



Red Hat Insights 1-latest

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

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

Playbook を作成して実行し、Insights に登録されたシステムの問題を修正します。Red Hat では、コード、ドキュメント、Web プロパティ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、用語の置き換えは、今後の複数のリリースにわたって段階的に実施されます。詳細は、Red Hat CTO である Chris Wright のメッセージをご覧ください。

目次

| | |
|--|-----------|
| 第1章 修復の概要 | 3 |
| 1.1. RED HAT HYBRID CLOUD CONSOLE のユーザーアクセス設定 | 3 |
| 第2章 INSIGHTS とのホスト通信の有効化 | 5 |
| 2.1. INSIGHTS によって直接管理されるシステムでの RHC クライアントの有効化 | 5 |
| 2.2. SATELLITE が管理するコンテンツホストの CLOUD CONNECTOR を有効にする | 6 |
| 第3章 INSIGHTS での修復 PLAYBOOK の作成と管理 | 9 |
| 3.1. RHEL システムの CVE 脆弱性を修復する PLAYBOOK の作成 | 9 |
| 3.2. INSIGHTS FOR RED HAT ENTERPRISE LINUX での修復 PLAYBOOK の管理 | 14 |
| 第4章 修復 PLAYBOOK の実行 | 16 |
| 4.1. INSIGHTS USER INTERFACE からの修復 PLAYBOOK の実行 | 16 |
| 4.2. SATELLITE USER INTERFACE からの修復の実行 | 16 |
| 第5章 修復用パッチテンプレートの使用 | 18 |
| 5.1. 修復を含むパッチテンプレートの使用 | 18 |
| 第6章 参照 | 19 |
| 6.1. SATELLITE SERVER コンテンツホストへの INSIGHTS クライアントのインストール | 19 |
| 6.2. SATELLITE SERVER 6.10 を 6.11 にアップグレードした後の CLOUD CONNECTOR の設定 | 19 |
| 6.3. SATELLITE SERVER コンテンツホストでの直接修復を無効にする | 19 |
| 6.4. SATELLITE SERVER コンテンツホストグループでの直接修復を無効にする | 20 |
| RED HAT ドキュメントへのフィードバック (英語のみ) | 21 |

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、修復 Playbook を作成して実行し、その問題を修正できます。

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

- Red Hat Hybrid Cloud Console (Hybrid Cloud Console) の Insights for Red Hat Enterprise Linux アプリケーションで修復機能にアクセスします。
- コンソールまたは Satellite アプリケーション UI で Red Hat Satellite が管理するシステムにアクセスします。
- 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。
- リモートシステムで Playbook を実行するには、事前定義済みの User Access ロールである **Remediations administrator** が必要です。このロールは、Hybrid Cloud Console の Identity & Access Management 設定で組織管理者が付与します。

1.1. RED HAT HYBRID CLOUD CONSOLE のユーザーアクセス設定

ユーザーアクセスは、ロールベースのアクセス制御 (RBAC) の Red Hat 実装です。組織管理者は、ユーザーアクセスを使用して、Red Hat Hybrid Cloud Console (コンソール) でユーザーが表示および実行できる内容を設定します。

- ユーザーに権限を個別に割り当てるのではなく、ロールを編成してユーザーアクセスを制御します。
- ロールとそれに対応する権限を含むグループを作成します。
- これらのグループにユーザーを割り当て、グループのロールに関連付けられた権限を継承できるようにします。

1.1.1. 定義済みのユーザーアクセスグループとロール

グループとロールを管理しやすくするために、Red Hat は2つの定義済みグループと一連の定義済みロールを提供しています。

1.1.1.1. 定義済みグループ

Default access group には、組織内のすべてのユーザーが含まれます。このグループには、多くの定義済みロールが割り当てられています。Red Hat によって自動的に更新されます。



注記

組織管理者が **Default access** グループに変更を加えると、名前が **Custom default access** グループに変更され、Red Hat による更新の対象外となります。

Default admin access グループには、組織管理者権限を持つユーザーのみが含まれます。このグループは自動的に維持され、このグループ内のユーザーとロールは変更できません。

Hybrid Cloud Console で [Red Hat Hybrid Cloud Console > Settings アイコン \(⚙️\) > Identity & Access Management > User Access > Groups](#) に移動し、アカウント内の現在のグループを表示します。このビューは組織管理者に限定されています。

