Red Hat Insights 1-latest

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

セキュリティー脅威に晒されている可能性のある環境についての理解

Last Updated: 2024-06-28

Red Hat Insights 1-latest 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

セキュリティー脅威に晒されている可能性のある環境についての理解

法律上の通知

概要

Vulnerability サービスを使用して、RHEL システムでのセキュリティー脆弱性の状況を評価して監視するだけでなく、インフラストラクチャーの脆弱性のレベルを理解して、一連のアクションを計画します。 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 INSIGHTS FOR RHEL VULNERABILITY サービスの概要

Vulnerability サービスを使用すると、RHEL インフラストラクチャーの Common Vulnerabilities and Exposures (CVE) に対するリスクを素早く評価して、全体的に監視し、最も重要な問題とシステムをこれまで以上に理解し、修復を効率的に管理できるようになります。

データが Vulnerability サービスにアップロードされると、システムおよび CVE のグループをフィルタリングしてソートし、ビューを絞り込み、最適化することができます。また、個別の CVE がシステムに深刻なリスクを及ぼす場合は、個別の CVE にコンテキストを追加することもできます。リスクの脆弱性を理解したら、CVE のステータスを適切なステークホルダーに報告してから、Ansible Playbook を作成して問題を修復し、組織のセキュリティーを保護します。

前提条件

Vulnerability サービスは、RHEL 6、7、8、および 9 のすべてのサポート対象バージョンで利用できます。Vulnerability サービスを使用する前に、以下の条件を満たしている必要があります。

- **各システムには、Insights クライアントがインストールされ、Insights for Red Hat Enterprise Linux アプリケーションに登録されています。**Red Hat Insights for Red Hat Enterprise Linux スタートガイドの手順 に従って、クライアントをインストールし、システムを登録します。
- **Vulnerability サービスが、Red Hat Subscription Manager (RHSM) および Satellite 6 以降が管理する RHEL システムで完全にサポートされている。**RHSM および Satellite 6、または subscription.redhat.com (カスタマーポータル) に登録されている RHSM 以外の、パッケージ更新の取得方法を使用すると、想定外の結果に陥る可能性があります。
- **Satellite 5 および Spacewalk がホストする RHEL システムでは、Vulnerability サービスの修正は完全にサポートされておらず、適切に機能しない場合がある。**
- **機能によっては、組織の管理者が提供する特別な権限が必要である。**具体的には、特定の CVE およびシステムに関連付けられた Red Hat セキュリティーアドバイザリー (RHSA) を表示し、Red Hat Insights for Red Hat Enterprise Linux Patch サービスで脆弱性を表示およびパッチするには、ユーザーアクセスで付与されるパーミッションが必要です。

関連情報

- **Vulnerability サービスレポートの生成**

1.1. VULNERABILITY サービスの仕組み

Vulnerability サービスは、Insights クライアントを使用して RHEL システムに関する情報を収集します。クライアントはシステムに関する情報を収集し、脆弱性サービスにアップロードします。

次に Vulnerability サービスは、Red Hat の CVE データベースとセキュリティーボットに対してデータを評価し、システムに影響を与える可能性のある未処理の CVE があるかを判断し、これらの比較の結果を提供します。

データを分析したら、表示される結果を表示して並べ替えたり、脆弱性のリスクと優先順位の評価、ステータスの報告、Ansible Playbook の作成およびデプロイ、修復ができます。Vulnerability サービスの目的は、RHEL インフラストラクチャーのセキュリティーの脆弱性から保護する反復可能なプロセスを有効にすることです。

1.2. RED HAT HYBRID CLOUD CONSOLE の USER ACCESS 設定

User Access 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ユーザーを設定します。

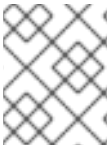
- ユーザーに個別にパーミッションを割り当てる代わりに、ロールを整理することで、ユーザーアクセスを制御します。
- ロールおよびそれらの対応する権限を含むグループを作成します。
- このグループにユーザーを割り当てることで、グループのロールに関連付けられたパーミッションを継承できるようになります。

1.2.1. 事前定義されたユーザーアクセスグループおよびロール

グループとロールの管理を容易にするため、Red Hat は事前定義された 2 つのグループと事前定義されたロールのセットを提供しています。

1.2.1.1. 事前定義されたグループ

Default access グループ には、組織内のすべてのユーザーが含まれます。事前定義されたロールの多くはこのグループに割り当てられます。これは Red Hat によって自動更新されます。



注記

組織管理者が **Default access** グループに変更を加えると、その名前が **Custom default access** グループに変更され、Red Hat では更新されなくなります。

Default admin access グループには、組織管理者のパーミッション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 に移動して、アカウント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ます。

1.2.1.2. グループに割り当てられた事前定義されたロール

Default access グループには、事前定義されたロールが多数含まれます。組織内の全ユーザーが **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たすべてのパーミッションは継承されます。

Default admin access グループには、更新および削除パーミッションを付与する多数の事前定義済みロールが含まれます（すべてではありません）。このグループのロールには、通常、名前に **administrator** が含まれます。

Hybrid Cloud Console で、Red Hat Hybrid Cloud Console > **Settings** アイコン(⚙)> Identity & Access Management > User Access > Roles に移動して、アカウント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。

1.2.2. アクセス権限

事前定義されたロールが持つ必要のあるパーミッションを提供する各手順一覧の **前提条件**。ユーザーとして、Red Hat Hybrid Cloud Console > **Settings** アイコン(⚙)> My User Access に移動して、現在継承されているロールとアプリケーションパーミッションを表示できます。

Insights for Red Hat Enterprise Linux 機能にアクセスしようとしたときに、このアクションを実行する権限がないというメッセージが表示される場合は、追加の権限を取得する必要があります。組織管理者または組織の User Access administrator により、これらのパーミッションが設定されます。

Red Hat Hybrid Cloud Console Virtual Assistant を使用して、Contact my Organization Administrator に問い合わせます。アシスタントは、お客様に代わって組織管理者にメールを送信します。

1.2.3. vulnerability-service ユーザーの User Access スロール

以下のロールにより、Insights for Red Hat Enterprise Linux の Vulnerability サービス機能への標準または拡張アクセスが有効になります。

- **Vulnerability ビューアー**: vulnerability-service リソースを読み取ります。
- **Vulnerability 管理者**: vulnerability-service リソースに対して利用可能な操作を実行します。

第2章 COMMON VULNERABILITIES AND EXPOSURES (CVE)

CVE は、公開されているソフトウェアパッケージで識別されているセキュリティーの脆弱性です。CVE は、Mitre Corporation が運用する連邦政府の調査および開発センターの「National CyberSecurity FFRDC (NCF)」で識別およびリスト表示され、National Cyber Security Division of the United States Department of Homeland Security から資金を得ています。CVE の全リストは、https://cve.mitre.org にあります。

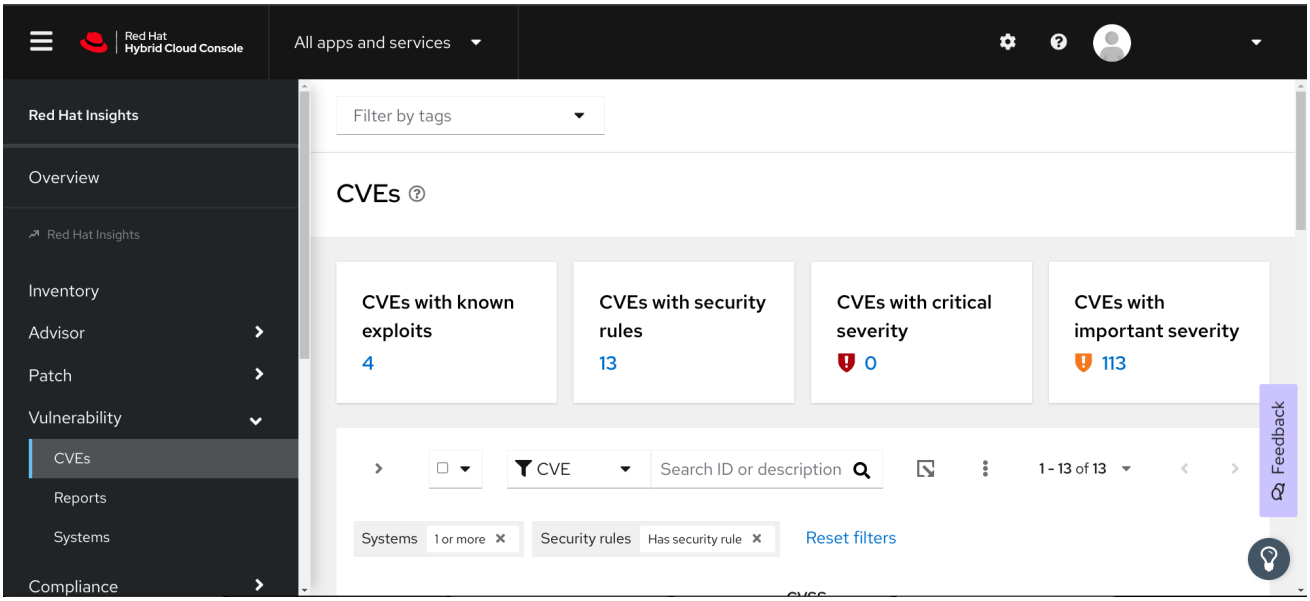
一般的に知られている不正使用の CVE や CVE に関連のあるセキュリティールールを強調表示することで、Vulnerability サービスは脅威インテリジェンスを強化し、RHEL 環境に最も影響を与える可能性のあるリスクをもたらす CVE を判断できるようにします。

重要

Vulnerability サービスには、https://cve.mitre.org のエントリーリストに含まれる CVE がすべて含まれるわけではありません。Red Hat CVE (Red Hat が 発行する セキュリティーアドバイザリー (RHSA)) のみが Vulnerability サービスに含まれています。

