Red Hat Insights 2022

コンプライアンスサービスレポートの生成

RHEL インフラストラクチャーのコンプライアンスステータスをセキュリティーステークホルダーに通信

Last Updated: 2022-06-20

Red Hat Insights 2022 コンプライアンスサービスレポートの生成

RHEL インフラストラクチャーのコンプライアンスステータスをセキュリティーステークホルダーに通信

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

さまざまなレポートを生成して、RHEL 環境の security-policy コンプライアンスステータスを企業セキュリティー監査サーバーと通信します。

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、弊社の CTO、Chris Wright のメッセージ を参照してください。

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 COMPLIANCE サービスレポート用の INSIGHTS の概要

Compliance サービスを使用すると、エクスポート時に設定されているフィルターをもとに詳細なデータをエクスポートできます。コンプライアンスレポートをエクスポートするには、以下の操作が必要です。

- 現在の OpenSCAP 結果のアップロード
- Complaince サービスでのビューのフィルタリング
- CSV または JSON ファイルへのエクスポートとダウンロードの保存

第2章 システムの現在の OPENSCAP データのアップロード

Compliance サービスは、OpenSCAP スキャンからデータを表示します。コンプライアンスサービスを使用してシステムコンプライアンスのステータスを表示したり、問題を修正したり、結果を報告したりしている場合でも、その他の手順を続行する**前**に OpenSCAP から最新のシステムデータをアップロードして現在のデータが表示されることを確認してください。

手順

1. 以下のコマンドを実行し、OpenSCAP から現在のデータをアップロードします。

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

第3章 選択したシステムのコンプライアンスレポートのエクスポート

以下の手順に従って、システムに影響する CVE を示し、エクスポート時のフィルタリングに基づくコンプライアンスレポートをエクスポートします。

3.1. 単一ポリシーのレポートのエクスポート

1 つのポリシーに関するコンプライアンスレポートをエクスポートするには、以下の手順を実行します。

手順

1. 必要に応じて、Red Hat Enterprise Linux > Compliance > Reports タブに移動してログインします。
2. ポリシーをクリックしてレポートを表示します。
3. 必要に応じてフィルターを適用して結果を絞り込みます。
4. コンプライアンスのしきい値やビジネス目標などの詳細情報を表示するには、**View policy** をクリックします。
5. システム一覧の上部で、Remediate ボタンの右側にあるダウンロードアイコンをクリックし、エクスポート設定に基づいて **Export to CSV** または **Export to JSON** を選択します。
6. ファイルを開くか、ファイルを保存します。**OK** をクリックします。

3.2. 選択したシステムのレポートのエクスポート

選択したシステムのコンプライアンスレポートをエクスポートするには、以下の手順を実行します。

手順

1. 必要に応じて、Red Hat Enterprise Linux > Compliance > Systems に移動してログインします。
2. 必要に応じてフィルターを適用して結果を絞り込みます。
3. 各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て、レポートに表示するシステムを選択します。
4. システム一覧の上部で、ダウンロードアイコンをクリックし、エクスポート設定に基づいて **Export to CSV** または **Export to JSON** を選択します。
5. ファイルを開くか、ファイルを保存します。**OK** をクリックします。

第4章 ポリシーレポート

Insights for RHEL コンプライアンスサービスを使用すると、個々のポリシーの PDF レポートを作成して、コンプライアンスチームや監査人などの利害関係者と共有できます。

レポートには次の情報が含まれます。

- ポリシーの詳細: ポリシーの種類、運用システム、コンプライアンスのしきい値、およびビジネス目標。
- ポリシーに準拠しているシステムの割合。
- 非準拠および準拠システムの数。
- 非準拠のシステム情報。レポートの作成時に準拠システムを含めるように選択できます。
- 失敗したルールのトップ 10 のリスト: 最も重大な失敗したルールと、各ルールの失敗したシステムの最大数が上位にランク付けされます。

4.1. ポリシーの PDF レポートの作成

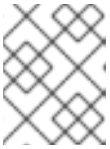
セキュリティーポリシーの PDF レポートをダウンロードするには、次の手順を実行します。

前提条件

- Red Hat Hybrid Cloud コンソールにログインしている 必要があります。
- ポリシーレポートは、ポイントインタイムレポートです。Red Hat は、コンプライアンスサービスでポリシーレポートを作成する前に、最新のシステムデータを Insights for RHEL にアップロードすることをお勧めします。

手順

1. 任意で、システムで **insights-client --compliance** を実行してスキャンし、現在のデータをコンプライアンスサービスにアップロードします。
2. Red Hat Enterprise Linux > Compliance > Reports に移動します。
3. レポートを作成するポリシーを見つけます。
4. ポリシー名と同じ行の右端にあるダウンロードアイコン をクリックします。



注記

ポリシー名をクリックして、ページの右上にある **Download PDF** をクリックすることもできます。

5. **コンプライアンスレポート** モーダルダイアログで、含めるシステムデータを選択します。
6. 含めるルールデータを選択します。
7. 必要に応じて、ユーザーメモを追加します。
8. **Export report** をクリックします。

第5章 通知およびインテグレーションの有効化

Red Hat Hybrid Cloud Console の通知サービスを有効にして、コンプライアンスポリシーがトリガーされるたびに通知を送信できます。たとえば、コンプライアンスポリシーが特定のしきい値を下回るたびにメールメッセージを自動送信する、または毎日発生するすべてのコンプライアンスポリシーイベントのメールダイジェストを送信するように通知サービスを設定できます。通知サービスを使用すると、コンプライアンスイベントによりトリガーされる通知を把握するために Red Hat Insights for RHEL のダッシュボードを繰り返し確認する必要がなくなります。

通知サービスを有効にするには、以下の 3 つの主要なステップが必要です。

- まず、組織管理者は通知管理者ロールを持つユーザーアクセスグループを作成し、そのグループにアカウントメンバーを追加します。
- 次に、通知管理者は通知サービス内のイベントの動作グループを設定します。動作グループは、通知ごとに配信方法を指定します。たとえば、動作グループは、メール通知をすべてのユーザーに送信するか、組織の管理者のみ送信するかを指定できます。
- 最後に、イベントごと個別メールを受信する、またはすべてのコンプライアンスイベントの日次ダイジェストを受信するユーザーは、各イベントの個別メールを受け取るようにユーザー設定する必要があります。

メールメッセージの送信に加え、他の方法でイベントデータを送信するように通知サービスを設定できます。

- 認証済みクライアントを使用して Red Hat Insights API にイベントデータをクエリーする
- Webhook を使用して受信要求を受け入れるサードパーティーのアプリケーションにイベントを送信する
- Splunk などのアプリケーションと通知を統合してコンプライアンスイベントをアプリケーションダッシュボードにルーティングする

関連情報

- コンプライアンスイベントの通知を設定する方法の詳細については、Configuring notifications and integrations on the Red Hat Hybrid Cloud Console を参照してください。

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。

- **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**
- **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**
- 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