Red Hat Satellite 6.15

セキュリティーコンプライアンスの管理

SCAP コンプライアンスポリシーを計画および設定し、ポリシーをホストにデプロイメントし、ホストのコンプライアンスを監視する

Last Updated: 2024-04-24

Red Hat Satellite 6.15 セキュリティーコンプライアンスの管理

SCAP コンプライアンスポリシーを計画および設定し、ポリシーをホストにデプロイメントし、ホストのコンプライアンスを監視する

Red Hat Satellite Documentation Team
satellite-doc-list@redhat.com

法律上の通知

概要

Satellite を使用すると、セキュリティーコンプライアンスポリシーを作成してホストにデプロイし、そのポリシーを使用してホストのコンプライアンスを監視して、ホストをセキュリティー標準に準拠させることができます。

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。この取り組みは膨大な作業を要するため、これらの変更による更新は可能な範囲で段階的に行われます。詳細は、Red Hat CTO である Chris Wright のメッセージ をご覧ください。

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに対するご意見をお聞かせください。ドキュメントの改善点があればお知らせください。

Bugzilla でチケットを作成することでフィードバックを送信できます。

1. Bugzilla のWeb サイトに移動します。
2. **Component** フィールドで、**Documentation** を使用します。
3. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも追加してください。
4. **Submit Bug** をクリックします。

第1章 セキュリティーコンプライアンス管理

セキュリティーコンプライアンス管理は、セキュリティーポリシーを定義し、それらのポリシーに準拠しているかどうかシステムを監査し、非準拠のインスタンスを解決する継続的なプロセスです。コンプライアンス違反は、組織の設定管理ポリシーに基づいて管理されます。セキュリティーポリシーは、ホスト固有のものから業界共通のものまでに及ぶため、ポリシー定義には柔軟性が必要になります。

Satellite を使用すると、登録されているすべてのホストに対するコンプライアンスの監査とレポートをスケジュールできます。

第2章 セキュリティーコンテンツ自動化プロトコル

Satellite は、Security Content Automation Protocol (SCAP) 標準を使用してセキュリティーポリシーを定義します。

SCAP は、XML ベースのいくつかの仕様 (Extensible Checklist Configuration description Format (XCCDF) で説明されているチェックリストや、Open Vulnerability and Assessment Language (OVAL) で説明されている脆弱性など) のフレームワークです。これらの仕様は、**データストリーム** ファイルとしてカプセル化されます。

XCCDF のチェックリスト項目 (**ルール** とも呼ばれます) は、システム項目の必要な設定を表します。たとえば、ルールによって、どのユーザーも **root** ユーザーアカウントを使用して SSH 経由でホストにログインできないように指定できます。ルールは 1 つ以上の **XCCDF プロファイル** にグループ化できます。これにより、複数のプロファイルでルールを共有できます。

OpenSCAP スキャナーツールは、ホスト上のシステム項目をルールに照らして評価し、Asset Reporting Format (ARF) でレポートを生成します。このレポートは、モニタリングと分析のために Satellite に返されます。

表2.1 OpenSCAP スキャナがサポートする SCAP フレームワーク 1.3 の仕様

タイトル	説明	バージョン
SCAP	Security Content Automation Protocol	1.3
XCCDF	Extensible Configuration Checklist Description Format	1.2
OVAL	Open Vulnerability and Assessment Language	5.11
-	Asset Identification	1.1
ARF	Asset Reporting Format	1.1
CCE	Common Configuration Enumeration	5.0
CPE	Common Platform Enumeration	2.3
CVE	Common Vulnerabilities and Exposures	2.0
CVSS	Common Vulnerability Scoring System	2.0

関連情報

- SCAP の詳細は、OpenSCAP プロジェクト を参照してください。

第3章 SATELLITE の SCAP コンテンツ

SCAP コンテンツは、コンプライアンス、設定、またはセキュリティーベースラインの実装を含む SCAP データストリームファイルです。通常、単一のデータストリームには複数の XCCDF プロファイルが含まれます。XCCDF プロファイルは、General Purpose Operating Systems (OSPP)、Health Insurance Portability and Accountability Act (HIPAA)、PCI-DSS v3.2.1 Control Baseline for Red Hat Enterprise Linux 9 など、Satellite のホスト設定のコンプライアンスを評価するための業界標準またはカスタムのセキュリティー標準を定義したものです。**テーラリングファイル** を使用すると、要件に応じて既存の XCCDF プロファイルを調整できます。

Satellite では、SCAP コンテンツからの XCCDF プロファイルを使用し、最終的にはテーラリングファイルを使用して、**コンプライアンスポリシー** を定義します。Satellite には、OpenSCAP プロジェクトによって提供される SCAP セキュリティーガイドのデフォルトの SCAP コンテンツが含まれています。

独自のコンテンツをダウンロード、デプロイ、変更、作成する方法の詳細は、以下を参照してください。

- **Red Hat Enterprise Linux 9 セキュリティーの強化**
- **Red Hat Enterprise Linux 8 セキュリティーの強化**
- **Red Hat Enterprise Linux 7 セキュリティーガイド**
- **Red Hat Enterprise Linux 6 セキュリティーガイド**