Vulnerability サービスは、RHEL システムに影響を与える CVE を特定し、重大度を示し、解決が最も重要な露出を効率的にトリアージできるようにします。ダッシュバーは、次の種類の CVE について警告します。

- 既知の不正使用
- セキュリティールール
- 重大度: Critical
- 重大度: Important

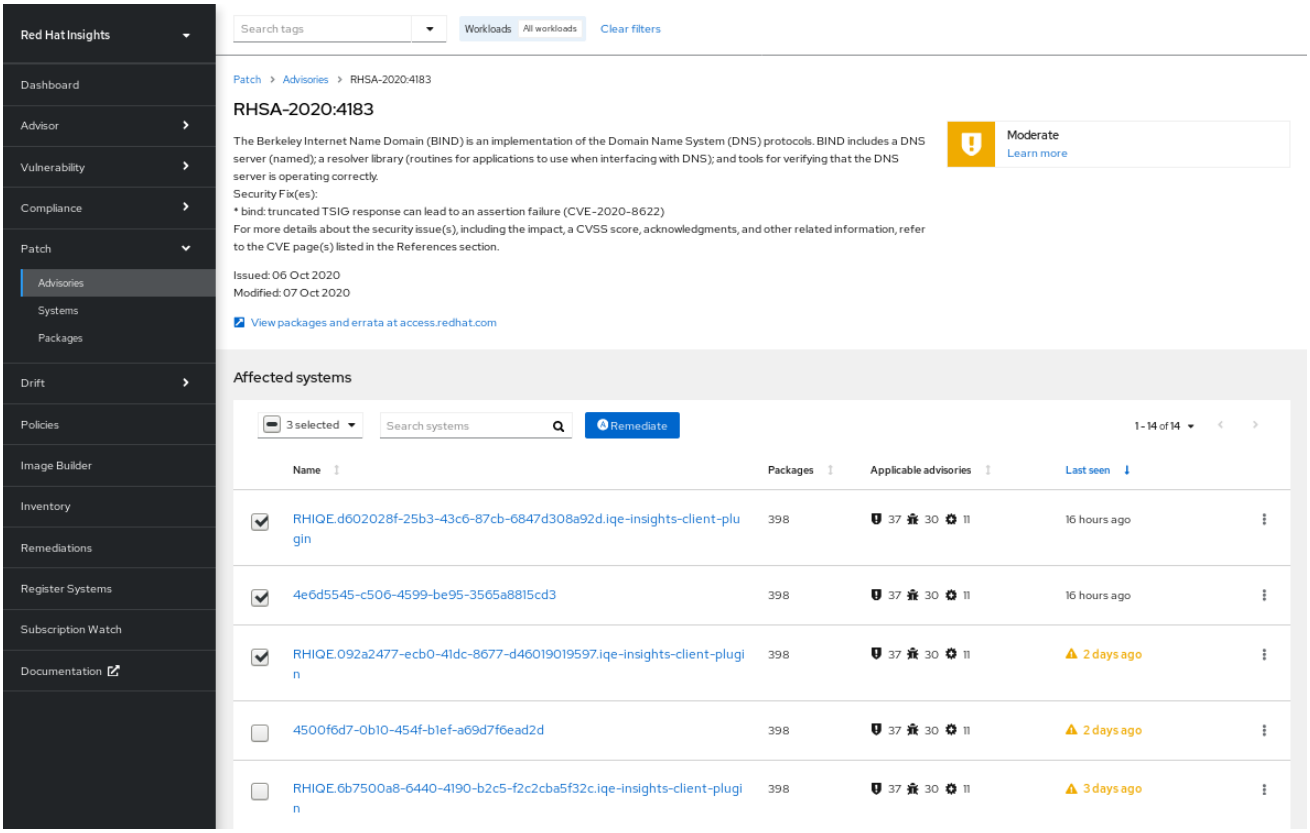


2.1. RED HAT SECURITY ADVISORY (RHSA)

Red Hat セキュリティーアドバイザリー (RHSA) のエラータでは、修正または軽減策が利用可能な Red Hat 製品のセキュリティー脆弱性が文書にまとめられています。Red Hat Insights for Red Hat Enterprise Linux の Vulnerability サービスは、CVE のリスクに晒されている各システムに紐付けられているアドバイザリー ID を表示します。

CVE を選び、セキュリティールールカードの **Filter by affected systems** のリンクを選択してこの情報を表示します。システムにアドバイザリーが存在する場合には、RHSA ID が **Exposed systems** リストの **Advisory** コラムで、システムの横にリンクとして表示されます。アドバイザリーがない場合は、Advisory 列が表示されなかったり、「Not available」と表示されます。

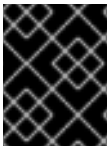
システムにアドバイザリーが存在する場合は、影響を受けるシステムのリストなど、RHSA に関する詳細情報を表示できます。Patch サービスでは、システムを選択し、Ansible Playbook を作成して修復を適用できます。



2.2. セキュリティールール

セキュリティールールは、リスクの割合が高いことや、CVE に関連するセキュリティーリスクが理由で、CVE が強調されています。これらは、重大なメディア報道を受ける可能性のあるセキュリティー上の欠陥であり、Red Hat Product Security チームによって精査され、Product Security Incident Response Plan ワークフローを使用して RHEL 環境の露出を判断するのに役立ちます。これらのセキュリティールールにより、組織を保護するための適切なアクションを実行できます。

セキュリティールールは、システムで実行している RHEL のバージョンを分析するだけにとどまらず、詳細にわたる脅威インテリジェンスを提供します。また、セキュリティールールは、Insights クライアントが収集するシステムメタデータを分析して、手動でキュレートされ、セキュリティーの脅威にさらされるかどうかを判断します。Vulnerability サービスにより、セキュリティールールのリスクに晒されるシステムが特定された場合には、セキュリティーリスクが高まる可能性があり、早急に問題を対処する必要があります。



重要

リスクに晒されているシステムでセキュリティールールに対応することが最優先事項です。

最後に、CVE に晒されているシステムすべてが、その CVE に関連するセキュリティールールのリスクに晒されているわけではありません。脆弱なバージョンのソフトウェアを実行している場合でも、他の環境条件により、特定のポートが閉じられたり、SELinux を実行している場合など、その他の環境状態

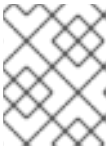
により脅威が緩和される可能性があります。

2.2.1. Insights for RHEL ダッシュボードでのセキュリティールールの特定

以下の手順に従って、インフラストラクチャーがセキュリティールールのリスクに晒されていることを確認します。

手順

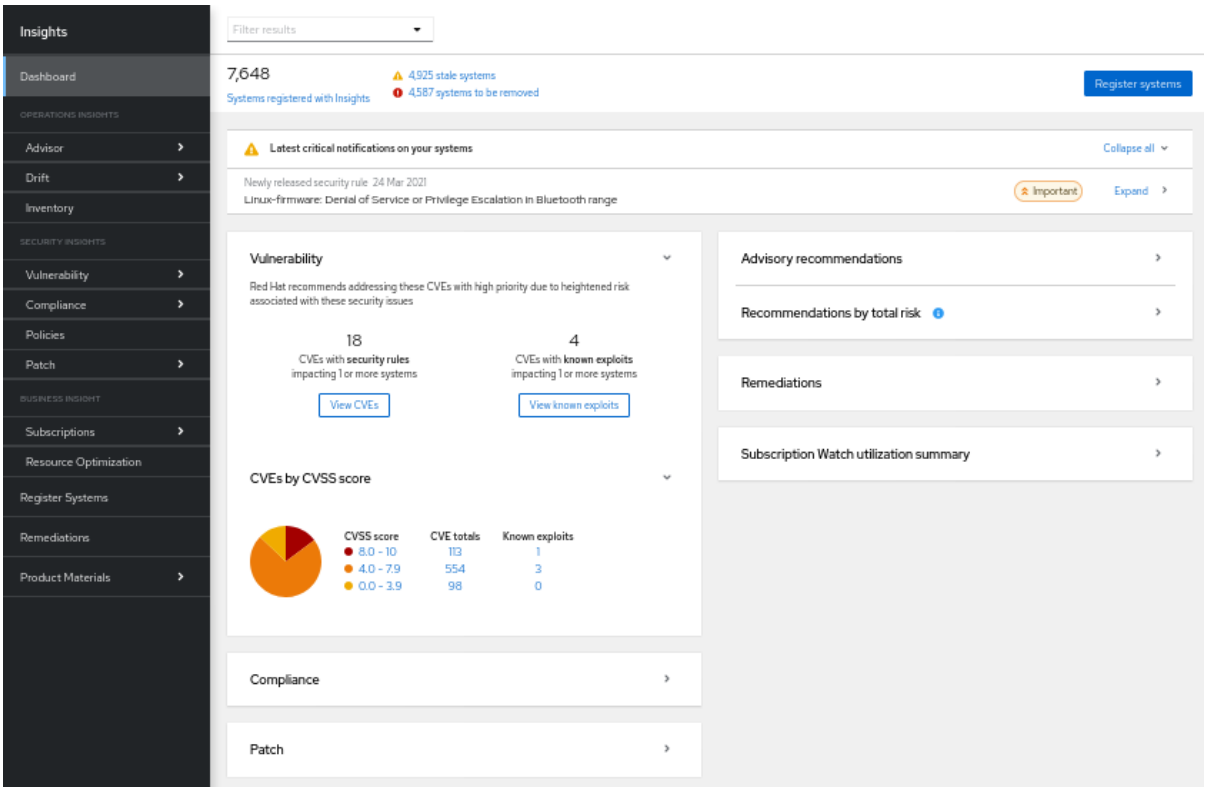
1. Red Hat Insights for Red Hat Enterprise Linux ダッシュボード に移動します。



注記

以下のスクリーンショットでは、セキュリティー脆弱性評価に関係のないサービスのパネルは最小化して簡潔にまとめています。

:



2. システムパネルで **最新の重要な通知** を確認します。これらは、セキュリティーリスクが高い「Important」または「Critical」と評価したセキュリティールールです。これらは最も重大な問題となる可能性があるため、修復を優先する必要があります。

   a. 各通知の右側にある **デプロイメント** ボタンをクリックして、関連する CVE およびインフラストラクチャーでセキュリティー上の問題点が含まれるシステムの数を表示します。

注記

重要な通知にセキュリティールールが表示されているにも関わらず、セキュリティーリスクのあるシステムが 0 の場合があります。この場合、CVE がインフラストラクチャーに存在しても、セキュリティールールの条件が存在しない場合もあります。

b. セキュリティールールの名前と関連する CVE の下にある CVE ID リンクをクリックします。

c. セキュリティールール CVE の影響を受けるシステムを表示し、任意でセキュリティーリスクに晒されたシステムを選択して Playbook を作成します。

3. 次に、**Vulnerability** カードに情報を表示します。

a. システムに影響のある **セキュリティールール** が割り当てられた CVE の数を書き留めます。この数字には、重大度に関係なく、システム 1 台以上に影響のあるセキュリティールールが含まれます。

i. **View CVEs** をクリックします。重大度の低いセキュリティールールの修復の優先順位は、重大度の高いセキュリティールールの次にするように検討します。

2.3. 既知の不正使用

Red Hat は Metasploit データを分析して、CVE を悪用するコードが公開されているか、また CVE が一般的に悪用されていないかを判断します。Vulnerability サービスは、対象基準を満たす CVE に「既知の不正使用」ラベルを適用します。

脅威評価がこのように強化されることで、極めてリスクの高い CVE を特定して先に対処できるようになります。Red Hat は、「既知の不正使用」ラベルの CVE を最優先ですべて確認し、これらの問題の修正に向けて取り組むことを推奨します。

重要

Vulnerability サービスで、悪用されていることが分かっている CVE がお使いのインフラストラクチャーのシステムに存在することが分かります。「既知の不正使用」のラベルは、RHEL システムで脆弱性の悪用が行われていることを示すわけではありません。Vulnerability サービスでは、そのような判断はされません。

2.4. COMMON VULNERABILITIES AND EXPOSURES は、トリアージ機能を備えた詳細な脅威インテリジェンスを提供します

Vulnerability サービスは、個々の Common Vulnerabilities and Exposures (CVE) と、Insights に登録されたシステムへの影響に関するデータを提供します。CVE は、**脆弱** または **影響を受けるが脆弱ではないものとして分類されます。**このレベルの脅威インテリジェンスは、**Security Rule** ラベルを持つ CVE、または Red Hat Product Security の厳密な分析を経た CVE で利用できます。

この強化された脅威インテリジェンスにより、問題をトリアージし、最も緊急性の高い問題に最初に対処することができます。大規模なサーバー群を管理する場合、これは迅速な保護と大幅な効率化につながります。

影響を受けているが脆弱ではない CVE ステータスは、脆弱性があるが現在悪用できないソフトウェアを実行していることを示します。このシステムには修復が必要ですが、すぐに対処する必要はありません。

脆弱な CVE ステータスは、コードに欠陥があり、悪用へのパスが開いていることを示します。オープンパスは、次のいずれかを許可するポートまたは OS バージョンである可能性があります: 機密情報の漏えい、システムの整合性の侵害、またはシステムの可用性の妨害。

脆弱な サーバーと、**影響を受けるが脆弱ではない** サーバーの例を見てみましょう。

サーバー A が、システムへの root アクセスを許可する脆弱なソフトウェアを実行しているとします。**サーバー A** は脆弱であると見なされ、すぐにパッチを適用する必要があります。

対照的に、**サーバー B** の現在の設定では、影響を受けるコードに脆弱性が存在する場合でも、脆弱性が顕在化しないとします。**サーバー B** は **影響を受けると見なされますが、脆弱ではありません**。これは、**サーバー B** が to-do リストに追いやられ、より差し迫った脅威である **サーバー A** を修復できることを意味します。

重要

サーバー B は潜在的に脆弱なコードを実行しているため、**サーバー A** に対処し次第、**サーバー B** にパッチを適用する必要があります。バージョンの更新やその他のイベントにより、将来脆弱になる可能性があります。

2.4.1. Red Hat Insights for RHEL ダッシュボードで既知の不正使用 CVE を特定する

次の手順を使用して、Insights for Red Hat Enterprise Linux ダッシュボードの脆弱性カードで既知のエクスプロイト CVE を特定します。

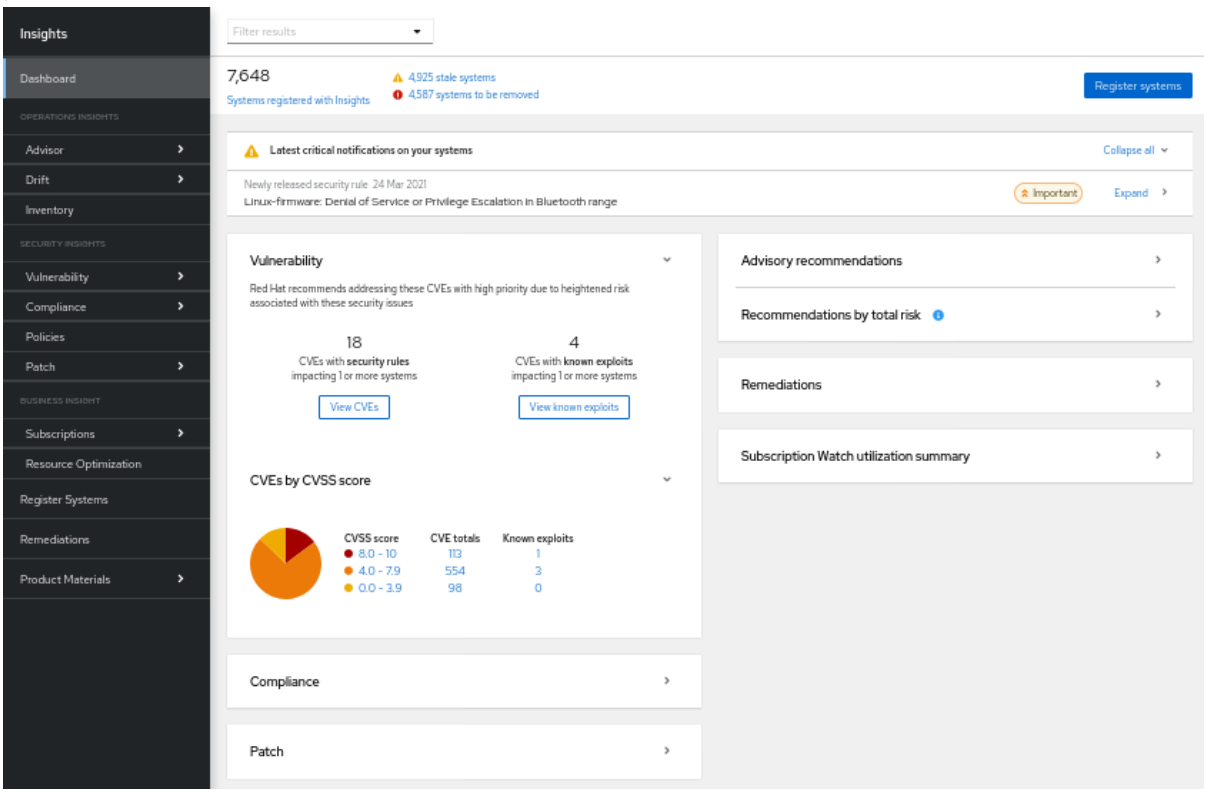
手順

1. Red Hat Insights for Red Hat Enterprise Linux ダッシュボード に移動します。

注記

以下のスクリーンショットでは、セキュリティー脆弱性評価に関係のないサービスのパネルは最小化して簡潔にまとめています。

:



2. **Vulnerability** カードで、**1台以上のシステムに影響を与える不正使用されている CVE と表示されている数** を書き留めます。

3. **View Known exploits** をクリックします。

4. CVE 一覧で、不正使用されていることが分かっている CVE がフィルタリングされたリストを確認します。

第3章 VULNERABILITY-SERVICE の結果調整

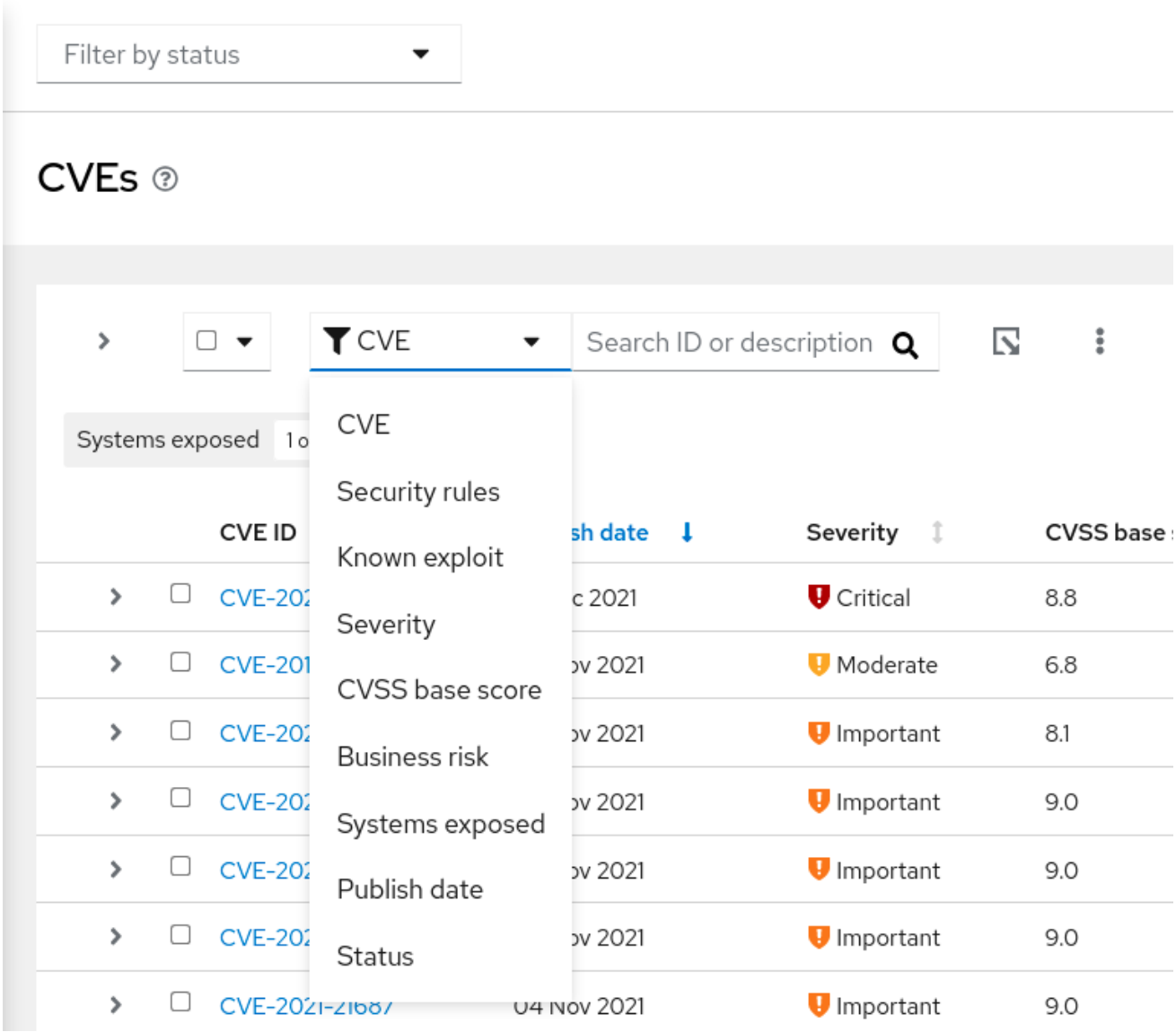
結果をステークホルダーに報告する場合も、システム修復の優先順位を決定する場合でも、Vulnerability サービスでは、データのビューを細かく調整し、最も重要なシステム、ワークロードまたは問題にフォーカスできるようにする方法が多数あります。以下のセクションでは、データの編成、および結果を絞り込むために使用できるソート、フィルタリング、およびコンテキスト機能について説明します。

3.1. CVE-LIST フィルターおよび SYSTEM-LIST フィルター

フィルタリングにより、CVE および関連システムの表示リストが絞り込まれるため、特定の問題にフォーカスしやすくなります。CVE リストにフィルターを適用して、重大度やビジネスリスクに応じて CVE にフォーカスします。以下に例を示します。個々の CVE を選択した後、影響を受けるシステムの結果リストにフィルターを適用して、たとえば、特定の 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に焦点を合わせます。

フィルターは、左側のフィルターのドロップダウンリストからプライマリーフィルターを選択し、右側のフィルターオプションのドロップダウンリストからセカンダリーサブフィルターを選択してアクティベートされます。選択したフィルターはフィルターメニューに表示され、各フィルターの横にある X をクリックしてフィルタリングを解除できます。

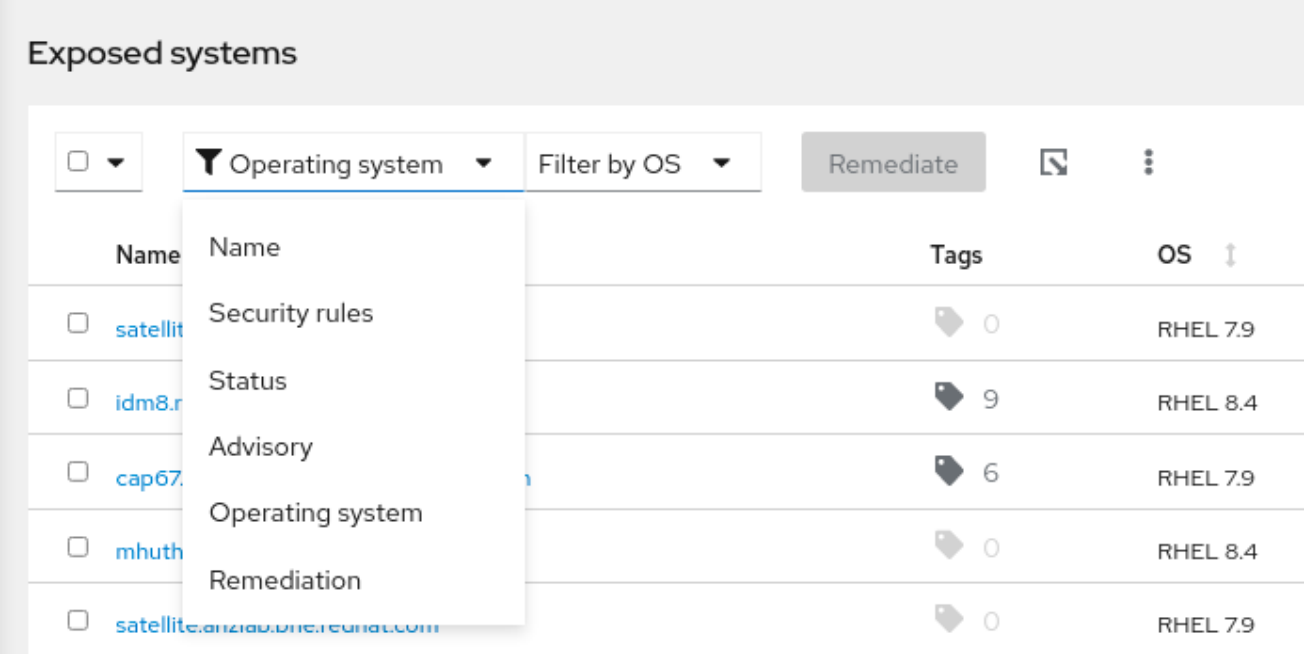
CVE リストのフィルター



以下の主要フィルターは、CVEs ページからアクセスできます。プライマリーフィルターを選択し、サブフィルターにパラメーターを定義します。

- **CVE。** ID または説明を検索します。
- **セキュリティールール。** Security rule ラベルの付いた CVE のみを表示します。
- **既知の不正使用。** Known exploit ラベルの付いた CVE のみを表示します。
- **セキュリティー。** 1 つ以上の値 (Critical、Important、Moderate、Low、または Unknown) を選択します。
- **CVSS ベーススコア。** All、0.0-3.9、4.0-7.9、8.0-10.0、N/A (該当なし) から、1 つまたは複数の範囲を選択します。
- **ビジネスリスク。** 1 つ以上の値を選択します (High、Medium、Low、Not defined)。
- **無防備なシステム。** 現在影響を受けるシステムがある CVE だけを表示するか、影響を受けるシステムがない CVE のみを表示するよう選択します。
- **公開日。** 以下から選択します (All、Last 7 days、Last 30 days、Last 90 days、Last year、More than 1 year)。
- **状態。** Not reviewed、In review、On-hold、Scheduled for patch、Resolved、No action - risk accepted, Resolved via mitigation から、1 つまたは複数の値を選択します。

システムリストフィルター



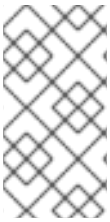
CVE の詳細ページのシステムリストから、以下のプライマリーフィルターにアクセスできます。

- **名前。** CVE ID を入力して、特定の CVE を検索します。
- **セキュリティールール。** CVE にそれに関連するセキュリティールールがある場合は、同じセキュリティールールに対して脆弱な他のシステムでフィルターするか、セキュリティールールの影響を受けるシステムを表示します。
- **状態。** 特定のステータスまたはワークフローカテゴリーのシステムを表示します。

- **アドバイザリー。**この CVE に Red Hat アドバイザリーが適用されるシステムを表示します。
- **Operating system**特定の RHEL (マイナー) バージョンを実行しているシステムを表示します。
- **修正。**Ansible Playbook に含まれるシステム、手動による修復、または現在の修復計画に含まれていないシステムを表示します。

3.1.1. セキュリティールールの CVE のフィルター

セキュリティールール (特に重大度の高いセキュリティールールなど) は、お使いのインフラストラクチャーに非常に大きな脅威となる可能性があり、リスクの特定および修復の優先順位を 1 番として考える必要があります。以下の手順に従い、CVE リストで重大度の高いセキュリティールール CVE だけを表示して影響を受けるシステムを特定します。



注記

CVE に晒されているシステムすべてが、その CVE に関連するセキュリティールールのリスクに晒されているわけではありません。脆弱なバージョンのソフトウェアを実行している場合でも、他の環境条件により、特定のポートが閉じられたり、SELinux が有効な場合など、その他の環境状態により脅威が緩和される可能性があります。

手順

1. Red Hat Insights for Red Hat Enterprise Linux で Security > Vulnerability > CVEs に移動します。
2. ツールバーでフィルタードロップダウンリストをクリックします。
   a. **Security rules** フィルターを適用します。
   b. **Has security rule** のサブフィルターを適用します。
3. 下方向にスクロールしてセキュリティールールの CVE を表示します。セキュリティールールのある CVE では、CVE ID のすぐ下にあるセキュリティールールラベルを表示します。

3.1.2. RHEL システムのセキュリティールールによる脆弱性の修復

セキュリティールールのある CVE とは、システムへのリスクが高い問題に重点を置いた Red Hat が優先する CVE です。これらの問題を修復することで、組織にとって最も重要な問題を優先するセキュリティー体制をサポートできます。Vulnerability サービスと修復サービスを使用すると、次の方法でシステムに対する最も重要な脅威の一部に優先順位を付け、修復できます。

