Red Hat Insights 1-latest

FedRAMP に準拠した Compliance 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連絡する

Last Updated: 2024-03-27

Red Hat Insights 1-latest FedRAMP に準拠した Compliance 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連絡する

法律上の通知

概要

FedRAMP® に準拠した形で、さまざまなレポートを生成し、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者に通知します。 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 COMPLIANCE サービスレポートの概要

Compliance サービスを使用すると、ダウンロード時に設定されているフィルターをもとにデータをダウンロードできます。コンプライアンスレポートをダウンロードするには、次の操作が必要です。

- Red Hat Insights for Red Hat Enterprise Linux への現在のシステムデータのアップロード
- Compliance サービス Web コンソールでの結果のフィルタリング
- レポートのダウンロード (コンマ区切り値 (CSV) または JavaScript Object Notation (JSON) データをエクスポートするか、PDF としてエクスポート)

第2章 INSIGHTS への現在のシステムデータのアップロード

Compliance サービスを使用して、システムのコンプライアンスステータスの表示、問題の修正、関係者へのステータスの報告を行う場合は、システムから現在のデータをアップロードして、最新の情報を確認します。

手順

- 各システムで次のコマンドを実行して、現在のデータを Insights for Red Hat Enterprise Linux にアップロードします。
  [root@server ~]# insights-client --compliance

第3章 重大度に基づくシステムのフィルタリング

失敗したルールの重大度に基づいて、レポート内のすべてのシステムをフィルタリングできます。これにより、システムに優先順位を付け、最も重大な問題を最初に修復できます。

前提条件

- Red Hat Hybrid Cloud Console へのログインアクセス。

手順

- Security > Compliance > Reports に移動します。
- 表示する **Policy** ルールを選択します。
- システムのリストの上にある **Name** フィルターをクリックします。
- **Failed rule severity** を選択します。
- **Failed rule severity** の右側にある **Filter by failed rule** をクリックし、**High** の左側にあるボックスをオンにします。表示されたシステムは、重大問題と見なされたもので、最初に修正する必要があります。

第4章 選択したシステムのコンプライアンスデータのエクスポート

エクスポート時のフィルタリングに基づいて、システムに影響を与えるコンプライアンスの問題を示すレポートをエクスポートするには、次の手順を実行します。

4.1. 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. Security > Compliance > Reports タブに移動し、必要に応じてログインします。
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. システムリストの上部で、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。

4.2. 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. Security > Compliance > Systems に移動し、必要に応じてログインします。
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. システムリストの上部で、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5章 PDF ポリシーレポートのダウンロード

Insights for Red Hat Enterprise Linux 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。

5.1. 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 Red Hat Enterprise Linux にアップロードすることを推奨します。

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. Security > 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6章 コンプライアンスレポートの削除

前提条件

- Red Hat Hybrid Cloud Console へのログインアクセス。

手順

1. Red Hat Insights > コンプライアンス > レポートに移動します。使用可能なレポートのリストが表示されます。
2. **オプション:**検索フィルターを使用して、削除するレポートを検索します。レポートは、ポリシー名、ポリシータイプ、オペレーティングシステム、または準拠しているシステムによってフィルター処理できます。
3. 削除するレポートの名前をクリックします。システムのリストが含まれるレポートが表示されます。
4. レポートの右上にある **Delete report** をクリックします。レポートの削除ダイアログボックスが表示され、**Deleting a report is permanent and cannot be undone.** というメッセージが表示されます。
5. **Delete report** ボタンをクリックして、レポートを削除することを確認します。

第7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、または各日に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、組織管理者が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、通知管理者が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、電子メール通知をすべてのユーザーに送信するか、組織の管理者に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。

関連情報

- コンプライアンスイベントの通知をセットアップする方法の詳細は、**Red Hat Hybrid Cloud Console での通知の設定** を参照してください。

第8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モニタリング**
- 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。