3.1. サポートされている SCAP バージョン

Satellite は、SCAP バージョン 1.2 および 1.3 のコンテンツをサポートします。

第4章 コンプライアンスポリシーのデプロイメントオプション

次のいずれかの方法を使用して、コンプライアンスポリシーをデプロイできます。

Ansible デプロイメント

Ansible ロールを使用して、コンプライアンススキャン用にホストを設定します。

Puppet デプロイメント

Puppet クラスと Puppet エージェントを使用して、コンプライアンススキャン用にホストを設定します。

手動デプロイメント

コンプライアンススキャン用にホストを手動で設定します。

第5章 コンプライアンスポリシーのデプロイメント方法の設定

次の手順のいずれかを使用して、コンプライアンスポリシーをデプロイするために選択した方法に合わせて Satellite を設定します。後で コンプライアンスポリシーを作成 するときに、これらの方法のいずれかを選択します。

Ansible デプロイメントの手順

1. **theforeman.foreman_scap_client** Ansible ロールをインポートします。
   詳細は、**Ansible 統合を使用した設定の管理** を参照してください。

2. 作成したポリシーと **theforeman.foreman_scap_client** Ansible ロールをホストまたはホストグループに割り当てます。

3. デプロイメントをトリガーするには、ホストまたはホストグループで Ansible ロールを手動で実行するか、定期的なポリシー更新のリモート実行を使用して定期的なジョブを設定します。
   詳細は、**ホストの管理** の リモートジョブの設定とセットアップを 参照してください。

Puppet デプロイメントの手順

1. Puppet が有効になっていることを確認します。

2. Puppet エージェントがホストにインストールされていることを確認します。

3. **foreman_scap_client** Puppet モジュールを含む Puppet 環境をインポートします。
   詳細は、**Puppet 統合を使用した設定の管理** を参照してください。

4. 作成したポリシーと **foreman_scap_client** Puppet クラスをホストまたはホストグループに割り当てます。
   Puppet は次回の定期実行時にデプロイメントをトリガーします。または、Puppet を手動で実行することもできます。Puppet はデフォルトで 30 分ごとに実行します。

手動デプロイメントの手順

- 手動デプロイメント方法の場合、追加の Satellite 設定は必要ありません。
  手動デプロイメントの詳細は、**Red Hat ナレッジベース** の How to set up OpenSCAP Policies using Manual Deployment option を参照してください。

第6章 利用可能な SCAP コンテンツのリスト表示

Satellite にすでにロードされている SCAP コンテンツを表示するには、この手順を使用してください。Satellite Web UI の代わりに CLI を使用するには、CLI 手順 を参照してください。

前提条件

- ユーザーアカウントに **view_scap_contents** 権限を持つロールが割り当てられている。

手順

- Satellite Web UI で、**Hosts** > **Compliance** > **SCAP contents** に移動します。

CLI 手順

- Satellite Server で次の Hammer コマンドを実行します。

```
# hammer scap-content list \
--location "My_Location" \
--organization "My_Organization"
```

第7章 SCAP コンテンツの設定

SCAP データストリームとテーラリングファイルをアップロードして、コンプライアンスポリシーを定義できます。

7.1. デフォルトの SCAP コンテンツの読み込み

デフォルト SCAP コンテンツを Satellite Server にロードすると、SCAP セキュリティーガイド (SSG) からのデータストリームがロードされ、すべての組織と場所に割り当てられるようになります。

SSG は、Satellite Server のオペレーティングシステムによって提供され、**/usr/share/xml/scap/ssg/content/** にインストールされます。利用可能なデータストリームは、Satellite が実行されているオペレーティングシステムのバージョンによって異なることに注意してください。この SCAP コンテンツは、Satellite Server と同じ RHEL マイナーバージョン持つホストをスキャンする場合にのみ使用できます。詳細は、「RHEL でサポートされている SCAP コンテンツの取得」 を参照してください。

前提条件

- ユーザーアカウントに **create_scap_contents** 権限を持つロールが割り当てられている。

手順

- Satellite Server で次の Hammer コマンドを使用します。

```
# hammer scap-content bulk-upload --type default
```

7.2. RHEL でサポートされている SCAP コンテンツの取得

Red Hat Enterprise Linux の最新の SCAP セキュリティーガイド (SSG) は Red Hat カスタマーポータルで入手できます。ホストの RHEL マイナーバージョン用に指定された SSG バージョンを取得する必要があります。

手順

1. パッケージブラウザーの SCAP セキュリティーガイド にアクセスします。
2. **バージョン** メニューから、ホストが実行している RHEL マイナーバージョン向けの最新の SSG バージョンを選択します。たとえば、RHEL 8.6 の場合は、***.el8_6** という名前のバージョンを選択します。
3. パッケージ RPM をダウンロードします。
4. RPM からデータストリームファイル (***-ds.xml**) を展開します。以下に例を示します。

```
$ rpm2cpio scap-security-guide-0.1.69-3.el8_6.noarch.rpm \
| cpio -iv --to-stdout ./usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml \
> ssg-rhel-8.6-ds.xml
```

5. データストリームを Satellite にアップロードします。詳細は、「追加の SCAP コンテンツのアップロード」 を参照してください。

関連情報

- **Red Hat ナレッジベース** の Supported versions of the SCAP Security Guide in RHEL
- **Red Hat Enterprise Linux 9 セキュリティーの強化**の RHEL 9 で対応する SCAP セキュリティーガイドプロファイル
- **Red Hat Enterprise Linux 8 セキュリティーの強化**の RHEL 8 で対応している SCAP セキュリティーガイドプロファイル
- **Red Hat Enterprise Linux 7 セキュリティーガイド** の RHEL 7 で対応する SCAP セキュリティーガイドプロファイル