- セキュリティールールのある CVE に焦点を当てます。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 セキュリティールールのリスクにさらされ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。
- CVE の修復CVE の修復に関する詳細は、**Red Hat Insights 修復ガイド**を参照してください。

3.1.3. 既知の不正使用 CVE のフィルタリング

「既知の不正使用」のラベルが付いた CVE で、Red Hat は、CVE を悪用するコードが公開されているか、不正使用が行われたと一般的に知られているかなど、不正使用が行われているかどうかを判断します。このような理由から、不正使用されていることが分かっている CVE は、優先的に特定と修復を図る必要があります。

重要

Red Hat では、登録されているシステムが悪用されているかどうかの判断は行いません。重大なリスクを伴う可能性がある CVE を特定するだけです。

以下の手順に従って、CVE リストから不正使用されていることが分かっている CVE をフィルタリングします。

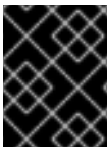
手順

1. Red Hat Insights for Red Hat Enterprise Linux で Security > Vulnerability > CVEs に移動します。
2. ツールバーでフィルタードロップダウンリストをクリックします。
   a. **Known exploit** フィルターを適用します。
   b. **Has a known exploit** サブフィルターを適用します。
3. スクロールダウンして、既知の不正使用 CVE のリストを表示します。

3.1.4. 関連するアドバイザリーのない CVE のフィルタリング

CVE によっては、関連するアドバイザリー (**エラータ** とも呼ばれます) がないものもあります。これは、次のいずれかの理由で発生する可能性があります。

- CVE に利用できる修正がない。
- 製品セキュリティー分析により、CVE がご利用の環境に影響を与えると判断されたものの、ご利用の環境で使用できるエラータがない (ただし、他の環境であれば、同じ CVE のエラータを使用できる可能性があります)。
- お使いのシステムがサポート対象外である。



重要

CVE 情報は現在、RHEL 6、7、8、および 9 で利用できます。同情報は RHEL 5 システムでは利用できません。

アドバイザリーのない CVE を特定できれば、それらの脆弱性に関連するリスクから組織を保護するための措置を講じることができ、問題に対処するために必要な手順を実施できます。

ご利用の RHEL バージョンに利用可能な修正がなく、“Will not fix” に分類されている場合は、次の基準を考慮してください。

- 脆弱性の影響 (重大度)
- お使いの RHEL バージョンのライフサイクルフェーズ

関連するアドバイザリーがない CVE に修正が必要であると判断した場合は、次の選択肢があります。

- リスクを受け入れる。
- 利用可能な場合は、脆弱性の修正が含まれる、サポート対象の製品バージョンにアップグレードする (推奨)。

- 軽減策を適用する (軽減策がある場合)。

関連情報

CVE の詳細は、Common Vulnerabilities and Exposures を参照してください。

脆弱性の重大度評価の詳細は、Understanding severity ratings を参照してください。

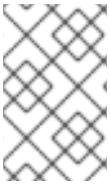
製品のライフサイクルの詳細は、Life cycle and update policies を参照してください。

カスタマーポータルでサポートケースを作成するには、Customer support を参照してください。

3.1.4.1. アドバイザリーのない CVE の有効化

アドバイザリーのない CVE を有効にすると、Insights で、アドバイザリーのない CVE の影響を受けるシステムにアクセスできるようになります。

この機能はデフォルトで有効になっていますが、メインビューではアドバイザリーのない CVE がデフォルトで非表示になります。そのため、アドバイザリーのない CVE を表示して確認するには、フィルターを使用する必要があります。



注記

Red Hat のポリシーでは、CVE に関連するアドバイザリーがあるかどうかに関係なく、Insights for Red Hat Enterprise Linux で高優先度、重大、および重要な CVE をすべて表示することを要求しています。

前提条件

- Red Hat Insights の環境への Vulnerability administrator アクセス権を持っている。

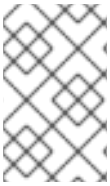
手順

1. Red Hat Insights for RHEL ダッシュボードから、**Security > Vulnerability > CVEs**に移動します。
2. **More options** アイコン (⋮) をクリックし、**Show CVEs without Advisories** を選択します。アドバイザリーのリストに、アドバイザリーのない CVE も含まれるようになります。

3.1.4.2. アドバイザリーのない CVE の無効化

アドバイザリーのない CVE 機能を無効にするには、**Show CVEs without Advisories**オプションの選択を解除します。

アドバイザリーのない CVE のオプションはデフォルトで有効になっていますが、デフォルトのビューではアドバイザリーのない CVE が非表示になります。



注記

Red Hat のポリシーでは、CVE に関連するアドバイザリーがあるかどうかに関係なく、Insights for Red Hat Enterprise Linux で高優先度、重大、および重要な CVE をすべて表示することを要求しています。

前提条件

- Red Hat Insights の環境への Vulnerability administrator アクセス権を持っている。
- アドバイザリーのリストに、アドバイザリーのない CVE が含まれている。

手順

1. Red Hat Insights for RHEL ダッシュボードから、**Security > Vulnerability > CVEs**に移動します。
2. **More options** アイコン (⋮) をクリックし、 **Hide CVEs without Advisories** を選択します。

3.1.4.3. アドバイザリーのない CVE の表示

Show CVEs without Advisories オプションで、アドバイザリーのない CVE を有効または無効にします。アドバイザリーのない CVE を表示するには、Show CVEs without Advisories オプションを有効にする必要があります。

前提条件

- 組織管理者がアドバイザリーのない CVE のオプションを有効にしている。

手順

1. Red Hat Insights for RHEL ダッシュボードから、**Security > Vulnerability > CVEs**に移動します。
2. フィルターのドロップダウンから、**Advisory** を選択します。
3. **Filter by Advisory** ドロップダウンから、**Not Available** を選択します。アドバイザリーのリストに、アドバイザリーのないすべての CVE が表示されます。

3.1.4.4. アドバイザリーのない CVE の影響を受けるシステムの特定

CVE の詳細ページには、選択した CVE の影響を受けるすべてのシステムのリストが表示されます。システムのリストをフィルタリングして、アドバイザリーのない CVE の影響を受けるシステムを表示できます。

前提条件

- 組織管理者がアドバイザリーのない CVE のオプションを有効にしている。

手順

1. CVE の影響を受けるシステムを確認するために、アドバイザリーのない CVE を特定します。アドバイザリーのない CVE を特定する方法の詳細は、「アドバイザリーのない CVE があるシステムの特定」を参照してください。
2. 特定した CVE を選択して、CVE の詳細ページに移動します。その CVE の CVE 詳細ページが表示されます。このページには、その CVE の影響を受けるすべてのシステムがリストされます。
    a. CVE を選択するときに **Filter by Advisory** および **Available** オプションを適用した場合は、これらのフィルターが CVE の詳細ページにも適用されます。
    b. そうでない場合は、CVE の詳細ページに移動するときに、ページの上部にあるフィルター

から **Advisory** を選択し、**Filter by Advisory** を選択して、**Not Available** チェックボックスをクリックします。システムのリストが更新され、アドバイザリーのない当該 CVE の影響を受けるシステムだけが表示されます。**Advisory** 列には、リスト内の各システムについて **Not Available** と表示されます。

3. **オプション:** システムの詳細を表示するには、表示するシステムの名前を選択します。システムの詳細ページが表示されます。

3.1.4.5. システムの詳細におけるアドバイザリーのない CVE の表示

システムの詳細ページには、選択したシステムに影響を与える全 CVE のリストが表示されます。CVE のリストをフィルタリングして、アドバイザリーのない CVE を表示できます。

前提条件

- 組織管理者がアドバイザリーのない CVE のオプションを有効にしている。

手順

1. Red Hat Insights for RHEL ダッシュボードから、**Security > Vulnerability > Systems**に移動します。Vulnerability systems ページが表示されます。
2. リストからシステム ID を選択します。そのシステムのシステム詳細ページが表示されます。このページには、選択したシステムに影響を与えるすべての CVE がリスト表示されます。
3. ページ上部のフィルターから **Advisory** を選択します。
4. **Filter by Advisory** を選択し、**Not Available** チェックボックスをオンにします。CVE のリストが更新され、アドバイザリーのない CVE のみが表示されます。Advisory 列には、リスト内の各 CVE について **Not Available** と表示されます。
5. **オプション:** CVE の詳細を表示するには、表示する CVE の CVE ID を選択します。CVE の詳細ページが表示されます。

3.2. 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

CVE リストをフィルタリングし、最も重大な脅威だけを表示した後に、個別の CVE を選択して、セキュリティーリスクに晒されたシステムリストを表示して、そのリストにフィルターを適用します。

手順

1. Security-rule CVE を選択したら、**Exposed systems** リストまで下方向にスクロールします。リストに含まれるシステムすべてに、CVE がセキュリティールールに追加される、セキュリティールールの条件が含まれるわけではありません。以下のフィルターを適用して、セキュリティールール条件のあるシステムのみを表示します。
2. プライマリーフィルターのドロップダウンリストから **Security rules** フィルターを選択します。
3. セカンダリードロップダウンリストの **Has security rule** ボックスにチェックを入れます。
4. セキュリティールールにも条件が存在する CVE に晒されているシステムを表示します。

3.3. INSIGHTS FOR RHEL グループフィルター

システムやワークロードのグループ別に Vulnerability サービスの結果をフィルタリングする機能を使用すると、特定のグループに所属するとのタグが付いたシステムだけを表示できます。これらは、Satellite ホストグループ、または Insights クライアント設定ファイルに追加されたカスタムタにより SAP ワークロード (または SAP ID) を実行しているシステムが考えられます。

