Red Hat Insights 1-latest

FedRAMP を使用した Red Hat Insights 修復ガイド

修復 Playbook を使用した RHEL システムの問題の修正

Last Updated: 2024-03-27

Red Hat Insights 1-latest FedRAMP を使用した Red Hat Insights 修復ガイド

修復 Playbook を使用した RHEL システムの問題の修正

法律上の通知

Copyright © 2024 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

Insights に登録されているシステムの問題を FedRAMP® を使用して修正するための Playbook を作成します。 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 修復の概要

Red Hat Enterprise Linux (RHEL) インフラストラクチャーで優先度が最も高い修復事項を特定したら、その問題を修正する修復 Playbook を作成できます。

サブスクリプションの要件

- Red Hat Insights for Red Hat Enterprise Linux は、すべての RHEL サブスクリプションに含まれています。Insights 修復機能を使用するために追加のサブスクリプションは必要ありません。

ユーザー要件

- Insights のすべてのユーザーは、修復 Playbook の読み取り、作成、および管理に自動的にアクセスできます。

1.1. USER ACCESS に関する考慮事項

アカウントのどのユーザーも、Insights for Red Hat Enterprise Linux のほとんどのデータにアクセスできます。

事前定義済みグループおよびロールの概要

アクセスには、以下の事前定義済みのグループおよびロールが関連します。

- **デフォルトのアクセスグループ:** アカウント上のすべてのユーザーが、デフォルトアクセスグループのメンバーです。デフォルトのアクセスグループのメンバーには読み取り専用アクセス権があります。これにより、Insights for Red Hat Enterprise Linux のほとんどの情報を表示できます。

1.1.1. 修復ユーザーの User Access ロール

Remediations Viewer ロールにより、Insights for Red Hat Enterprise Linux の修復機能への標準または拡張アクセスが有効になります。Remediations viewer ロールは、デフォルトのアクセスグループに含まれています。Remediations viewer ロールは、アカウントの既存の Playbook を表示し、新しい Playbook を作成するためのアクセスを許可します。Remediations viewer は、システムで Playbook を実行できません。

第2章 INSIGHTS での修復 PLAYBOOK の作成と管理

Playbook を作成するワークフローは、Insights for Red Hat Enterprise Linux の各サービスで似ています。一般に、1 つのシステムまたはシステムのグループの 1 つ以上の問題を修正します。

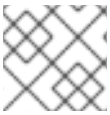
> Playbooks focus on issues identified by Insights services. A recommended practice for playbooks is to include systems of the same RHEL major/minor versions because the resolutions will be compatible.

2.1. RHEL システムの CVE 脆弱性を修復する PLAYBOOK の作成

Red Hat Insights 脆弱性サービスで修復 Playbook を作成します。Playbook を作成するワークフローは、Insights for Red Hat Enterprise Linux の他のサービスと同様です。

前提条件

- Red Hat Hybrid Cloud Console にログインしている。



注記

修復 Playbook を作成するために、拡張 User Access 権は必要ありません。

手順

1. Security > Vulnerability > CVEs ページに移動します。
2. 必要に応じてフィルターを設定し、CVE をクリックします。
3. 下にスクロールして、影響を受けるシステムを表示します。
4. システム ID の左側にあるボックスをクリックして、修復 Playbook に含めるシステムを選択します。

注記

同じ RHEL メジャー/マイナーバージョンのシステムを含めてください。これは、影響を受けるシステムのリストをフィルタリングすることで実行できます。

5. **Remediate** ボタンをクリックします。
6. 修復を **既存** または **新規** の Playbook に追加するかどうかを選択し、以下のアクションを実行します。
   a. **Add to existing playbook** をクリックし、ドロップダウンリストから必要な Playbook を選択します。または、
   b. **Create new playbook** をクリックし、Playbook 名を追加します。
   c. Next をクリックします。
7. Playbook に含めるシステムを確認し、**Next** をクリックします。
8. 修復レビューの概要で情報を確認します。

a. デフォルトでは、**autoreboot** が有効になっています。**Turn off autoreboot** をクリックすると、このオプションを無効にできます。

b. **Submit** をクリックします。

検証手順

1. Automation Toolkit > Remediations に移動します。
2. Playbook を検索します。Playbook が表示されます。

2.1.1. 推奨解決策および代替解決策が存在する場合に、セキュリティールールのある CVE を修復する Playbook を作成する

Red Hat Insights for RHEL のほとんどの CVE では、問題の解決に使用できる修復オプションは 1 つです。セキュリティールールのある CVE の修復には、複数の推奨解決策と代替解決策が含まれる場合があります。複数の解決策がある CVE 用の Playbook を作成するワークフローは、Advisor サービスの修復手順と似ています。