1.1.1.2. グループに割り当てられた定義済みロール

Default access グループには、定義済みロールが多数含まれています。組織内のすべてのユーザーは **Default access** グループのメンバーであるため、そのグループに割り当てられているすべての権限を継承します。

Default admin access グループには、更新権限や削除権限を付与する多くの (ただしすべてではない) 定義済みロールが含まれています。通常、このグループのロールの名前には **administrator** が含まれません。

Hybrid Cloud Console で [Red Hat Hybrid Cloud Console > Settings アイコン \(⚙️\) > Identity & Access Management > User Access > Roles](#) に移動し、アカウント内の現在のロールを表示します。各ロールが割り当てられているグループの数を確認できます。このビューは組織管理者に限定されています。

詳細は、[ロールベースアクセス制御 \(RBAC\) のユーザーアクセス設定ガイド](#) を参照してください。

1.1.2. アクセス権限

各手順の **Prerequisites** には、必要な権限を提供する定義済みロールがリストされています。ユーザーは、[Red Hat Hybrid Cloud Console > Settings アイコン \(⚙️\) > My User Access](#) に移動して、現在継承しているロールとアプリケーションの権限を表示できます。

Insights for Red Hat Enterprise Linux 機能にアクセスしようとしたときに、そのアクションの実行権限がないというメッセージが表示された場合は、追加の権限を取得する必要があります。それらの権限は、組織の組織管理者またはユーザーアクセス管理者が設定します。

Red Hat Hybrid Cloud Console 仮想アシスタントに、"Contact my Organization Administrator" と依頼します。アシスタントがあなたに代わって組織管理者にメールを送信します。

1.1.3. 修復ユーザーの User Access ロール

次のロールにより、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**。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。
- **Remediations administrator**。Remediations administrator は、システム上での Playbook のリモート実行を含む、すべての修復機能へのアクセスを許可します。

第2章 INSIGHTS とのホスト通信の有効化

Red Hat Insights for Red Hat Enterprise Linux からリモートシステムで Playbook を実行するには、システムが Red Hat Insights と通信できる必要があります。

- **Red Hat Satellite で管理されていない** Red Hat Enterprise Linux システムの場合、以下の手順に従って、そのシステムで rhc クライアントを有効にする必要があります。
- Satellite によって **管理されている** システムの場合、そのシステムのホストサーバーで Cloud Connector を設定します。:context: host-communication-with-insights

2.1. INSIGHTS によって直接管理されるシステムでの RHC クライアントの有効化

Insights for Red Hat Enterprise Linux から修復 Playbook を実行できるようにするには、インフラストラクチャー内のシステムで rhc クライアントを有効にする必要があります。 **rhc connect** コマンドは、システム (RHEL8.6 以降、および 9.0 以降) を Red Hat Subscription Manager および Red Hat Insights に登録し、Insights for Red Hat Enterprise Linux でリモートホスト設定 (rhc) 機能を有効にすることでこれを行います。

前提条件

- Red Hat Enterprise Linux ホストシステムでの sudo アクセス

RHEL8.5 システムで rhc を接続する

RHEL 8.5 のリモートホスト設定には、 **ansible** と **rhc-worker-playbook** の依存関係があります。依存関係をインストールするには、最初に Subscription Manager に登録する必要があります。

- 次のコマンドを使用して、RHEL 8.5 システムで rhc を有効化します。

```
[root]# subscription-manager repos --enable ansible-2.9-for-rhel-8-x86_64-rpms
[root]# dnf -y install ansible rhc-worker-playbook-0.1.5-3.el8_4
[root]# rhc connect
```

RHEL8.6 以降のシステムでの rhc の接続

- 次のコマンドを使用して、RHEL8.6 以降のシステムで rhc を有効化します。

```
[root]# dnf -y update rhc
[root]# dnf -y install rhc-worker-playbook
[root]# rhc connect
```

RHEL9.0 以降のシステムでの rhc の接続

- 次のコマンドを使用して、RHEL9.0 以降のシステムで rhc を有効化します。

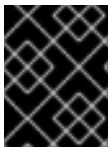
```
[root]# dnf -y install rhc rhc-worker-playbook
[root]# rhc connect
```