グループフィルタリングは、Insights for Red Hat Enterprise Linux アプリケーション全体のページ上部にある **フィルター結果** ボックスを使用して、Insights for Red Hat Enterprise Linux でグローバルに設定できます。サービスやページが変わっても、グループの選択項目は維持されます。ただし、機能は、さまざまな Insights for Red Hat Enterprise Linux サービス内で異なります。

グループのフィルタリングは、Vulnerability ダッシュボードと Vulnerability サービスの CVE およびシステムリストで機能します。

本書の **タグおよびシステムグループ** のセクションでは、グループタグや、カスタムタグの設定について説明します。

3.3.1. グループ別のダッシュボード、CVE、およびシステムリストのフィルタリング

以下の手順に従って、グループ別に Vulnerability サービスの CVE およびシステムのリストを絞り込みます。

手順

1. Red Hat Hybrid Cloud Console に移動し、ログインします。
2. Red Hat Insights for Red Hat Enterprise Linux アプリケーションを開きます。
3. Insights アプリケーションのページの上部にある **Filter results** ボックスの下矢印をクリックします。
4. システムのフィルタリングに使用するグループを選択します。
   検索またはスクロールして、利用可能なタグを表示します。利用可能なタグの全リストを確認するには、リストの下部までスクロールし、**View more** をクリックします。

   任意:

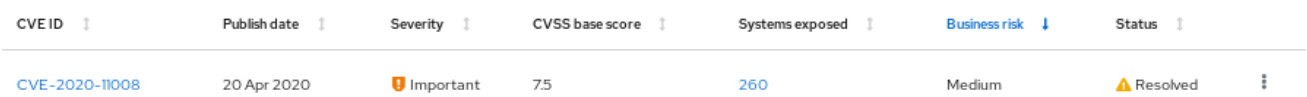
   a. SAP ワークロードを選択します。
   b. 特定の SAP ID でシステムを選択します。
   c. Satellite ホストコレクションを選択します。
   d. カスタムグループタグで識別されるシステムを選択します。
      カスタムタグの作成方法は、本書の「**カスタムのシステムタグ付け**」を参照してください。
5. サービスに移動し、選択したグループに所属するシステムまたは CVE のみを表示します。

3.4. CVE のビジネスリスクの定義

Vulnerability サービスでは、CVE のビジネスリスクを、High、Medium、Low、または Not Defined (デフォルト) などのオプションで定義できます。

CVE のリストでは各 CVE の重大度を示していますが、ビジネスリスクを割り当てることで、組織に与える可能性のある影響に基づいて CVE をランク付けできます。これにより、大規模な環境でリスクを効率的に管理し、運用上の意思決定を改善できます。

デフォルトでは、特定の CVE のビジネスリスクフィールドは **Not Defined** に設定されます。ビジネスリスクを設定したら、CVE 行の Security > Vulnerability > CVEs 一覧に表示されます。



また、各 CVE の詳細カードにビジネスリスクが表示されます。これには、より多くの情報が表示され、影響を受けるシステムがリスト表示されます。

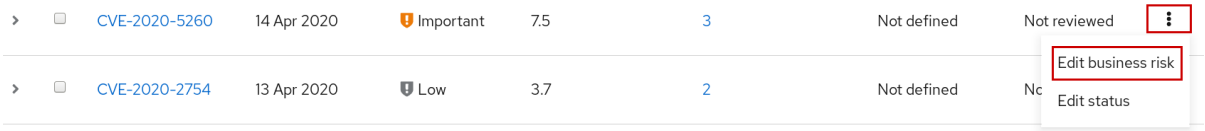
3.4.1. 単一の CVE のビジネスリスクの設定

単一の CVE にビジネスリスクを設定するには、以下の手順を実施します。

注記

CVE のビジネスリスクは、影響を受ける**すべて**のシステムで同じになります。

1. 必要に応じて Security > Vulnerability > CVEs ページに移動し、ログインします。
2. ビジネスリスクを設定する CVE を特定します。
3. CVE 行の右側にある **more-actions** アイコン (垂直ドット) をクリックし、**Edit business risk** をクリックします。



4. ビジネスリスクの値を適切なレベルに設定し、必要に応じてリスク評価の証明を追加します。
5. **Save** をクリックします。

3.4.2. 複数の CVE のビジネスリスクの設定

以下の手順に従い、選択する複数の CVE に同じビジネスリスクを設定します。

1. Security > Vulnerability > CVEs に移動し、必要に応じてログインします。
2. ビジネスリスクを設定する CVE のボックスにチェックを入れます。
3. ビジネスリスクを設定するには、以下の手順を実行します。

a. ツールバーで Filter ドロップダウンメニューの右側にある **more-actions** (3 つの垂直ドット) をクリックし、**Edit business risk** をクリックします。

b. 適切なビジネスリスク値を設定し、必要に応じてリスク評価の理由を追加します。

c. **Save** をクリックします。

3.5. VULNERABILITY サービス分析からのシステムの除外

Vulnerability サービスを使用すると、特定のシステムを脆弱性分析から除外することができます。除外することで、組織の目標と関連せのないシステムで問題を確認、再確認する時間と労力を軽減できます。

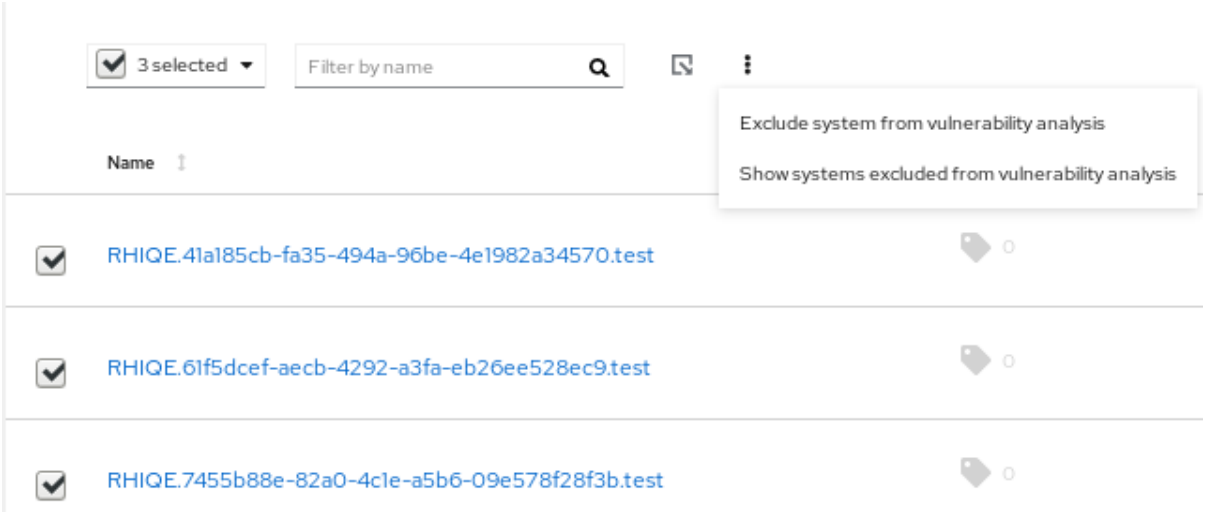
たとえば、QA、Dev、および Production というサーバーのカテゴリーがあり、QA サーバーの脆弱性を確認する必要がない場合は、Vulnerability サービスの分析対象からこれらのシステムを除外できます。

脆弱性分析からシステムを除外すると、Insights クライアントはシステム上のスケジュールに従ってそのまま実行されますが、システムの結果は Vulnerability サービスには表示されません。クライアントがそのまま稼働されるので、他の Red Hat Insights for Red Hat Enterprise Linux サービスで必要なデータをアップロードできます。また、フィルターを使用してこれらのシステムの結果を確認することもできます。

選択した RHEL システムをVulnerability サービスの分析から除外するには、以下の手順を実行します。

手順

1. Security > Vulnerability > Systems タブに移動し、必要に応じてログインします。
2. 脆弱性分析から除外する各システムのボックスにチェックを入れます。
3. システムのリストの上部のツールバーにある **more-actions** アイコンをクリックし、**脆弱性分析からシステムの除外** を選択します。



4. 任意で、**システムの行** の more-actions アイコンをクリックし、**脆弱性分析からシステムの除外** を選択して、**単一** のシステムを除外できます。

3.6. 以前に除外したシステムの表示

以前に除外したシステムを表示するには、以下の手順を実行します。

手順

1. Security > Vulnerability > Systems タブに移動し、必要に応じてログインします。
2. システムのリストの上部にあるツールバーにある **more-actions** アイコンをクリックし、**Show systems excluded from analysis** を選択します。
3. 脆弱性分析から除外されたシステムを参照してください。これは、**Applicable CVEs** 行の **Excluded** の値で検証できます。

3.7. システムの脆弱性分析の再開

システムの脆弱性分析を再開するには、以下の手順を実行します。

手順

1. Security > Vulnerability > Systems タブに移動し、必要に応じてログインします。
2. システムのリストの上部にあるツールバーにある **more-actions** アイコンをクリックし、**Show systems excluded from analysis** を選択します。
3. 結果のリストで、脆弱性分析を再開する各システムのボックスにチェックを入れます。
4. **その他のアクション** アイコンを再度クリックし、**Resume analysis for system**を選択します。

3.8. CVE ステータス

システムに影響を与える CVE を管理する方法として他に、CVE のステータスを設定することが挙げられます。Vulnerability サービスを使用すると、以下の方法で CVE のステータスを設定できます。

- **全** システムに CVE のステータスを設定します。
- **特定の CVE + システムペア** のステータスを設定します。

ステータス値は事前設定されており、以下のオプションが含まれます。

- Not reviewed (デフォルト)
- In-review
- On-hold
- Scheduled for patch
- Resolved
- No action - risk accepted
- Resolved via mitigation

CVE のステータスを設定すると、ライフサイクルによる順序づけが、順序の認識から変更までにわたり容易になります。ステータスを定義すると、組織は、ライフサイクル内のどの部分で重大度の最も高い