セキュリティールールの詳細は、セキュリティールール、および RHEL システムでのセキュリティー脆弱性の評価および監視 の セキュリティールールのリスクに晒されているシステムリストのフィルタリング を参照してください。

前提条件

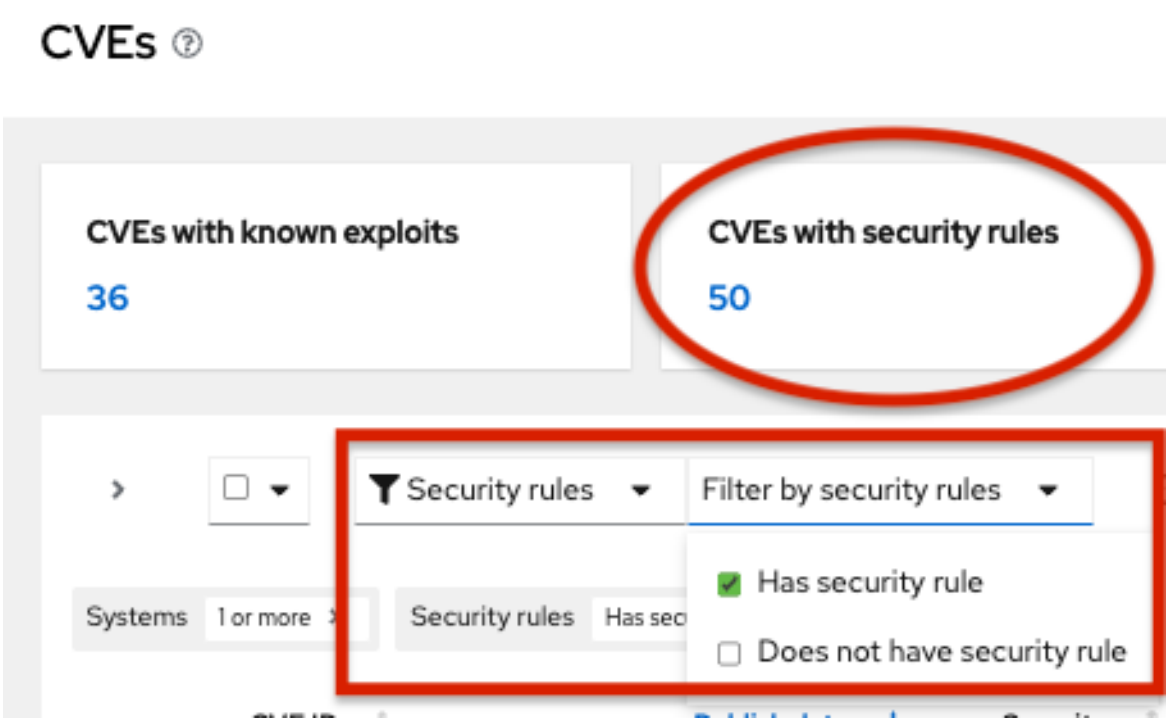
- Red Hat Hybrid Cloud Console にログインしている。

注記

修復 Playbook を作成するために、拡張 User Access 権は必要ありません。

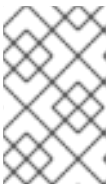
手順

1. **Security > Vulnerability > CVEs**に移動します。
2. 必要に応じてフィルターを設定します (たとえば、CVE に関連するリスクが大きい問題に焦点を当てるために、**セキュリティールールのある CVE** をフィルタリングして表示します)。または、ダッシュバーの CVEs with security rules タイルをクリックします。2 つのオプションをイメージで例示します。