関連情報

- rhc を有効にすると、[Red Hat Hybrid Cloud Console > Red Hat Insights > Inventory > System Configuration > Remote Host Configuration \(RHC\)](#) で設定を管理できます。
- rhc の完全なドキュメントについては、[リモートホストの設定および管理](#) を参照してください。

2.2. SATELLITE が管理するコンテンツホストの CLOUD CONNECTOR を有効にする

Red Hat Hybrid Cloud Console の Insights for Red Hat Enterprise Linux ユーザーインターフェイスから、Satellite が管理するコンテンツホストの問題をリモートで修復できます。Insights からリモート修復を行うには、まず Satellite Server で Cloud Connector プラグインを設定する必要があります。



重要

Satellite Web コンソールからホストの修復を完全に管理および実行する場合は、Cloud Connector プラグインを有効にする必要はありません。

Satellite Server の設定は、次の前提条件すべてを満たす必要があります。

前提条件

- Satellite がバージョン 6.9 以降である。
- Satellite Server への root アクセス権がある。
- Satellite が管理するコンテンツホストには、Insights クライアントがインストールされ、オンになっている。Insights クライアントのインストールおよび有効化の手順は、このドキュメントの参照セクションで確認してください。
- サブスクリプションマニフェストを Satellite にインポートする。詳細は、[Red Hat Satellite のコンテンツ管理ガイド](#) の [Satellite Server へのサブスクリプションマニフェストのインポート](#) を参照してください。
- アクティベーションキーを使用して Satellite にホストを登録し、Red Hat サブスクリプションを割り当てる。詳細は、[Red Hat Satellite のホストの管理](#) ガイドの [ホストの登録](#) を参照してください。

2.2.1. Cloud Connector の設定と Satellite Server コンテンツホストインベントリーの Red Hat Insights へのアップロード

Insights からリモートで修復 Playbook を実行する前に、Satellite Server に Cloud Connector プラグインをインストールして設定する必要があります。以下のタスクを実行して、Cloud Connector の設定をインストール、設定、および確認します。

手順

1. Satellite Server で、Satellite Server のバージョンに応じて次のコマンドのいずれかを入力し、**remote-execution** プラグインを有効にします。
 - a. **Satellite Server 6.12 以降の場合**

```
[root]# satellite-installer --foreman-proxy-plugin-remote-execution-script-install-key true
```

b. On Satellite Server 6.9 - 6.11 の場合

```
[root]# satellite-installer --foreman-proxy-plugin-remote-execution-ssh-install-key true
```



注記

Cloud Connector を設定するには、Satellite が Satellite 上でリモート実行を行う必要があります。そのため、最初の手順として **remote-execution** スクリプトまたはプラグインを有効にします。

- Satellite Server Web UI で、**Configure > Red Hat Cloud > Inventory Upload**に移動します。**Automatic Inventory Upload**スイッチが **ON** になっていることを確認します。これはデフォルト設定です。
- オプション: Obfuscate host names** スwitchを **ON** の位置に切り替えて、Satellite Server が Hybrid Cloud Console に報告するホスト名を非表示にします。



注記

Obfuscate ホスト名の設定は、**rh_cloud** レポートにのみ影響します。ホスト名および IP アドレスを難読化する場合は、Insights クライアント設定で、難読化を設定する必要があります。Satellite はこの設定を読み取る方法を備えており、その設定に従います。Red Hat Insights のクライアント設定ガイドの [ホスト名の難読化](#) セクションおよび [IPv4 アドレスの難読化](#) セクションを参照してください。

Automatic inventory upload と **Obfuscate host names** はグローバル設定です。これらは、すべての組織に属するコンテンツホストに影響します。

- Configure Cloud Connector** をクリックします。Notice ダイアログボックスには、このアクションにより自動レポートのアップロードも有効になることが警告されます。**Confirm** をクリックします。
- 進捗状況が完了になるまで待機します。これには約1分かかります。ジョブを表示するには、**Jobs > Configure Cloud Connector**に移動します。
最終的に、**Red Hat Hybrid Cloud Console > Settings アイコン (⚙) > Integrations** の **Red Hat** タブに Satellite が表示されます。ジョブが Satellite Web コンソールに表示されるまで最大1時間かかります。