7.3. 追加の SCAP コンテンツのアップロード

追加の SCAP コンテンツ (自分で作成したコンテンツ、または他の場所で取得したコンテンツ) を Satellite Server にアップロードできます。Red Hat は、Red Hat から取得した SCAP コンテンツのサポートのみを提供することに注意してください。Satellite Web UI の代わりに CLI を使用する場合は、CLI 手順 を参照してください。

前提条件

- ユーザーアカウントに **create_scap_contents** 権限を持つロールが割り当てられている。
- SCAP データストリームファイルを取得している。

手順

1. Satellite Web UI で、**Hosts** > **Compliance** > **SCAP contents** に移動します。
2. **Upload New SCAP Content** をクリックします。
3. **Title** テキストボックスにタイトルを入力します (**My SCAP Content** など)。
4. **Scap File** で、**Choose file** をクリックし、SCAP データストリームファイルが含まれる場所に移動して、**Open** をクリックします。
5. **Locations** タブで場所を選択します。
6. **Organizations** タブで組織を選択します。
7. **Submit** をクリックします。

SCAP コンテンツファイルが正常にロードされると、**Successfully created My SCAP Content** のようなメッセージが表示されます。

CLI 手順

1. SCAP データストリームファイルを Satellite Server 上のディレクトリー (**/usr/share/xml/scap/my_content/** など) に配置します。
2. Satellite Server で次の Hammer コマンドを実行します。

```
# hammer scap-content bulk-upload --type directory \
--directory /usr/share/xml/scap/my_content/ \
--location "My_Location" \
--organization "My_Organization"
```

検証

- 利用可能な SCAP コンテンツをリストします。SCAP コンテンツのリストに新しいタイトルが含まれています。

7.4. XCCDF プロファイルのカスタマイズ

元の SCAP コンテンツを編集せずに、**テーラリングファイル** を使用して既存の XCCDF プロファイルをカスタマイズできます。1 つのテーラリングファイルに複数の XCCDF プロファイルのカスタマイズを含めることができます。

テーラリングファイルは SCAP Workbench ツールを使用して作成できます。SCAP ワークベンチツールの使用方法の詳細は、Customizing SCAP Security Guide for your use case を参照してください。

作成したら、テーラリングファイルをコンプライアンスポリシーに割り当てて、ポリシー内の XCCDF プロファイルをカスタマイズできます。

7.5. 調整ファイルのアップロード

テーラリングファイルをアップロードすると、それをコンプライアンスポリシーに適用して、XCCDF プロファイルをカスタマイズできます。

前提条件

- ユーザーアカウントに **create_tailoring_files** 権限を持つロールが割り当てられている。

手順

1. Satellite Web UI で、**ホスト** > **コンプライアンス** > **テーラリングファイル** に移動し、**新規テーラリングファイル** をクリックします。
2. **Name** テキストボックスに、名前を入力します。
3. **Choose File** をクリックし、テーラリングファイルが含まれる場所に移動して、**Open** を選択します。
4. **Submit** をクリックして、選択したテーラリングファイルをアップロードします。

第8章 コンプライアンスポリシーの管理

コンプライアンスポリシー は、SCAP コンテンツの特定の XCCDF プロファイルに対して、指定されたホストのコンプライアンスをチェックする定期的な監査です。

Satellite Server 上でスキャンのスケジュールを指定すると、ホスト上でスキャンが実行されます。スキャンが完了すると、ARF 形式のレポートが生成され、Satellite Server にアップロードされます。コンプライアンスポリシーがスキャンされたホストに変更を加えることはありません。

コンプライアンスポリシーは、SCAP クライアント設定と cron スケジュールを定義します。ポリシーは、ポリシーが割り当てられているホスト上に SCAP クライアントとともにデプロイされます。

8.1. コンプライアンスポリシーの作成

コンプライアンスポリシーを作成することで、セキュリティーコンプライアンス要件を定義および計画し、ホストがセキュリティーポリシーに準拠した状態を維持できます。

前提条件

- 選択した コンプライアンスポリシーのデプロイメント方法 に合わせて Satellite を設定している。
- Satellite で、SCAP コンテンツ、最終的にはテーラリングファイルが利用可能である。
  - 利用可能な SCAP コンテンツを確認するには、*6章 利用可能な SCAP コンテンツのリスト表示* を参照してください。
  - SCAP コンテンツとテーラリングファイルをアップロードするには、*7章SCAP コンテンツの設定* を参照してください。
- ユーザーアカウントに **view_policies** および **create_policies** 権限を持つロールが割り当てられている。

手順

1. Satellite Web UI で、**ホスト** > **コンプライアンス** > **ポリシー** に移動します。
2. **New Policy** または **New Compliance Policy** をクリックします。
3. デプロイメント方法を **Ansible**、**Puppet**、または **Manual** から選択します。**Next** をクリックします。
4. ポリシーの名前、説明 (省略可能) を入力してから **次へ** をクリックします。
5. 適用する **SCAP Content** および **XCCDF Profile** を選択し、**Next** をクリックします。
   Satellite は、選択された XCCDF プロファイルにルールが含まれているかどうかを検出しないことに注意してください。**Default XCCDF Profile** などの空の XCCDF プロファイルは、空のレポートを返します。
6. オプション: XCCDF プロファイルをカスタマイズするには、**Tailoring File** と **XCCDF Profile in Tailoring File** を選択し、**Next** をクリックします。
7. ポリシーを適用するスケジュール時刻を指定します。**Period** のリストから、**Weekly**、**Monthly**、または **Custom** を選択します。**Custom** オプションを使用すると、ポリシーのスケジュールをより柔軟に行うことができます。