3. リスト内の CVE をクリックします。

4. スクロールして影響を受けるシステムを表示し、**Review systems** ページでシステム ID の左側にあるボックスをクリックして、修復 Playbook に含めるシステムを選択します。(1 つ以上のシステムを選択すると、Remediate ボタンがアクティブになります。)



注記

推奨: 影響を受けるシステムのリストをフィルタリングして、同じ RHEL メジャーバージョンまたはマイナーバージョンのシステムを含めることを推奨します。

5. **Remediate** をクリックします。

6. 次のいずれかのアクションを実行して、修復を既存の Playbook に追加するか新しい Playbook に追加するかを決定します。

   - **Add to existing playbook** を選択し、ドロップダウンリストから必要な Playbook を選択します。または、

   - **Create new playbook** を選択し、Playbook 名を追加します。この例では、HCCDOC-392 と入力します。

7. **Next** をクリックします。システムのリストが画面に表示されます。

8. Playbook に含めるシステムを確認します (Playbook に含めないシステムの選択を解除します)。

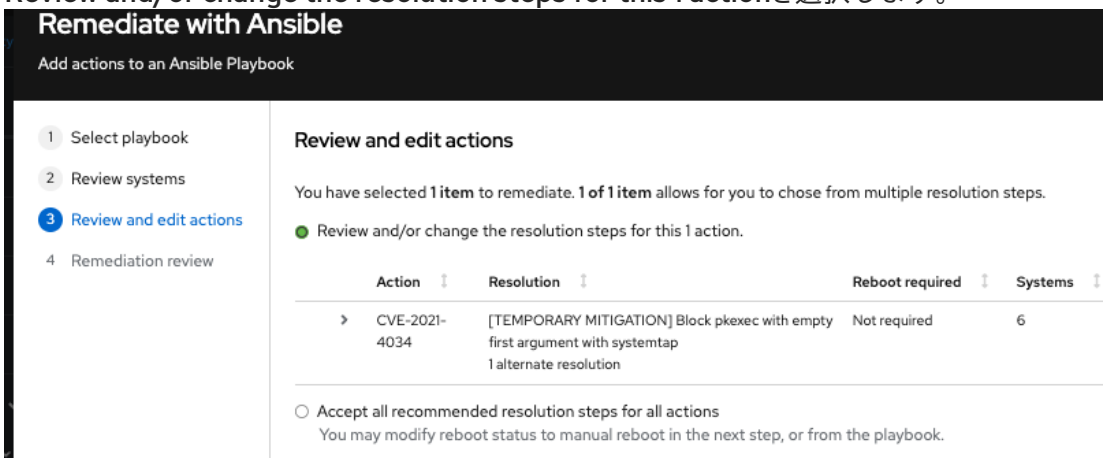
9. **Next** をクリックすると、**Review and edit actions** ページが表示され、CVE を修復するオプションが表示されます。修復する項目の数はさまざまです。次のような、CVE に関する追加情報 (展開や折りたたみが可能) も表示されます。

- **Action:** CVE ID を示します。
- **Resolution:** CVE の推奨解決策を示します。代替解決策があるかどうかを示します。
- **Reboot required:** システムを再起動する必要があるかどうかを示します。
- **Systems:** 修復するシステムの数を示します。