CVE が存在するのか、またビジネスのニーズに合わせて最も重要な問題への対処に焦点を合わせる必要がある状況について、より効果的に監視できます。CVE のステータスは、Vulnerability サービスおよび個別の CVE ビューの全 CVE テーブルに表示されます。

3.8.1. 影響を受ける全システムの CVE のステータス設定

以下の手順を完了して CVE のステータスを設定し、影響を受けるすべてのシステムでそのステータスが CVE に適用されるようにします。

手順

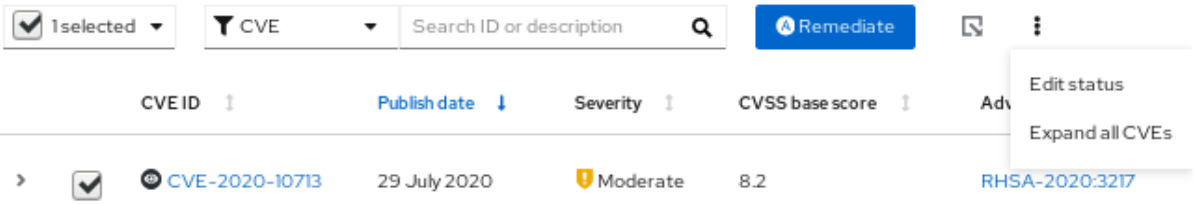
1. Security > Vulnerability > CVEs タブに移動し、必要に応じてログインします。
2. CVE 行の右側にある **more-actions** アイコンをクリックし、**Edit status** を選択します。
3. 適切なステータスを選択し、必要に応じて、**Justification** テキストボックスに決定の絞り込みを入力します。
4. 個別のシステムにこの CVE に設定されたステータスがあり、これを保持する場合は、**個別のシステムステータスを上書きしない** にチェックを入れます。そうでない場合は、チェックボックスのチェックを外して、このステータスを、影響を受けるすべてのシステムに適用します。
5. **Save** をクリックします。

3.8.2. CVE およびシステムペアのステータスの設定

CVE とシステムのペアのステータスを設定するには、以下の手順を実行します。

手順

1. Security > Vulnerability > Systems タブに移動し、必要に応じてログインします。
2. システムを特定し、システム名をクリックして開きます。
3. リストから CVE を選択し、CVE ID の横にあるチェックボックスにチェックを付けます。
4. ツールバー内の **more-option** アイコンをクリックし、**Edit status** を選択します。



5. ポップアップカードで、以下のアクションを実行します。
   a. CVE およびシステムペアのステータスを設定します。

注記

Use overall CVE status ボックスにチェックマークを入れると、ペアのステータスを設定することはできません。

   b. 必要に応じて、ステータス決定の根拠を入力します。

c. **Save** をクリックします。

6. リストで CVE を見つけ、ステータスが設定されていることを確認します。

3.9. 検索ボックスの使用

Vulnerability サービスの検索機能は、表示中のページのコンテキストで機能します。

- **CVE ページ。**検索ボックスは、CVE リストの上部にあるツールバーにあります。CVE フィルターが設定されている場合は、CVE ID と説明を検索します。

- **Systems page.**検索ボックスは、リストの上部にあるツールバーにあります。システム名または UUID を検索します。

3.10. CVE リストデータのソート

Vulnerability サービスのソート機能は、表示ページのコンテキストにより異なります。

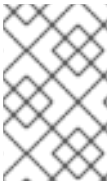
手順

1. **CVEs タブ** では、以下の列にソートを適用できます。
   - CVE ID
   - Publish date
   - Severity
   - CVSS base score
   - Systems exposed
   - Business risk
   - Status
2. **System タブ** では、以下のコラムをソートできます。
   - Name
   - Applicable CVEs
   - Last seen
3. Systems タブでシステムを選択すると、システム固有の CVE のリストでは、以下のソートオプションを使用できます。
   - CVE ID

- Publish date
- Impact
- CVSS base score
- Business risk
- Status

第4章 システムタグとグループ

Red Hat Insights for Red Hat Enterprise Linux を使用すると、管理者はグループタグを使用して、インベントリー内のシステムや個々のサービスでシステムのグループをフィルターできます。グループは、Insights for Red Hat Enterprise Linux へのシステムデータの取り込み方法によって識別されます。Insights for RHEL を使用すると、SAP ワークロードを実行しているシステム、Satellite ホストグループ、Microsoft SQL Server ワークロード、およびルートアクセス権を持つシステム管理者がシステムで Insights クライアントを設定するために定義したカスタムタグによって、システムのグループをフィルタリングできます。



注記

2022 年 春の時点で、インベントリー、アドバイザー、コンプライアンス、脆弱性、パッチ、ドリフト、およびポリシーで、グループとタグによるフィルタリングが有効になります。その他のサービスは後から続きます。

重要

タグ付けを有効にする他のサービスとは異なり、コンプライアンスサービスは、コンプライアンスサービス UI のシステムのリスト内にタグを設定します。詳細は、次のセクション **コンプライアンスサービスのグループフィルターとタグフィルター** を参照してください。

グローバルな **フィルター結果** ボックスを使用して、SAP ワークロード、Satellite ホストグループ、MS SQL Server ワークロード、または Insights クライアント設定ファイルに追加されたカスタムタグでフィルター処理します。

前提条件

Red Hat Insights for Red Hat Enterprise Linux のタグ付け機能を使用するには、以下の前提条件および条件を満たしている必要があります。

- Red Hat Insights クライアントが各システムにインストールされている。
- カスタムタグを作成したり、**/etc/insights-client/tags.yaml** ファイルを変更したりするには、ルート権限、または同等の権限が必要です。

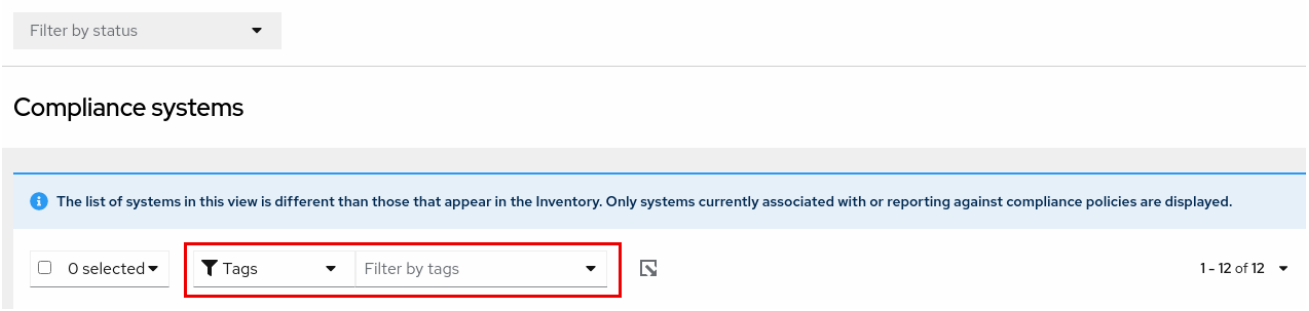
4.1. コンプライアンスサービスのグループおよびタグフィルター

コンプライアンスサービスを使用すると、ユーザーは、コンプライアンスデータを報告するシステムにタグおよびグループフィルターを適用できます。ただし、**Filter by status** ドロップダウンを使用して設定することはできません。Insights for Red Hat Enterprise Linux アプリケーションの他のほとんどのサービスとは異なり、コンプライアンスサービスは、次の条件下でのシステムのデータのみを表示します。

- システムは、コンプライアンスサービスのセキュリティーポリシーに関連付けられています。
- システムは、**insights-client --compliance** コマンドを使用して、コンプライアンスデータをインサイトに報告しています。

これらの条件のため、コンプライアンスサービスのユーザーは、コンプライアンスサービス UI のシステムのリストの上にあるプライマリーフィルターとセカンダリフィルターを使用して、タグフィルターとグループフィルターを設定する必要があります。

コンプライアンスサービスのシステムリスト上のタグおよびグループフィルター



4.2. SAP ワークロード

2025 年に Linux は SAP ERP ワークロードの必須オペレーティングシステムになるため、Red Hat Enterprise Linux および Red Hat Insights for Red Hat Enterprise Linux では、Insights for RHEL が SAP 管理者に選ばれる管理ツールとなるように取り組んでいます。

この継続的な取り組みの一環として、Insights for Red Hat Enterprise Linux は、管理者によるカスタマイズを必要とせずに、SAP ワークロードを実行しているシステムに SAP ID (SID) によって自動的にタグを付けます。ユーザーは、グローバル **Filter by tags** ドロップダウンメニューを使用して、Insights for Red Hat Enterprise Linux アプリケーション全体でこれらのワークロードを簡単にフィルター処理できます。

4.3. SATELLITE ホストグループ

Satellite ホストグループは Satellite で設定され、Insights for Red Hat Enterprise Linux で自動的に認識されます。

4.4. MICROSOFT SQL SERVER のワークロード

タグによるグローバルフィルター 機能を使用して、Red Hat Insights for Red Hat Enterprise Linux ユーザーは、Microsoft SQL Server ワークロードを実行しているシステムのグループを選択できます。

2019 年 5 月、Red Hat Insights チームは、Red Hat Enterprise Linux (RHEL) で実行されている Microsoft SQL Server 向けの RHEL 推奨事項の新しい一連の Insights を導入しました。これらのルールは、オペレーティングシステムレベルの設定が Microsoft および Red Hat から文書化された推奨事項に準拠していないことを管理者に警告します。