- **Weekly** を選択したら **Weekday** リストから曜日を選択します。
- **Monthly** を選択したら **Day of month** フィールドで日付を指定します。
- **Custom** を選択したら **Cron line** フィールドに有効な Cron 式を入力します。

8. ポリシーを適用する場所を選択し、**Next** をクリックします。
9. ポリシーを適用する組織を選択し、**Next** をクリックします。
10. オプション: ポリシーを割り当てるホストグループを選択します。
11. **Submit** をクリックします。

8.2. コンプライアンスポリシーの表示

特定の OpenSCAP コンテンツおよびプロファイルの組み合わせ別に適用されるルールをプレビューできます。これは、ポリシーを計画するときに役立ちます。

前提条件

- ユーザーアカウントに **view_policies** 権限を持つロールが割り当てられている。

手順

1. Satellite Web UI で、**ホスト** > **コンプライアンス** > **ポリシー** に移動します。
2. 必要なポリシーの **Actions** 列で、**Show Guide** をクリックするか、リストから Show Guide を選択します。

8.3. コンプライアンスポリシーの編集

Satellite Web UI では、コンプライアンスポリシーを編集できます。

Puppet エージェントが、次回の実行時に、編集されたポリシーをホストに適用します。これはデフォルトで 30 分ごとに実行されます。Ansible を使用する場合は、Ansible ロールを手動で再度実行するか、ホスト上で Ansible ロールを実行する定期的なリモート実行ジョブを設定する必要があります。

前提条件

- ユーザーアカウントに **view_policies** および **edit_policies** 権限を持つロールが割り当てられている。

手順

1. Satellite Web UI で、**ホスト** > **コンプライアンス** > **ポリシー** に移動します。
2. 必要なポリシーの名前をクリックします。
3. 必要な属性を編集します。
4. **Submit** をクリックします。

8.4. コンプライアンスポリシーの削除

Satellite Web UI では、既存のコンプライアンスポリシーを削除できます。

前提条件

- ユーザーアカウントに **view_policies** および **destroy_policies** 権限を持つロールが割り当てられている。

手順

1. Satellite Web UI で、**ホスト** > **コンプライアンス** > **ポリシー** に移動します。
2. 必要なポリシーの **Actions** 列で、リストから **Delete** を選択します。
3. 確認メッセージで **OK** をクリックします。

第9章 コンプライアンスポリシーの導入

コンプライアンスポリシーをデプロイするには、SCAP クライアントをインストールし、cron スケジュールファイルを更新して、ポリシーで選択されている SCAP コンテンツをホストにアップロードする必要があります。

9.1. リモート SCAP リソースの組み込み

SCAP データストリームは、OVAL ファイルなどのリモートリソースを参照できます。これは、SCAP クライアントがホスト上で実行する際にインターネット上で取得するものです。データストリームにリモートリソースが必要な場合は、以下のような Satellite Server の OpenSCAP Scanner ツールから以下のような警告が表示されます。

```
# oscap info /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml | grep "WARNING"
WARNING: Datastream component 'scap_org.open-scap_cref_security-data-oval-com.redhat.rhsa-
RHEL8.xml.bz2'
points out to the remote 'https://access.redhat.com/security/data/oval/com.redhat.rhsa-
RHEL8.xml.bz2'.
Use '--fetch-remote-resources' option to download it.
WARNING: Skipping 'https://access.redhat.com/security/data/oval/com.redhat.rhsa-RHEL8.xml.bz2'
file
which is referenced from datastream
```

デフォルトでは、SCAP クライアントはリモートリソースを無視し、リソースに依存する XCCDF ルールをスキップするように設定されています。スキップされたルールは **notchecked** ステータスになります。

インターネットにアクセスできるホストの場合、Satellite 内のホスト上のリモートリソースのダウンロードを有効にすることができます。インターネットにアクセスできないホストにリモート SCAP リソースを適用する方法については、以下を参照してください。「非接続環境でのリモート SCAP リソースの適用」。

Ansible デプロイメント方法の使用

次の Ansible 変数をオーバーライドします。

- 名前: **foreman_scap_client_fetch_remote_resources**
- 型: **boolean**
- 値: **true**

詳細は、**Ansible 統合を使用した設定の管理** の Satellite での Ansible 変数の上書き を参照してください。

Puppet デプロイメント方法の使用

以下の Puppet Smart Class パラメーターを設定します。

- 名前: **fetch_remote_resources**
- 型: **boolean**
- 値: **true**

詳細は、**Puppet 統合を使用した設定の管理** の Puppet スマートクラスパラメーターの設定を 参照してください。

9.2. 非接続環境でのリモート SCAP リソースの適用

SCAP データストリームには、OVAL ファイルなどのリモートリソースを含めることができます。これは、SCAP クライアントがホスト上で実行する際にインターネット上で取得できるものです。ホストがインターネットにアクセスできない場合は、カスタムファイルタイプリポジトリーからホスト上のファイル をダウンロードして、リモート SCAP リソースをダウンロードし、Satellite Server からホストにローカルファイルとして配布する必要があります。

前提条件

- リモート実行を有効にして、ホストを Satellite に登録しました。
- リモートリソースの取得が無効になっている (デフォルト)。詳細は、「リモート SCAP リソースの組み込み」 を参照してください。

手順

1. Satellite Server で、コンプライアンスポリシーで使用するデータストリームを調べて、ダウンロードする必要がある不足しているリソースを見つけます。

```
# oscap info /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml | grep "WARNING"
WARNING: Datastream component 'scap_org.open-scap_cref_security-data-oval-com.redhat.rhsa-RHEL8.xml.bz2'
points out to the remote 'https://access.redhat.com/security/data/oval/com.redhat.rhsa-RHEL8.xml.bz2'.
Use '--fetch-remote-resources' option to download it.
WARNING: Skipping 'https://access.redhat.com/security/data/oval/com.redhat.rhsa-RHEL8.xml.bz2' file
which is referenced from datastream
```