10. **Review and edit actions**ページで、次の 2 つの選択肢のどちらかを選択して、Playbook の作成を完了します。

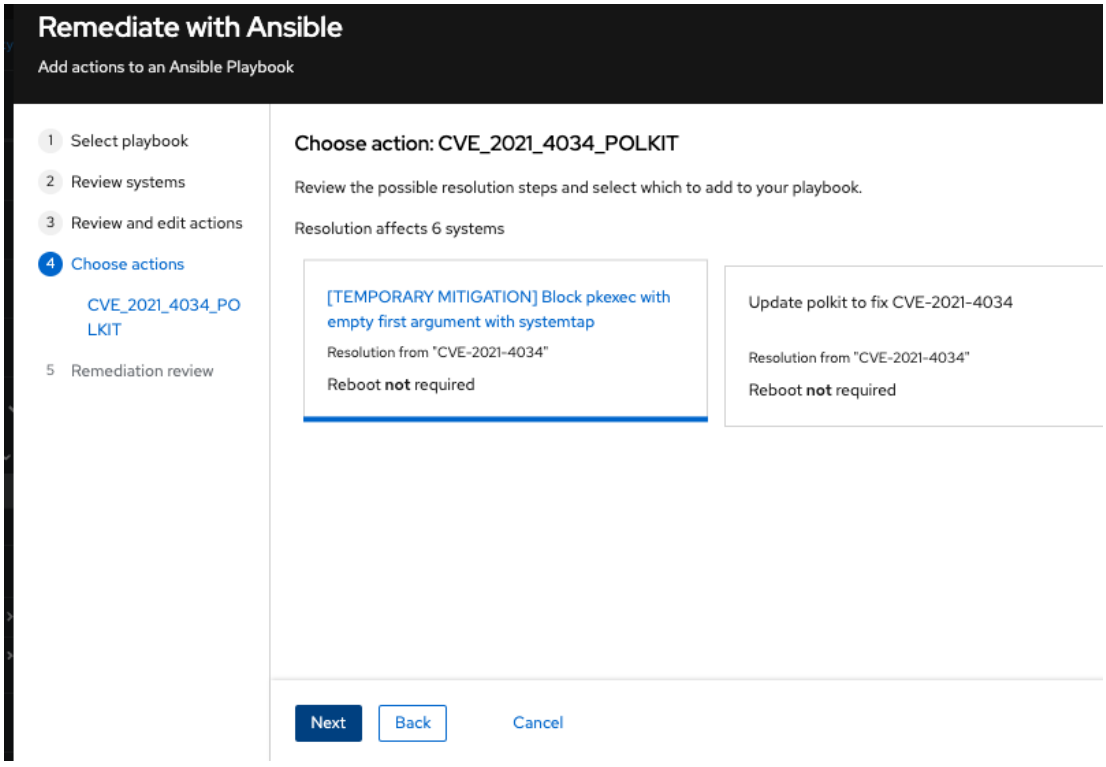
    - **選択肢 1:** 利用可能な推奨修復オプションと代替修復オプションをすべて確認します (その中からいずれかのオプションを選択します)。

        a. **Review and/or change the resolution steps for this 1 action**を選択します。



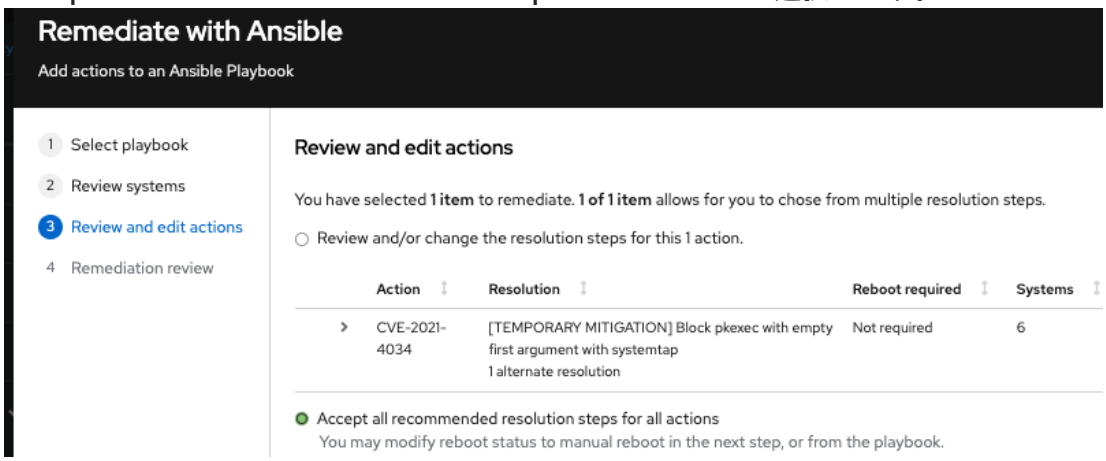
        b. **Next** をクリックします。

        c. **Choose action: <CVE information>**ページで、タイルをクリックして希望する修復オプションを選択します。タイルを選択すると、タイルの下端が強調表示されます。推奨解決策はデフォルトで強調表示されます。

