必要があるロールの名前。例: Remediations administrator
 - 組織管理者にアクセスを提供する方法を知らせるのに役立つ、完全な [ユーザーアクセスドキュメント](#) へのリンク。

1.4.1. コンプライアンスサービスユーザーのユーザーアクセスロール

以下のロールは、Red Hat Enterprise Linux の Insights の修復機能への標準または拡張アクセスを有効にします。

- **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。

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:

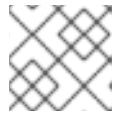
```
[root@insights]# dnf install scap-security-guide-0.1.57-3.el8_4
```

5. コンプライアンスサービス UI の [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。

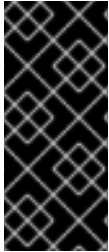
7. [Generating Compliance Service Reports](#) に移動し、結果を表示します。
8. 必要に応じて、[コンプライアンスジョブ](#) を cron で実行するようにスケジュールします。

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 セキュリティー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

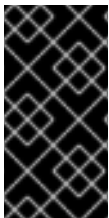
その他のほとんどの Red Hat Insights for Red Hat Insights サービスとは異なり、コンプライアンスサービスはデフォルトのスケジュールで自動的に実行されません。OpenSCAP データを Insights for Red Hat Enterprise Linux アプリケーションにアップロードするには、**insights-client --compliance** をオンデマンドで、または設定したスケジュールされたジョブで実行する必要があります。

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. [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。

Create SCAP policy

Create a new policy for managing SCAP compliance

1 Create SCAP policy

2 Details

3 Systems

4 Rules

5 Review

Create SCAP policy

Select the operating system and policy type for this policy.

Operating system

RHEL 6

RHEL 7

RHEL 8

Policy type

Criminal Justice Information Services (CJIS) Security Policy

This profile is derived from FBI's CJIS v5.4 Security Policy. A copy of this policy can be found at the CJIS Security Policy Resource Center:
<https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>

Unclassified Information in Non-federal Information Systems and Organizations (NIST 800-171)

From NIST 800-171, Section 2.2: Security requirements for protecting the confidentiality of CUI in nonfederal information systems and organizations have a well-defined structure that consists of: (i) a basic security requirements section; (ii...

Next
Back
Cancel

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。

RHEL 8.2 2
RHEL 8.1 1
RHEL 8.0 2





- 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カラー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。

RHEL 8.2 **2** RHEL 8.1 **1** RHEL 8.0 **2**

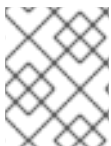
RHEL 8.2 **2 systems**

SSG version: 0.1.48 

Severity  Filter by severity  

Severity  High   Medium  [Clear filters](#)

- 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

コンプライアンスポリシーの作成後に、ポリシーを編集して、含め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、特定のルールまたはシステムを追加または削除します。コンプライアンスポリシーの編集は、Red Hat Hybrid Cloud Console のコンプライアンスサービスポリシーページで行われます。ポリシーの詳細ビューから、含めるルールをルールタブで、含めるシステムをシステムタブで編集できます。

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

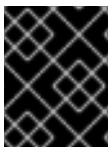
1. [Red Hat Enterprise Linux > Compliance > SCAP policies](#) ページに移動し、編集したポリシーを見つけます。
2. ポリシーをクリックし、追加したルールが編集した内容と一致していることを確認します。

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

[Red Hat Enterprise Linux > 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、特定のレポートの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

[Red Hat Enterprise Linux > 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

