Red Hat Insights 2020-10

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

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: 2021-03-02

Red Hat Insights 2020-10 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

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。 フィードバックの提供: 本書の改善に関するご意見がある場合や、エラーを発見された場合は、Bugzilla レポートを http://bugzilla.redhat.com まで送信してください。Cloud Software Services (cloud.redhat.com) 製品を選択し、Documentation コンポーネントを使用します。

目次

第1章 コンプライアンスサービスのレポートおよび評価

Red Hat Insights Compliance サービスを利用すると、Red Hat Enterprise Linux (RHEL) システムの SCAP セキュリティポリシーへのコンプライアンスを評価し、監視することができます。

Compliance サービスは、シンプルながらも強力なユーザーインターフェースを提供し、SCAP セキュリティポリシーの作成、設定、管理を可能にします。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、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。

このドキュメントでは、管理者が Compliance サービスのレポートを理解し、問題を管理して、Compliance サービスから修正を得られるように、Compliance 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、コンプライアンスステータスと通信するためにステークホルダーとレポートを共有できます。

関連資料

- **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**
- **コンプライアンスレポートの生成**

1.1. 要件および前提条件

Compliance サービスは、Red Hat Insights の一部で、Red Hat Enterprise Linux (RHEL) サブスクリプションに含まれています。現在 Red Hat がサポートしているすべてのバージョンの RHEL で使用することができます。Red Hat Insights およびコンプライアンスサービスを使用するには、追加の Red Hat サブスクリプションは必要ありません。

Compliance サービスを使用する前に、以下の条件が満たされていることを確認します。

- **Insights クライアントをインストールして登録します。**RHEL システムに Insights クライアントがインストールされておらず、稼働していない場合は、『Red Hat Insights のスタートガイド』に従って、監視する各システムにクライアントをインストールし、登録してください。
- **OpenSCAP の設定**OpenSCAP は、SCAP セキュリティーガイド (SSG) とデータストリームで組織用に設定され、コンプライアンスサービスにデータを報告できます。その後、Compliance サービスを使用してポリシーを追加および変更できます。OpenSCAP に慣れていない場合は、「OpenSCAP スタートガイド」を参照してください。

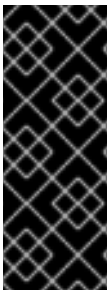
1.2. サポートされる設定

RHEL のマイナーバージョンで対応している SCAP Security Guide (SSG) のバージョンを使用します。

正確なレポートを生成するには、システムにインストールされている **RHEL マイナーバージョン** の正しい Red Hat サポートバージョンの SCAP Security Guide (SSG) を使用する必要があります。RHEL に関連するマイナーリリースまたは RHEL に関連するバッチ更新で提供されるバージョンが、SCAP セキュリティーガイドで正式にサポートされています。ポリシーに、サポートされていない SSG バージョンがインストールされているシステムが 1 つ以上含まれている場合は、影響を受けるシステムの数の前に、**unsupported** (サポートなし) 通知が コンプライアンスサービス > レポート に表示されます。

サポートされていないバージョンの SSG がインストールされているシステムで、失敗したルールが引き続き表示される可能性があります。ただし、コンプライアンスレポートの目的で、結果が正確でないと考慮されることがあります。以下の条件は、サポート対象外の設定の結果に適用されます。

- これらの結果は、Red Hat でサポートされるバージョン以外の SSG バージョンを使用すると結果の精度が落ちるため、ベスト推測となります。
- サポートされていないバージョンの SSG を持つシステムからの結果は、ポリシーに関する全体的なコンプライアンスアセスメントに含まれません。
- サポートされていないバージョンの SSG がインストールされているシステムのルールは、修正できません。



重要

以下の表は、RHEL の各マイナーバージョンでサポートされる SSG バージョンの一覧です。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。

表1.1 RHEL の SCAP セキュリティーガイドで対応しているバージョン

Red Hat Enterprise Linux のバージョン	SCAP セキュリティーガイドのバージョン
RHEL 6.6	scap-security-guide-0.1.18-3.el6
RHEL 6.9	scap-security-guide-0.1.28-3.el6
RHEL 6.10	scap-security-guide-0.1.28-4.el6
RHEL 7.2 AUS	scap-security-guide-0.1.25-3.el7
RHEL 7.3 AUS	scap-security-guide-0.1.30-5.el7_3
RHEL 7.4 AUS, E4S	scap-security-guide-0.1.33-6.el7_4
RHEL 7.5 (バッチ更新)	scap-security-guide-0.1.36-10.el7_5
RHEL 7.6 EUS	scap-security-guide-0.1.40-13.el7_6
RHEL 7.7 EUS	scap-security-guide-0.1.43-13.el7
RHEL 7.8 (バッチ更新)	scap-security-guide-0.1.46-11.el7
RHEL 7.9	scap-security-guide-0.1.49-13.el7 scap-security-guide-0.1.52-2.el7_9
RHEL 8.0 SAP	scap-security-guide-0.1.42-11.el8