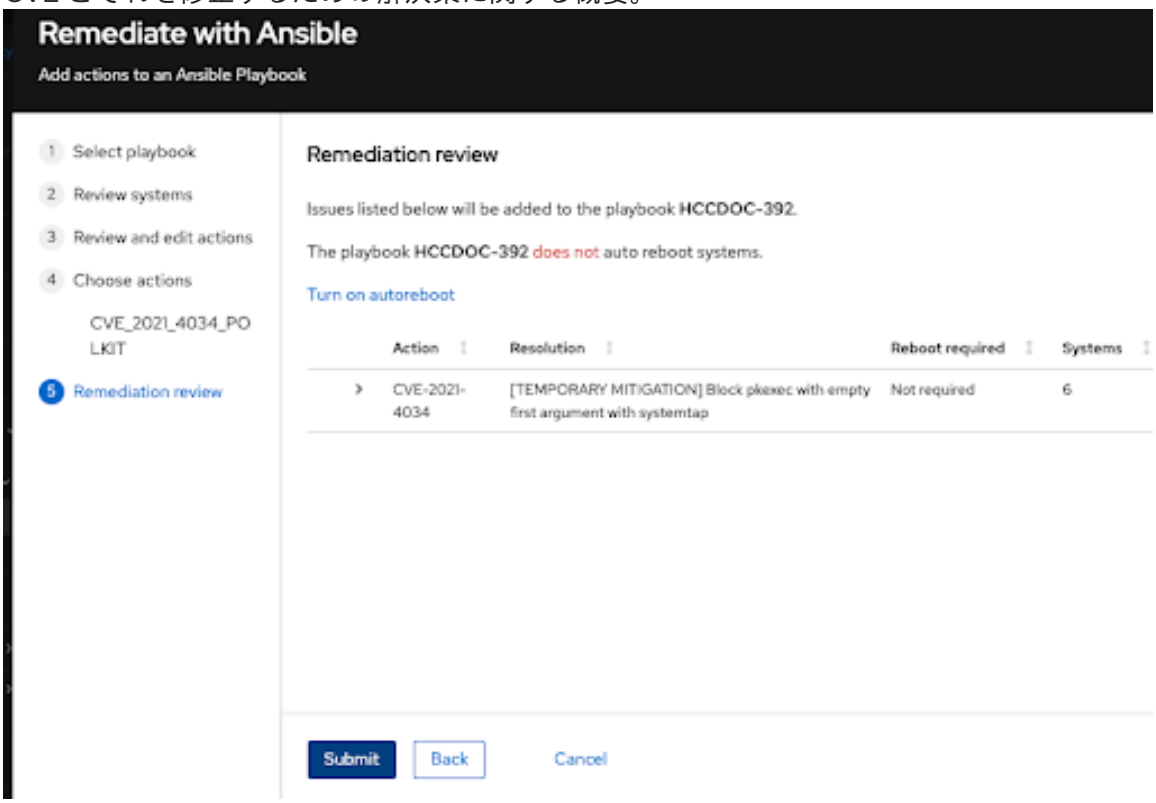


        d. **Next** をクリックします。

- **選択肢 2:** 推奨される修復をすべて受け入れます。
  - **Accept all recommended resolutions steps for all actions**を選択します。



11. **Remediations review** ページで、選択した内容に関する情報を確認し、システムの自動再起動のオプションを変更します。このページには次の内容が表示されます。
    - Playbook に追加する問題。
    - システムの自動再起動の要件を変更するためのオプション。
    - CVE とそれを修正するための解決策に関する概要。



12. オプションです。必要に応じて、**Remediation review** ページで自動再起動オプションを変更します。(自動再起動はデフォルトで有効になっていますが、使用する設定は修復オプションによって異なります。)

13. **Submit** をクリックします。Playbook に追加された修復アクションの数と、Playbook に関するその他の情報を示す通知が表示されます。

検証手順

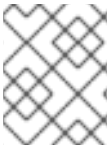
1. **Automation Toolkit > Remediations** に移動します。
2. Playbook を検索します。
3. Playbook を実行するには、Insights for Red Hat Enterprise Linux からの修復 Playbook の実行 を参照してください。