2. データストリームによって参照されるローカルファイルの名前を調べます。

```
# oscap info /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
...
  Referenced check files:
   ssg-rhel8-oval.xml
    system: http://oval.mitre.org/XMLSchema/oval-definitions-5
   ssg-rhel8-ocil.xml
    system: http://scap.nist.gov/schema/ocil/2
   security-data-oval-com.redhat.rhsa-RHEL8.xml.bz2
    system: http://oval.mitre.org/XMLSchema/oval-definitions-5
...
```

3. オンラインのマシンで、不足しているリソースをダウンロードします。

```
# curl -o security-data-oval-com.redhat.rhsa-RHEL8.xml.bz2
https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL8.xml.bz2
```

重要

ダウンロードしたファイルの名前が、データストリームによって参照される名前と一致していることを確認してください。

4. ファイルを新しいカスタムファイルタイプコンテンツとして Satellite Server に追加します。詳細は、**コンテンツの管理** の カスタムファイルタイプコンテンツの管理 を参照してください。**http://satellite.example.com/pulp/content/My_Organization_Label/Library/custom/My_Product_Label/My_Repo_Label/** など、リポジトリーが公開されている URL をメモします。

5. ホスト上の **root** のホームディレクトリーにファイルをアップロードするリモートジョブをスケジュールします。たとえば、**Run Command - Script Default** ジョブテンプレートを使用して、次のコマンドを入力します。

```
# curl -o /root/security-data-oval-com.redhat.rhsa-RHEL8.xml.bz2
http://satellite.example.com/pulp/content/My_Organization_Label/Library/custom/My_Product_Label/My_Repo_Label/security-data-oval-com.redhat.rhsa-RHEL8.xml.bz2
```

   リモートジョブの実行の詳細は、**ホストの管理** の リモートジョブの実行 を参照してください。

6. コンプライアンスポリシーのデプロイに進みます。

9.3. ANSIBLE を使用してホストグループにポリシーを展開する

Ansible を使用してホストグループにコンプライアンスポリシーをデプロイすると、Ansible ロールによって SCAP クライアントがインストールされ、選択したコンプライアンスポリシーに従ってホスト上で OpenSCAP スキャンが設定されます。

コンプライアンスポリシーの SCAP コンテンツでは、リモートリソースが必要になる場合があります。詳細は、「リモート SCAP リソースの組み込み」 を参照してください。

前提条件

- Capsule で OpenSCAP を有効にしている。詳細は、**Capsule Server のインストール** の Capsule Server での OpenSCAP の有効化 を参照してください。
- オペレーティングシステムリポジトリーを有効にして Satellite に同期し、ホスト上で有効にしている。
  - Red Hat Enterprise Linux 9 for x86_64 - BaseOS および Appstream (RPM) - **rhel-9-for-x86_64-baseos-rpms** および **rhel-9-for-x86_64-appstream-rpms**
  - Red Hat Enterprise Linux 8 for x86_64 - BaseOS および Appstream (RPM) - **rhel-8-for-x86_64-baseos-rpms** および **rhel-8-for-x86_64-appstream-rpms**
  - Red Hat Enterprise Linux 7 Server および Extras (RPM) - **rhel-7-server-rpms** および **rhel-7-server-extras-rpms**
- Satellite Client 6 リポジトリーを有効にして Satellite に同期し、ホスト上でそれを有効にしている。
- Ansible デプロイメント方法を使用して コンプライアンスポリシーを作成 し、ホストグループを割り当てている。

手順

1. Satellite Web UI で、**Configure** > **Host Groups** に移動します。
2. OpenSCAP レポート用に設定するホストグループをクリックします。

3. **OpenSCAP Capsule** リストから、使用する OpenSCAP が有効な Capsule を選択します。
4. **Ansible Roles** タブで、**foreman.foreman_scap_client** Ansible ロールを割り当てます。
5. オプション: **Parameters** タブで、ロールの Ansible 変数を設定します。
6. **Submit** をクリックして変更を保存します。
7. 必要なホストグループの行で、**Actions** 列に移動し、**Run all Ansible roles** を選択します。

9.4. ANSIBLE を使用してホストにポリシーを展開する

Ansible を使用してホストにコンプライアンスポリシーをデプロイすると、Ansible ロールによって SCAP クライアントがインストールされ、選択したコンプライアンスポリシーに従ってホスト上で OpenSCAP スキャンが設定されます。

コンプライアンスポリシーの SCAP コンテンツでは、リモートリソースが必要になる場合があります。詳細は、「リモート SCAP リソースの組み込み」 を参照してください。

前提条件

- Capsule で OpenSCAP を有効にしている。詳細は、**Capsule Server のインストール** の Capsule Server での OpenSCAP の有効化 を参照してください。
- オペレーティングシステムリポジトリーを有効にして Satellite に同期し、ホスト上で有効にしている。
  - Red Hat Enterprise Linux 9 for x86_64 - BaseOS および Appstream (RPM) - **rhel-9-for-x86_64-baseos-rpms** および **rhel-9-for-x86_64-appstream-rpms**
  - Red Hat Enterprise Linux 8 for x86_64 - BaseOS および Appstream (RPM) - **rhel-8-for-x86_64-baseos-rpms** および **rhel-8-for-x86_64-appstream-rpms**
  - Red Hat Enterprise Linux 7 Server および Extras (RPM) - **rhel-7-server-rpms** および **rhel-7-server-extras-rpms**
- Satellite Client 6 リポジトリーを有効にして Satellite に同期し、ホスト上でそれを有効にしている。
- Ansible デプロイメント方法を使用して コンプライアンスポリシーを作成 している。