デフォルトで [Red Hat Enterprise Linux > Compliance > Systems](#) の機能は、システム名で検索します。

- **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。

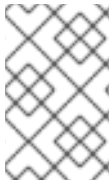
4.4. 検索

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。

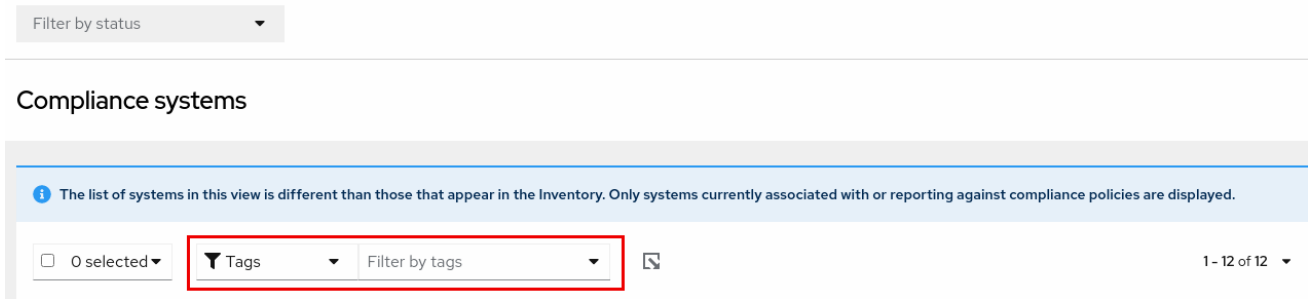
5.1. コンプライアンスサービスのグループおよびタグフィルター

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一リポジトリです。

```
# 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 -LJO -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/
```

- 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"
```

- 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

- [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**
- 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/
```

- 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 Enterprise Linux > 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. 一覧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一覧の結果に含まれていることを確認します。
6. システムがタグ付けされていることを確認する手順
7. 必要に応じて [Red Hat Enterprise Linux > Inventory](#) に移動し、ログインします。
8. **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。
9. 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、または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、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 root 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 (またはスケジュールされた次の Insights アップロードを待っている間)、[Red Hat Enterprise Linux > 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に表示される内容の例を示しています。

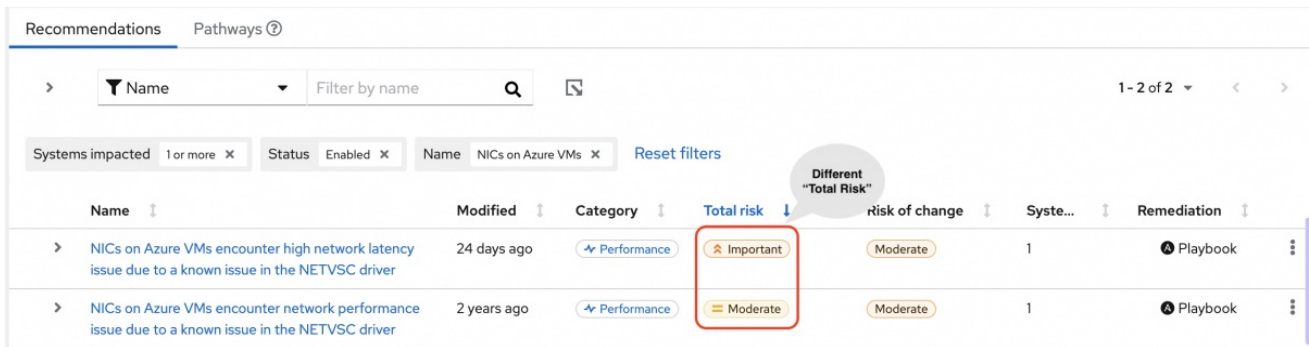
The screenshot shows the 'Inventory' page for a system named 'ruledev.jaylin.org'. A table titled 'Filter tags' displays the following data:

Name	Value	Tag source
group	redhat	insights-client
location	Brisbane/Australia	insights-client
security	strict	insights-client
description	RHEL8	insights-client
description	SAP	insights-client
network_performance	latency	insights-client

The 'security' and 'network_performance' rows are highlighted with red boxes in the original image. The page also shows system details like 'Host name' and 'Display name' on the left, and 'System properties' like 'RHEL 9.1' and '5.14.0' on the right.

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。



Name	Modified	Category	Total risk	risk of change	Syste...	Remediation
> NICs on Azure VMs encounter high network latency issue due to a known issue in the NETVSC driver	24 days ago	Performance	Important	Moderate	1	Playbook
> NICs on Azure VMs encounter network performance issue due to a known issue in the NETVSC driver	2 years ago	Performance	Moderate	Moderate	1	Playbook

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。

- [Compliance 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)

当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、コメントを追加してください。

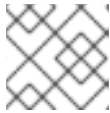
前提条件

- Red Hat カスタマーポータルにログインしている。
- Red Hat カスタマーポータルで、**Multi-page HTML** 形式でドキュメントを表示している。

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 **Feedback** 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、**Multi-page 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. 強調表示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。