Red Hat Enterprise Linux のバージョン	SCAP セキュリティーガイドのバージョン
RHEL 8.1 EUS	scap-security-guide-0.1.46-1.el8 scap-security-guide-0.1.47-8.el8_1
RHEL 8.2 (バッチ更新)	scap-security-guide-0.1.48-7.el8
RHEL 8.3	scap-security-guide-0.1.50-14.el8

1.3. ベストプラクティス

Red Hat では、最適なユーザーエクスペリエンスを得て、コンプライアンスサービスで最も正確な情報を受け取るためにも、いくつかのベストプラクティスに従うことを推奨しています。

RHEL システムが Insights クライアントに登録されていることを確認します。

Insights クライアントは、Compliance レポートを表示するシステムにインストールおよび登録されている必要があります。--register オプションを指定して insights-client コマンドを入力し、RHEL システムを Insights に登録します。

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

システムで使用されている RHEL OS マイナーバージョンが Insights クライアントで表示されていることを確認します。

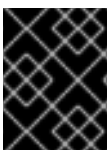
Insights クライアントでは、Red Hat Insights にアップロードしたデータペイロードから、RHEL OS のマイナーバージョンを含め、特定のデータを再編集できます。コンプライアンスサービスが RHEL OS のマイナーバージョンを表示できない場合は、対応している SCAP セキュリティーガイドのバージョンを検証できず、レポートが正確にならない可能性があります。

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

Compliance サービス内のセキュリティーポリシーの定義

2020 年 11 月時点では、Compliance サービス内で組織のセキュリティーポリシーを作成して定義する必要があります。外部で作成されたポリシーはサポートされなくなります。また、これらのポリシーの結果は、結果に含まれなくなります。

Compliance サービス内でポリシーを作成すると、最も機能に富んだユーザーエクスペリエンスと信頼できるレポートを取得できます。複数のシステムをポリシーに関連付けます。RHEL バージョンに Red Hat がサポートする SSG を使用するようにしてください。ポリシーに含まれるルールは、組織の特定の要件に基づいて編集します。

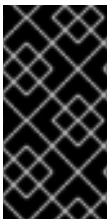


重要

Compliance サービスは、2020 年 11 月の後に、外部から取得したポリシーおよびアップロードしたポリシーをサポートしなくなります。

第2章 COMPLIANCE サービスにおける SCAP セキュリティーポリシーの管理

Compliance サービス内のみで 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、関連付けるルールやシステムを選択します。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 Red Hat Insights サービスとは異なり、Compliance 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 データをコンプライアンスサービス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。

2.1. 新しい SCAP ポリシーの作成

コンプライアンスサービスを使用するには、SCAP セキュリティーポリシーを、Insights で登録した RHEL システムに関連付ける必要があります。ポリシーは、RHEL 7 などの単一のメジャーリリースに対して定義されますが、複数のマイナーバージョンにまたがる可能性があります。RHEL サーバーが RHEL の複数のメジャーリリースにまたがる場合は、メジャーリリースごとにポリシーを 1 つ作成する必要があります。Compliance サービスユーザーは、コンプライアンスサービス内でポリシーを作成する必要があります。

Compliance サービスを使用して新しいポリシーを作成するには、次の手順を実行します。

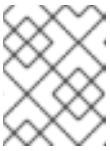
手順

1. コンプライアンスサービス > SCAP ポリシー ページに移動し、必要に応じてログインします。
2. 青の **Create new policy** ボタンをクリックし、**Create SCAP ポリシーウィザード**を開きます。
3. ウィザードの **Create SCAP policy** ページで、以下の選択を行います。
   a. 監視するシステム上の正しい RHEL **オペレーティングシステム** のバージョンを選択します。

注記

SCAP ポリシーは、RHEL バージョン固有のものです。たとえば、RHEL 7 を実行しているシステムや、RHEL 8 を実行しているシステムなど、DISA STIG ポリシータイプを使用する場合は、RHEL の各主要バージョンに対してポリシーを作成する必要があります。

   b. **ポリシータイプ**を選択します。



注記

プロファイルオプションは、以前の手順で選択した OS バージョンに対して、最新の利用可能な scap-scurity-guide で事前に決められています。

注記

ポリシーがすでにその RHEL バージョンで使用されている場合は、新しいシステムを追加することができます。

c. **Next** をクリックします。

4. **ポリシー詳細** ページで、各フィールドに事前に投入された情報を確認するか、必要に応じて変更します。

   a. 記述的な**ポリシー名**を指定します。

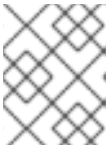
   b. **リファレンス ID** を変更することはできません。

   c. **説明** には OpenSCAP のポリシー記述が事前に設定されていますが、さらに詳細を追加できます。

   d. このポリシーに関連付けられたシステムの**コンプライアンスのしきい値**を指定します。100% のコンプライアンスが現実的ではない場合、ここでコンプライアンスの許容レベルを指定できます。

   e. **Next** をクリックします。

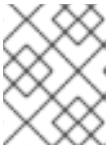
5. **ルール** ページで、ルールのリストを検索またはスクロールし、不要なルールをクリアして要件に合わせたポリシーを作成し、**Next** をクリックします。