2.2. INSIGHTS FOR RED HAT ENTERPRISE LINUX での修復 PLAYBOOK の管理

組織の既存の修復 Playbook をダウンロード、アーカイブ、および削除できます。次の手順では、一般的な Playbook 管理タスクを実行する方法について説明します。

前提条件

- Red Hat Hybrid Cloud Console にログインしている。



注記

既存の Playbook に関する情報を表示、編集、またはダウンロードするために、拡張アクセス権は必要ありません。

2.2.1. 修復 Playbook のダウンロード

次の手順を使用して、Insights for Red Hat Enterprise Linux アプリケーションから修復 Playbook をダウンロードします。

手順

1. Automation Toolkit > Remediations に移動します。
2. 管理する Playbook を見つけて、Playbook の名前をクリックします。Playbook の詳細が表示されます。
3. **Download playbook** ボタンをクリックして、Playbook YAML ファイルをローカルドライブにダウンロードします。

2.2.2. 修復 Playbook のアーカイブ

不要になった修復 Playbook をアーカイブできますが、詳細は保持しておきます。

手順

1. Automation Toolkit > Remediations に移動します。
2. アーカイブする Playbook を見つけます。
3. オプションアイコン (⋮) をクリックし、**Archive playbook** を選択します。Playbook がアーカイブされます。

2.2.3. アーカイブされた修復 Playbook の表示

Insights for Red Hat Enterprise Linux で、アーカイブされた修復 Playbook を表示できます。

手順

1. Automation Toolkit > Remediations に移動します。
2. Playbook のダウンロードボタンの右側にある **More options** アイコン ( ) をクリックし、Show archived playbooks を選択します。

2.2.4. 修復 Playbook の削除

不要になった Playbook を削除できます。

手順

1. Automation Toolkit > Remediations に移動します。
2. 削除する Playbook の名前を見つけてクリックします。
3. Playbook の詳細ページで **More options** アイコン をクリックして **Delete** を選択します。

2.2.5. 修復ステータスの監視

各 Playbook の修復ステータスを表示できます。ステータス情報は、最新のアクティビティーの結果と、当該 Playbook に関するすべてのアクティビティーの概要を示しています。ログ情報も表示できます。

前提条件

- Red Hat Hybrid Cloud Console にログインしている。

手順

1. Automation Toolkit > Remediations に移動します。このページには、修復 Playbook のリストが表示されます。
2. Playbook の名前をクリックします。
3. **Actions** タブで、**Status** 列の任意の項目をクリックして、解決のステータスを示すポップアップボックスを表示します。

Satellite Web UI で Playbook のステータスを監視するには、Red Hat Satellite の **ホストの管理** ガイドの リモートジョブの監視 を参照してください。

第3章 修復用パッチテンプレートの使用

Red Hat Insights パッチアプリケーションは、スケジュールされたパッチ適用サイクルをサポートします。

パッチテンプレートは、ホストの **yum**/**dnf** 操作には影響しませんが、Red Hat Insights でパッチステータスレポートを絞り込むことができます。テンプレートを使用して、簡単なパッチサイクルの Remediation Playbook を作成できます。

3.1. 修復を含むパッチテンプレートの使用

パッチテンプレートには、複数のシステムに適用する 1 つ以上の修復を含めることができます。テスト環境でシステムのグループを更新するパッチテンプレートを作成し、同じパッチテンプレートを使用して実稼働環境のシステムを別の日に更新できます。

修復を含むパッチテンプレートの作成および使用の詳細は、**修復による Ansible Playbook を使用したシステムパッチ適用** を参照してください。

注記

割り当てたシステムにパッチテンプレートを適用すると、それらのシステムに該当する、最近公開されたアドバイザリーは表示されなくなります。Red Hat Hybrid Cloud Console の通知を使用すると、インフラストラクチャーに影響を与える可能性のある新しく公開されたアドバイザリーを確実に把握できます。

Red Hat Hybrid Cloud Console の通知の詳細は、**Red Hat Hybrid Cloud Console での通知の設定** を参照してください。

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。