Inventory Uploads ページの下部には組織名が表示されます。その上にマウスを置くと、その領域が灰色になります。名前をクリックすると展開され、アップロードの進行状況を監視できる **Generating** タブと **Uploading** タブが表示されます。

- Restart** をクリックすると、Insights クライアントが実行されている各コンテンツホストからデータペイロードが生成され、ホストインベントリが Insights for Red Hat Enterprise Linux にアップロードされます。
コンテンツホストインベントリをアップロードする組織ごとに **Restart** をクリックし、この手順を繰り返します。
- 画面の右上にある切り替えを使用して、**Configure > Red Hat Cloud(Sat 6.11 以降) > Insights** で組織の自動同期を設定します。

検証

アップロードが成功したことを確認するには、[Red Hat Hybrid Cloud Console > Red Hat Enterprise Linux > Red Hat Insights > Inventory](#) にログインし、コンテンツホストの **satellite_id** タグを検索します。

必要に応じて、**Sync inventory status** ボタンを押して、タスクが完了するまで待ちます。Insights インベントリーにより認識されたコンテンツホストの数が表示されます。

第3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。

Playbook は、Insights サービスによって特定された問題に重点を置いています。Playbook の推奨プラクティスは、解像度に互換性があるため、同じ RHEL メジャー/マイナーバージョンのシステムを含めることです。

3.1. 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。

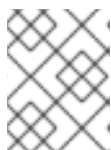


注記

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。

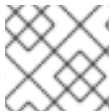
3.1.1. 推奨解決策および代替解決策が存在する場合に、セキュリティールールのある CVE を修復する Playbook を作成する

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。

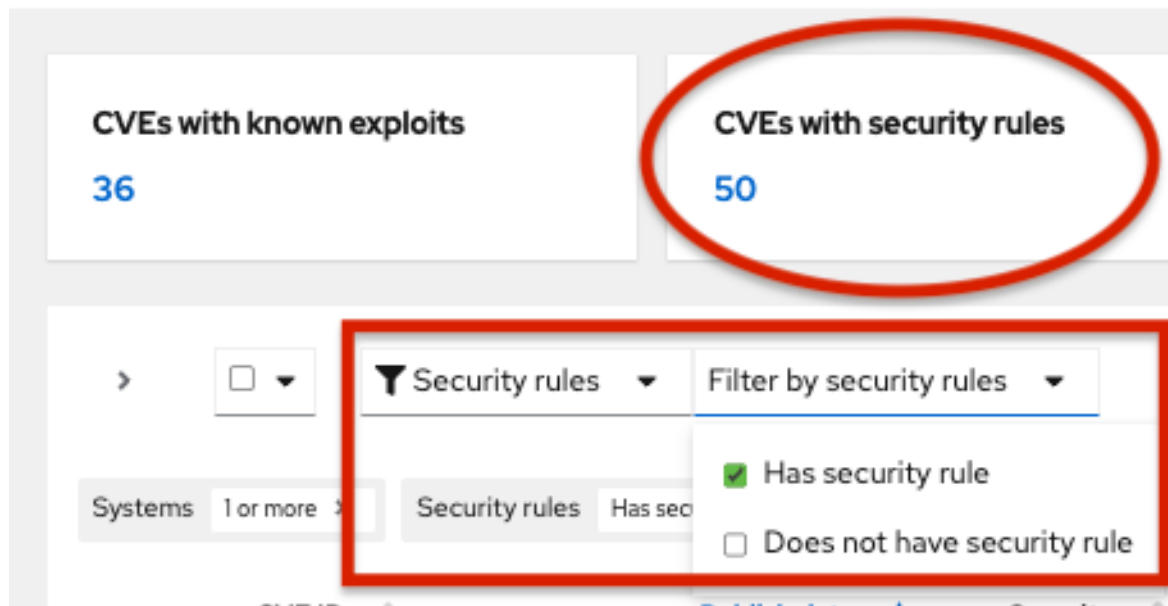


注記

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。

CVEs 

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。

Remediate with Ansible
Add actions to an Ansible Playbook

1 Select playbook
2 Review systems
3 **Review and edit actions**
4 Remediation review

Review and edit actions

You have selected 1 item to remediate. 1 of 1 item allows for you to chose from multiple resolution steps.