注記

このとき、ルールセットを変更できるのは、ポリシーが作成されたときだけです。既存のポリシーでルールを変更することは、現在のところできません。

6. **System** ページで、このポリシーに関連付ける各システムの横にあるチェックボックスにチェックを入れてから、**Next** をクリックします。



注記

検索ボックスにシステム名を入力します。システムのサブセットを表示するには、ステータスまたはソースでフィルターします。

7. **Review** ページでポリシー情報が正しいことを確認てから、**Finish** をクリックします。

8. Compliance サービス > レポート ページで、ポリシーをクリックし、システムを含む詳細が正しいことを確認します。

2.2. 既存のポリシーの編集

次の手順を使用して、ポリシーの詳細、事業目的、コンプライアンスのしきい値、および含まれるシステムを変更するために、Compliance サービスの既存のポリシーを編集します。

注記

既存のポリシーを編集する機能は、進化し続けます。これには、既存のポリシーに含まれるルールを追加または削除できる機能を含め、新しい機能が追加されます。

手順

1. cloud.redhat.com にログインし、Compliance > SCAP Policy ページに移動します。
2. 検索またはフィルタリング機能を使用して、編集するポリシーを検索します。
3. ポリシー行の右端で、more-actions アイコンをクリックし、Edit policy を選択します。
4. Edit <Policy name> カードで、各タブをクリックして以下の情報を編集します。
    a. **Details** で、**Policy description**、**Business goal** および **Compliance のしきい値** を編集します。
    b. **ルール** の編集はまもなく実装されます。
    c. **System** タブで、ポリシーに追加するシステムを選択するか、検索およびフィルターを使用して、不要になったシステムを特定して消去します。
5. SCAP Policies ページに移動し、編集したポリシーを見つけます。
6. ポリシーをクリックし、詳細と含まれるシステムが、編集した内容と一致していることを確認します。

第3章 COMPLIANCE サービスのレポートについて

Compliance サービスは、各システムで利用可能な最新の OpenSCAP 結果を表示します。Red Hat Insights コンプライアンス > レポート の各ポリシーについての概要を確認します。

システムごとのコンプライアンスステータスをさらに理解し、多くのシステム報告データの「ノイズ」を減らすために、データをフィルタリングして並べ替えて、どのルールが渡され、失敗したかを確認できます。

以下のセクションでは、Compliance サービスの場所に応じてデータを改良し、最も重要な問題にフォーカスする方法を説明します。

3.1. SCAP ポリシー

Search 機能を使用して、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**名前および重大度を指定して、特定の SSG バージョンに含まれるルールを表示して絞り込み、ルール名、重大度、または Ansible Playbook のサポート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、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。

3.2. 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。
- 以下で小規模なグループにシステムを分割します。
  - **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で検索して、RHEL 7 または RHEL 8 システムのみを表示します。

3.3. 検索

Compliance サービスの検索機能は、表示している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 RHEL オペレーティングシステム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。

3.4. フィルタリング

フィルタリングは、コンプライアンスサービスの複数のビューから利用できます。また、フィルターオプションはページビューに固有のものです。Filters アイコンは検索フィールドの左側にあります。下矢印をクリックして、フィルターを設定するボックスにチェックを入れます。

- **システムリスト**名前、ステータス、およびソースでフィルターします。
- **単一システムルールリスト**渡された、または渡されていないルール、またはルールの重大度によるルールにフィルターをかけます。

3.5. データのソート

ポリシーの Compliance サービス System と Rule リストの列を並び替えて、結果を順序付けることができます。以下のコラムは、各リストでソートできます。

- **コンプライアンスサービスシステムの一覧**
  - システム名 (アルファベット)
  - ポリシー名 (アルファベット)
  - コンプライアンススコア (システムに渡されるルールの影響)
  - 最終スキャン (最後のスキャンから経過した時間)
- **ポリシーのルールリスト**
  - ルール名 (アルファベット)
  - 重大度 (低、中、高、重大)
  - Ansible サポート (Playbook が利用可能か否か)

第4章 参考資料

Compliance サービスの詳細は、以下のリソース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**
- **コンプライアンスレポートの生成**
- Red Hat Insights Documentation
- Red Hat Insights Product Support ページ