手順

1. Satellite Web UI で **Hosts** > **All Hosts** に移動して、OpenSCAP レポートを設定するホストで、**Edit** をクリックします。
2. **OpenSCAP Capsule** リストから、使用する OpenSCAP が有効な Capsule を選択します。
3. **Ansible Roles** タブで、**theforeman.foreman_scap_client** Ansible ロールを追加します。
4. オプション: **Parameters** タブで、ロールの Ansible 変数を設定します。
5. **Submit** をクリックして変更を保存します。
6. **Hosts** ブレッドクラムリンクをクリックして、ホストのインデックスページに戻ります。

7. ポリシーを追加するホストを選択します。
8. **Select Action** をクリックします。
9. リストから **Assign Compliance Policy** を選択します。
10. **Assign Compliance Policy** ウィンドウで、**Remember hosts selection for the next bulk action** を選択します。
11. 使用可能なポリシーのリストから必要なポリシーを選択し、**Submit** をクリックします。
12. **Select Action** をクリックします。
13. リストから **Run all Ansible roles** を選択します。

9.5. PUPPET を使用してホストグループにポリシーを展開する

Puppet を使用してホストグループにコンプライアンスポリシーをデプロイすると、Puppet エージェントによって SCAP クライアントがインストールされ、選択したコンプライアンスポリシーに従って次回の Puppet 実行時にホスト上で OpenSCAP スキャンが設定されます。

コンプライアンスポリシーの SCAP コンテンツには、リモートリソースが必要になる場合があります。詳細は、「リモート SCAP リソースの組み込み」 を参照してください。

前提条件

- Capsule で OpenSCAP を有効にしている。詳細は、**Capsule Server のインストール** の Capsule Server での OpenSCAP の有効化 を参照してください。
- オペレーティングシステムリポジトリーを有効にして Satellite に同期し、ホスト上で有効にしている。
  - Red Hat Enterprise Linux 9 for x86_64 - BaseOS および Appstream (RPM) - **rhel-9-for-x86_64-baseos-rpms** および **rhel-9-for-x86_64-appstream-rpms**
  - Red Hat Enterprise Linux 8 for x86_64 - BaseOS および Appstream (RPM) - **rhel-8-for-x86_64-baseos-rpms** および **rhel-8-for-x86_64-appstream-rpms**
  - Red Hat Enterprise Linux 7 Server および Extras (RPM) - **rhel-7-server-rpms** および **rhel-7-server-extras-rpms**
- Satellite Client 6 リポジトリーを有効にして Satellite に同期し、ホスト上でそれを有効にしている。
- Puppet デプロイメント方法を使用して コンプライアンスポリシーを作成 し、ホストグループを割り当てている。

手順

1. Satellite Web UI で、**Configure** > **Host Groups** に移動します。
2. OpenSCAP レポート用に設定するホストグループをクリックします。
3. **Environment** リストで、**foreman_scap_client*** Puppet クラスを含む Puppet 環境を選択します。

4. **OpenSCAP Capsule** リストで、使用する OpenSCAP が有効になっている Capsule を選択します。
5. **Puppet ENC** タブで、**foreman_scap_client** Puppet クラスを追加します。
6. オプション: **Puppet Class Parameters** を設定します。
7. **Submit** をクリックして変更を保存します。

9.6. PUPPET を使用してホストにポリシーを展開する

Puppet を使用してホストにコンプライアンスポリシーをデプロイすると、Puppet エージェントによって SCAP クライアントがインストールされ、選択したコンプライアンスポリシーに従って次回の Puppet 実行時にホスト上で OpenSCAP スキャンが設定されます。

コンプライアンスポリシーの SCAP コンテンツには、リモートリソースが必要になる場合があります。詳細は、「リモート SCAP リソースの組み込み」 を参照してください。

前提条件

- Capsule で OpenSCAP を有効にしている。詳細は、**Capsule Server のインストール** の Capsule Server での OpenSCAP の有効化 を参照してください。
- オペレーティングシステムリポジトリーを有効にして Satellite に同期し、ホスト上で有効にしている。
  - Red Hat Enterprise Linux 9 for x86_64 - BaseOS および Appstream (RPM) - **rhel-9-for-x86_64-baseos-rpms** および **rhel-9-for-x86_64-appstream-rpms**
  - Red Hat Enterprise Linux 8 for x86_64 - BaseOS および Appstream (RPM) - **rhel-8-for-x86_64-baseos-rpms** および **rhel-8-for-x86_64-appstream-rpms**
  - Red Hat Enterprise Linux 7 Server および Extras (RPM) - **rhel-7-server-rpms** および **rhel-7-server-extras-rpms**
- Satellite Client 6 リポジトリーを有効にして Satellite に同期し、ホスト上でそれを有効にしている。
- Puppet デプロイメント方法を使用して コンプライアンスポリシーを作成 している。