Review and/or change the resolution steps for this 1 action.

| Action | Resolution | Reboot required | Systems |
|-----------------|--|-----------------|---------|
| > CVE-2021-4034 | [TEMPORARY MITIGATION] Block pkexec with empty first argument with systemtap 1 alternate resolution | Not required | 6 |

Accept all recommended resolution steps for all actions
You may modify reboot status to manual reboot in the next step, or from the playbook.

- a. **Next** をクリックします。
- b. **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。

Remediate with Ansible
Add actions to an Ansible Playbook

1 Select playbook
2 Review systems
3 Review and edit actions
4 **Choose actions**
5 Remediation review

CVE_2021_4034_POLKIT

Choose action: CVE_2021_4034_POLKIT
Review the possible resolution steps and select which to add to your playbook.
Resolution affects 6 systems

[TEMPORARY MITIGATION] Block pkexec with empty first argument with systemtap
Resolution from "CVE-2021-4034"
Reboot **not** required

Update polkit to fix CVE-2021-4034
Resolution from "CVE-2021-4034"
Reboot **not** required

Next Back Cancel

c. 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。

Remediate with Ansible
Add actions to an Ansible Playbook

1 Select playbook
2 Review systems
3 **Review and edit actions**
4 Remediation review

Review and edit actions
You have selected 1 item to remediate. 1 of 1 item allows for you to chose from multiple resolution steps.

Review and/or change the resolution steps for this 1 action.

| Action | Resolution | Reboot required | Systems |
|-----------------|--|-----------------|---------|
| > CVE-2021-4034 | [TEMPORARY MITIGATION] Block pkexec with empty first argument with systemtap 1 alternate resolution | Not required | 6 |

Accept all recommended resolution steps for all actions
You may modify reboot status to manual reboot in the next step, or from the playbook.

1. **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。

+
image:img-remedy-remediation-review-summary.png[summary of remediation actions]

2. オプション: 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。)
3. **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。

3.2. 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を説明します。

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。

3.2.1. 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。

3.2.2. 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。

3.2.3. 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。

3.2.4. 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。

3.2.5. 修復ステータスの監視

Insights for Red Hat Enterprise Linux 修復サービスから実行する各 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、Playbook の実行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。Playbook の実行に関するログ情報を表示することもできます。

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4章 修復 PLAYBOOK の実行

修復 Playbook を作成したら、組織の Ansible ワークフローを使用して Playbook をダウンロードして実行するか、Insights for Red Hat Enterprise Linux アプリケーションからリモートシステムで Playbook を実行することができます。

4.1. INSIGHTS USER INTERFACE からの修復 PLAYBOOK の実行

インフラストラクチャー内のシステムに rhc クライアントをインストールした後、Insights for Red Hat Enterprise Linux アプリケーションから直接、リモート RHEL システム上で修復 Playbook を実行できます。

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。
- **Remediations administrator** ロールを持つ User Access グループのメンバーである必要があります。

手順

1. [Automation Toolkit > Remediations](#) に移動します。
2. 実行する修復 Playbook を選択し、Playbook 名をクリックします。
3. **Execute playbook** ボタンをクリックします。
4. ポップアップされたウィンドウで、**Execute playbook on systems** ボタンをクリックします。Playbook がそのシステムで実行されます。

4.2. SATELLITE USER INTERFACE からの修復の実行

Satellite User Interface を使用して修復することもできます。

前提条件

- **クラウド管理者** である。
- **修復管理者** である。
- Insights クライアントを使用したホストの登録が完了している。

具体的な手順については、Satellite のホストの管理ドキュメントの [ホストに関する Insights 修復プランの作成](#) を参照してください。



注記

プロビジョニングまたは登録によって新しいホストを Satellite インベントリに導入すると、2つの自動バックグラウンドタスクが開始されます。これらのタスクが完了するまでに 24 時間かかります。これは自動同期の一般的な時間枠です。

セキュリティ上の問題や、自動同期を 24 時間待たなくてもよい別のシナリオが見つかった場合は、UI の同期ボタンをクリックして手動で同期できます。この手動同期は数分で完了します。

自動および手動同期を有効にする手順を確認するには、Satellite ドキュメントの [ホストに関する Insights 推奨事項の同期の設定](#) を参照してください。