手順

1. Satellite Web UI で **Hosts** > **All Hosts** に移動して、OpenSCAP レポートを設定するホストで、**Edit** をクリックします。
2. **Environment** リストから、**foreman_scap_client** および **foreman_scap_client::params** が含まれる Puppet 環境を選択します。
3. **OpenSCAP Capsule** リストから、使用する OpenSCAP が有効な Capsule を選択します。
4. **Puppet ENC** タブで、**foreman_scap_client** Puppet クラスを追加します。
5. オプション: **Puppet Class Parameters** を設定します。
6. **Hosts** ブレッドクラムリンクをクリックして、ホストのインデックスページに戻ります。
7. ポリシーを追加するホストを選択します。

8. **Select Action** をクリックします。
9. リストから **Assign Compliance Policy** を選択します。
10. **Assign Compliance Policy** ウィンドウで、 **Remember hosts selection for the next bulk action** を選択します。
11. 使用可能なポリシーのリストから必要なポリシーを選択し、**Submit** をクリックします。

第10章 オンデマンドのセキュリティーコンプライアンススキャンの実行

ホストは、ホストに割り当てられたコンプライアンスポリシーで定義された CRON スケジュールに従って、OpenSCAP スキャンを定期的に実行します。ただし、ホスト上で、設定されているすべてのコンプライアンスポリシーのスキャンを随時手動で実行することもできます。

前提条件

- ユーザーアカウントに **view_hosts**、**create_job_invocations**、および **view_job_invocations** 権限を持つロールが割り当てられている。
- コンプライアンスポリシーを作成し、ホストにデプロイしている。
  - ポリシーの管理の詳細は、8章 *コンプライアンスポリシーの管理* を参照してください。
  - ポリシーのデプロイの詳細は、9章 *コンプライアンスポリシーの導入* を参照してください。

手順

1. **Hosts** > **All Hosts** に移動します。
2. 必要なホストのホスト名をクリックします。
3. ホストの詳細ページで、**Schedule a job** ドロップダウンメニューを展開します。
4. **Run OpenSCAP scan** を選択します。

検証

1. ホストの詳細の概要で、**Recent jobs** カードを見つけます。
2. **Running** タブを選択します。ジョブがすでに終了していない限り、表に **Run scan for all OpenSCAP policies** というジョブが表示されます。
3. **Recent jobs** カードで、**Finished** タブを選択します。
4. ジョブが正常に終了すると、ジョブの行に **succeeded** ステータスが表示されます。
5. オプション: ジョブ名をクリックして呼び出しの詳細を確認します。

第11章 コンプライアンスの監視

Satellite を使用すると、コンプライアンスの監視と管理を一元化できます。コンプライアンスダッシュボードでは、ホストのコンプライアンスの概要が表示され、そのポリシーの範囲内にある各ホストの詳細を表示できます。コンプライアンスレポートでは、適用可能なポリシーを使用して、各ホストのコンプライアンスの詳細を分析します。この情報を使用して、各ホストが提示するリスクを評価し、ホストがコンプライアンスを満たすために必要なリソースを管理できます。SCAP を使用してコンプライアンスを監視することで、ポリシーのコンプライアンスを確認し、コンプライアンスの変化を検出できます。

11.1. コンプライアンスレポートの検索

コンプライアンスレポート検索フィールドを使用して、ホストのサブセットで使用可能なレポートのリストをフィルタリングします。

手順

1. Satellite Web UI で、**ホスト** > **コンプライアンス** > **レポート** に移動します。
2. オプション: 空の **Search** フィールドをクリックすると、利用可能な検索パラメーターがリスト表示されます。
3. **Search** フィールドに検索クエリーを入力し、**Search** をクリックします。検索クエリーでは大文字と小文字は区別されません。

検索クエリーの例

5 つを超えるルールが失敗したすべてのコンプライアンスレポートを検索する

```
failed > 5
```

2023 年 1 月 1 日以降に作成された、ホスト名に prod- が含まれるホストのすべてのコンプライアンスレポートを検索します。

```
host ~ prod- AND date > "Jan 1, 2023"
```

1 時間前に rhel7_audit コンプライアンスポリシーによって生成されたすべてのレポートを検索する

```
"1 hour ago" AND compliance_policy = date = "1 hour ago" AND compliance_policy = rhel7_audit
```

XCCDF ルールに合格するレポートを検索する

```
xccdf_rule_passed = xccdf_org.ssgproject.content_rule_firefox_preferences-auto-download_actions
```

XCCDF ルールに不合格となるレポートを検索する

```
xccdf_rule_failed = xccdf_org.ssgproject.content_rule_firefox_preferences-auto-download_actions
```

結果が XCCDF ルールに合格または不合格以外のレポートを検索する

```
xccdf_rule_othered = xccdf_org.ssgproject.content_rule_firefox_preferences-auto-download_actions
```

関連情報

- 論理演算子 **and**、**not**、および **has** を使用すると、複雑なクエリーを作成できます。論理 Operator の詳細は、**Red Hat Satellite の管理** の 詳細な検索でサポートされている Operators を参照してください。
- 正規表現は、検索クエリーで使用できません。ただし、1 つの検索式に複数のフィールドを使用できます。利用可能なすべての検索 Operator の詳細は、**Red Hat Satellite の管理** の 詳細な検索でサポートされている Operators を参照してください。
- 検索をブックマークすると、同じ検索クエリーを再利用できます。詳細は、**Red Hat Satellite の管理** の ブックマークの作成を 参照してください。

11.2. コンプライアンスメール通知

Satellite Server は、**コンプライアンスポリシーサマリー** のメール通知をサブスクライブしているすべてのユーザーに、OpenSCAP サマリーメールを送信します。メール通知のサブスクライブに関する詳細は、**Red Hat Satellite の管理** の メール通知の設定 を参照してください。