第5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せん。

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。

5.1. 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、[Remediation Playbook を使用したシステムパッチの適用](#) 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。

第6章 参照

次のトピックは、Insights 修復 Playbook の設定、作成、および管理に関連しています。

6.1. SATELLITE SERVER コンテンツホストへの INSIGHTS クライアントのインストール

Insights クライアントは、Red Hat Enterprise Linux のほとんどのバージョンにプリインストールされています。ただし、インストールする必要がある場合は、この手順を使用して各システムに Insights クライアントをインストールしてください。

前提条件

- ホストを Satellite に登録する。
すでに Red Hat Enterprise Linux ホストがある場合は、グローバル登録テンプレートを使用して Satellite に登録できます。詳細は、[Satellite へのホストの登録](#) を参照してください。

手順

1. Insights for Red Hat Enterprise Linux クライアントをインストールします。

```
# yum install insights-client
```

2. ホストを Insights for Red Hat Enterprise Linux に登録します。

```
# insights-client --register
```

3. 各ホストでこれらの手順を繰り返します。

または、**RedHatInsights.insights-client** Ansible ロールを使用して Insights クライアントをインストールし、ホストを登録することもできます。詳細は、[ホストの管理](#) ガイドの [Satellite のホストでの Red Hat Insights の使用](#) を参照してください。

6.2. SATELLITE SERVER 6.10 を 6.11 にアップグレードした後の CLOUD CONNECTOR の設定



注記

これは、Satellite バージョン 6.10 から 6.11 へのアップグレードにのみ適用されます。詳細は、[Red Hat Satellite のアップグレードおよび更新](#) ガイドを参照してください。

Satellite Server をアップグレードした後に Cloud Connector を設定するには、**Configure > RH Cloud - Inventory Upload** から **Configure Cloud Connector** ボタンをクリックして、新しいバージョンの Satellite Server で有効にします。同時に、Satellite Server のアップグレード後に、Red Hat Hybrid Cloud Console で以前のソースを手動でクラウドから削除する必要があります。

Cloud Connector を設定すると、レセプタービットが削除され、RHC ビットがインストールされます。同時に、Cloud Connector は Satellite のすべての組織をソースに通知し、接続を受け取る準備が整います。

6.3. SATELLITE SERVER コンテンツホストでの直接修復を無効にする

デフォルトでは、パラメーターは各ホストには設定されていません。パラメーターは、Cloud Connector でデフォルトで Playbook を実行できるように、**ホストグループに対して True** に設定されています。その特定の組織に存在するすべてのホストは、同じパラメーターを継承することに注意してください。

Satellite が Cloud Connector から修復 Playbook の実行リクエストを受信したとき、そのリクエストには、それを実行する必要があるホストのリストが含まれています。

シングルホスト上のクラウドから Playbook 実行が呼び出されないようにするには、次の手順を実行します。

手順

1. Satellite Web UI で、**Hosts menu > All Hosts**に移動します。
2. ホストを見つけて、**Edit button > Parameters タブ**をクリックし、そのホストで **enable_cloud_remediations** パラメーターを **False** に設定します。

6.4. SATELLITE SERVER コンテンツホストグループでの直接修復を無効にする

デフォルトでは、パラメーターは **システム** には設定されていません。パラメーターは、Cloud Connector を使用してデフォルトで Playbook を実行できるように、**ホストグループに対して True** に設定されています。



注記

その特定の組織に存在するすべてのホストは、同じパラメーターを継承します。

オプションで、組織管理者は組織全体またはホストグループのクラウド修復を無効にできます。修復を無効にするには、Red Hat Satellite ユーザーインターフェイスで **Global Parameter** を変更します。この編集を行うには、次の手順を使用します。

手順

1. **Satellite ダッシュボード** に移動します。
2. 左側のナビゲーションで **Configure** をクリックします。
3. **Global Parameters** をクリックします。
4. **Create Parameter** をクリックします。
5. **Name** フィールドに **enable_cloud_remediations** と入力します。
6. **Value** フィールドに **false** と入力します。
7. **Submit** をクリックします。

検証手順

Global Parameters の表にリストされている新しいパラメーターを見つけます。

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。フィードバックをご提供いただきありがとうございました。