ポリシーが実行されるたびに、Satellite は直前の実行との比較で結果をチェックし、変更がないかどうかを確認します。メールは各サブスクライバーがリクエストする頻度で送信され、各ポリシーのサマリーと直近の結果を提供します。

11.3. コンプライアンスポリシーの統計の表示

コンプライアンスポリシーダッシュボードを表示して、特定のポリシーのコンプライアンスレポートを確認できます。コンプライアンスポリシーダッシュボードでは、ホストのコンプライアンスの統計的なサマリーが表示され、そのポリシーの範囲内にある各ホストのレポートの詳細を表示できます。

コンプライアンスレポートを表示するときは、次のホストを優先することを検討してください。

- **Failed** と評価されたホスト
- ステータスが不明なため **Never audited** とラベル付けされたホスト

前提条件

- ユーザーアカウントに **view_policies** 権限を持つロールが割り当てられている。

手順

1. Satellite Web UI で、**ホスト** > **コンプライアンス** > **ポリシー** に移動します。
2. 必要なポリシーの行で、**Actions** 列に移動し、**Dashboard** をクリックします。

11.4. ルール準拠結果ごとのホストの調査

簡略化されたレポートを調べ、ポリシールールを使用して、特定のルールの不合格など、特定のコンプライアンス結果を持つホストをリスト表示できます。

前提条件

- ユーザーアカウントに **view_arf_reports** および **view_hosts** 権限を持つロールが割り当てられている。

手順

1. Satellite Web UI で、**ホスト** > **コンプライアンス** > **レポート** に移動します。
2. **Reported At** 列で、必要なホストとコンプライアンスポリシーのレポートに移動し、時刻のリンクをクリックします。
3. Satellite で、ポリシールールの簡略化されたリストとスキャンの結果が表示されます。
4. オプション: チェック結果によってルールをフィルターします。**Show log messages** ドロップダウンリストから、次のフィルターのいずれかを選択します。
   - **Failed and othered** - 不合格となったルール、またはスキャン中にチェックされなかったルールを表示します。
   - **Failed only** - 不合格となったルールのみを表示します。
5. オプション: ルールの詳細を調べます。**Message** 列で、ルール名の横にあるアイコンをクリックします。
6. 必要なルールの行で、**Actions** 列に移動し、**Hosts failing this rule** をクリックします。

11.5. ホストのコンプライアンス違反の調査

完全なコンプライアンスレポートを調べて、ホストがルールに準拠できなかった理由を特定できます。場合によっては、非準拠状態を修復する方法を確認できます。

警告

推奨される修復アクションやスクリプトは、先に実稼働以外の環境でテストしてから実装してください。修復によりシステムが機能しなくなる可能性があります。

コンプライアンスレポートは次のエリアで構成されています。

- 導入部分
- Evaluation Characteristics (評価特性)
- Compliance and Scoring (コンプライアンスおよびスコアリング)
- ルールの概要

前提条件

- ユーザーアカウントに **view_arf_reports** および **view_hosts** 権限を持つロールが割り当てられている。

手順

1. Satellite Web UI で、**ホスト** > **コンプライアンス** > **レポート** に移動して、すべてのコンプライアンスレポートをリスト表示します。
2. 必要なホストの行で、**Actions** 列に移動し、**Full Report** をクリックして、評価レポートの完全な詳細を表示します。
3. **Evaluation Characteristics** エリアに移動して、特定のプロファイルに対するホストの評価に関する基本情報を確認します。
4. **Compliance and Scoring** エリアに移動して、評価の統計情報とホストのコンプライアンススコアを確認します。
5. **Rule Overview** に移動してルールを調べます。
6. オプション: **pass**、**notapplicable**、または **fix** など、非表示にするチェックステータスの選択を解除します。
7. オプション: **Group rule by** ドロップダウンメニューから、**Severity** などのルールのグループ化の基準を選択します。
8. オプション: 検索フィールドに検索文字列を入力して、ルールをタイトルでフィルターします。検索は大文字と小文字を区別せず、入力時に動的に適用されます。
9. ルールのタイトルをクリックして、結果の詳細を調べます。
   - ルールの説明と、ホストのコンプライアンスを満たすための指示 (利用できる場合)。
   - ルールの根拠。
   - 場合により、修復スクリプト。

11.6. コンプライアンスレポートの削除

Satellite のコンプライアンスレポートを削除できます。

前提条件

- ユーザーアカウントに **view_arf_reports** および **destroy_arf_reports** 権限を持つロールが割り当てられている。

手順

1. Satellite Web UI で、**ホスト** > **コンプライアンス** > **レポート** に移動します。
2. コンプライアンスレポートウィンドウで、削除するポリシーを特定し、ポリシーの名前の右側にある **Delete** を選択します。
3. **OK** をクリックします。

11.7. 複数のコンプライアンスレポートを削除する

複数のコンプライアンスポリシーを同時に削除できます。ただし、Satellite Web UI では、コンプライアンスポリシーはページ分割されているため、レポートを 1 ページずつ削除する必要があります。すべての OpenSCAP レポートを削除する場合は、**API ガイド** の OpenSCAP レポートの削除 にあるスクリ

プトを使用します。

前提条件

- ユーザーアカウントに **view_arf_reports** および **destroy_arf_reports** 権限を持つロールが割り当てられている。

手順

1. Satellite Web UI で、**ホスト** > **コンプライアンス** > **レポート** に移動します。
2. コンプライアンスレポートウィンドウで、削除するコンプライアンスレポートを選択します。
3. リストの右上の **Delete reports** を選択します。
4. 削除するページ数だけ、この手順を繰り返します。