これらのルールの制限は、データベース自体ではなく、主にオペレーティングシステムを分析することでした。Insights for Red Hat Enterprise Linux および RHEL 8.5 の最新リリースでは、Microsoft SQL Assessment API が導入されています。SQL Assessment API は、MS SQL Server のデータベース設定のベストプラクティスを評価するメカニズムを提供します。API には、Microsoft SQL Server チームが提案するベストプラクティスルールを含むルールセットが付属しています。このルールセットは新しいバージョンのリリースで拡張されていますが、API は高度にカスタマイズ可能で拡張可能なソリューションを提供することを目的として構築されており、ユーザーはデフォルトのルールを調整して独自のルールを作成できます。

SQL Assessment API は PowerShell for Linux (Microsoft から入手可能) でサポートされており、Microsoft は、API を呼び出してその結果を JSON 形式のファイルとして保存するために使用できる PowerShell スクリプトを開発しました。RHEL 8.5 では、Insights クライアントがこの JSON ファイルをアップロードし、結果を Insights for Red Hat Enterprise Linux UI にわかりやすい形式で表示するようになりました。

Insights for Red Hat Enterprise Linux での SQL Server 評価の詳細については、Red Hat Insights で利用できるようになった SQL Server データベースのベストプラクティス を参照してください。

4.4.1. SQL Server 評価の設定

Red Hat Insights に情報を提供するように Microsoft SQL Assessment API を設定するには、データベース管理者は以下の手順を実行する必要があります。

手順

1. 評価するデータベースで、SQL 認証を使用して SQL Server 評価用のログインを作成します。次の Transact-SQL は、ログインを作成します。**<*PASSWORD*>** を強力なパスワードに置き換えます。

```
USE [master]
GO
CREATE LOGIN [assessmentLogin] with PASSWORD= N'<*PASSWORD*>'
ALTER SERVER ROLE [sysadmin] ADD MEMBER [assessmentLogin]
GO
```

2. システムにログインするための認証情報を次のように保存します。ここでも <*PASSWORD*> をステップ 1 で使用したパスワードに置き換えます。

```
# echo "assessmentLogin" > /var/opt/mssql/secrets/assessment
# echo "<*PASSWORD*>" >> /var/opt/mssql/secrets/assessment
```

3. mssql ユーザーのみが資格情報にアクセスできるようにして、評価ツールで使用される資格情報を保護します。

```
# chmod 0600 /var/opt/mssql/secrets/assessment
# chown mssql:mssql /var/opt/mssql/secrets/assessment
```

4. microsoft-tools リポジトリーから PowerShell をダウンロードします。これは、SQL Server インストールの一部として **mssql-tools** および **mssqlodbc17** パッケージをインストールしたときに設定したものと同じリポジトリーです。

```
# yum -y  install powershell
```

5. PowerShell 用の SQLServer モジュールをインストールします。このモジュールには、評価 API が含まれています。

```
# su mssql -c "/usr/bin/pwsh -Command Install-Module SqlServer"
```

6. Microsoft のサンプル GitHub リポジトリーから runassessment スクリプトをダウンロードします。mssql によって所有され、実行可能であることを確認してください。

```
# /bin/curl -LJ0 -o /opt/mssql/bin/runassessment.ps1
https://raw.githubusercontent.com/microsoft/sql-server-samples/master/samples/manage/sql-assessment-api/RHEL/runassessment.ps1
# chown mssql:mssql /opt/mssql/bin/runassessment.ps1
# chmod 0700 /opt/mssql/bin/runassessment.ps1
```

7. Red Hat Insights が使用するログファイルを保存するディレクトリーを作成します。繰り返しますが、mssql によって所有され、実行可能であることを確認してください。

```
# mkdir /var/opt/mssql/log/assessments/
# chown mssql:mssql /var/opt/mssql/log/assessments/
# chmod 0700 /var/opt/mssql/log/assessments/
```

8. 最初の評価を作成できるようになりましたが、mssql ユーザーとしてより安全に cron または systemd を介して後続の評価を自動的に実行できるように、必ずユーザー mssql として作成してください。

```
# su mssql -c "pwsh -File /opt/mssql/bin/runassessment.ps1"
```

9. Insights for Red Hat Enterprise Linux は、次回の実行時に評価を自動的に含めます。または、次のコマンドを実行して Insights クライアントを開始することもできます。

```
# insights-client
```

4.4.1.1. タイマーでの SQL 評価の設定

SQL Server の評価は完了するまでに 10 分以上かかる場合があるため、評価プロセスを毎日自動的に実行することが理にかなっている場合とそうでない場合があります。それらを自動的に実行したい場合は、Red Hat SQL Server コミュニティーが評価ツールで使用する systemd サービスとタイマーファイルを作成しています。

手順

1. Red Hat public SQL Server Community of Practice GitHub サイト から次のファイルをダウンロードします。
   - **mssql-runassessment.service**
   - **mssql-runassessment.timer**
2. 両方のファイルをディレクトリー **/etc/systemd/system/** にインストールします。

```
# cp mssql-runassessment.service /etc/systemd/system/
# cp mssql-runassessment.timer /etc/systemd/system/
# chmod 644 /etc/systemd/system/
```

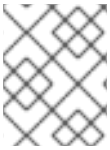
3. 次のコマンドでタイマーを有効にします。

```
# systemctl enable --now mssql-runassessment.timer
```

4.5. システムタグ付けのカスタム

システムにカスタムグルーピングとタグ付けを適用して、個別のシステムにコンテキストマーカーを追加したり、Insights for Red Hat Enterprise Linux アプリケーションでこれらのタグ別にフィルタリングしたり、より簡単に関連システムに焦点を当てたりすることができます。この機能は、何百または何千ものシステムが管理されている環境で、Red Hat Enterprise Linux の Insights を大規模にデプロイメントする場合に特に価値があります。

複数の Insights for Red Hat Enterprise Linux サービスにカスタムタグを追加する機能に加えて、定義済みタグを追加できます。advisor サービスは、これらのタグを使用して、より高いレベルのセキュリティーを必要とするシステムなど、より注意が必要なシステムに的を絞った推奨事項を作成できます。



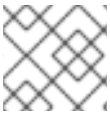
注記

カスタムタグと定義済みタグを作成するには、**/etc/insights-client/tags.yaml** ファイルに追加または変更するための root 権限、またはそれと同等の権限が必要です。

4.5.1. タグ構造

タグは、**namespace/key=value** のペアの構造を使用します。

- **名前空間。**名前空間は、インジェストポイントである **insights-client** の名前であり、変更することはできません。**tags.yaml** ファイルは名前空間から抽象化され、アップロード前に Insights クライアントによって挿入されます。
- **キー。**キーは、ユーザーが選択したキーまたはシステムの定義済みのキーにすることができます。大文字、文字、数字、記号、および空白文字の組み合わせを使用できます。
- **値。**独自の記述文字列値を定義します。大文字、文字、数字、記号、および空白文字の組み合わせを使用できます。



注記

advisor サービスには、Red Hat がサポートする定義済みタグが含まれています。

4.5.2. tags.yaml ファイルの作成とカスタムグループの追加

insights-client --group=<name-you-choose> を使用してタグ作成し、**/etc/insights-client/tags.yaml** に追加します。これは、以下を実行します。

- **etc/insights-client/tags.yaml** ファイルを作成します。
- **group=** キーおよび **<name-you-choose>** の値を **tags.yaml** に追加します。
- システムから Insights for Red Hat Enterprise Linux アプリケーションに新規アーカイブをアップロードすることで、最新の結果とともに新しいタグがすぐに表示されます。

初期 **グループ** タグを作成したら、必要に応じて **/etc/insights-client/tags.yaml** ファイルを編集し、タグを追加します。

次の手順は、**/etc/insights-client/tags.yaml** ファイルと初期グループを作成し、そのタグが Insights for Red Hat Enterprise Linux インベントリーに存在することを確認する方法を示しています。

グループの新規作成手順

1. **--group=** の後にカスタムグループ名を追加して、root で以下のコマンドを実行します。

```
[root@server ~]# insights-client --group=<name-you-choose>
```

tags.yaml 形式の例

次の **tags.yaml** ファイルの例は、新しいグループに追加されたファイル形式と追加のタグの例を示しています。

```
# tags
---
group: eastern-sap
```

```
name: Jane Example
contact: jexample@corporate.com
Zone: eastern time zone
Location:
- gray_rack
- basement
Application: SAP
```

カスタムグループが作成されたことを確認する手順

1. 必要に応じて Red Hat Insights > RHEL > Inventory に移動し、ログインします。
2. **Filter results** ドロップダウンメニューをクリックします。
3. リストをスクロールするか、検索機能を使用してタグを見つけます。
4. タグをクリックしてフィルター処理を行います。
5. システムが、アドバイザーシステムリストの結果に含まれていることを確認します。

システムがタグ付けされていることを確認する手順

1. 必要に応じて Red Hat Insights > RHEL > Inventory に移動し、ログインします。
2. **Name** フィルターをアクティブにし、システムが表示されるまでシステム名を入力してから選択します。
3. システム名の横にタグシンボルがグレイになり、適用されるタグの正確な数を表す数字が表示されることを確認します。

4.5.3. タグの追加または変更を行うための tags.yaml の編集

グループフィルターを作成したら、必要に応じて **/etc/insights-client/tags.yaml** の内容を編集して、タグの追加または変更を行います。

手順

1. コマンドラインで、編集するタグ設定ファイルを開きます。
   [root@server ~]# vi /etc/insights-client/tags.yaml
2. 必要に応じてコンテンツを編集するか、追加値を追加します。以下の例は、システムに複数のタグを追加する際の **tags.yaml** の管理方法を示しています。

```
# tags
---
group: eastern-sap
location: Boston
description:
- RHEL8
- SAP
key 4: value
```

注記

必要な数の key=value ペアを追加します。大文字、文字、数字、記号、および空白文字の組み合わせを使用します。

3. 変更を保存してエディターを閉じます。

4. オプションで、Red Hat Enterprise Linux の Insights へのアップロードを生成します。

```
# insights-client
```

4.5.4. 定義済みのシステムタグを使用した Red Hat Insights advisor サービスの推奨事項の精度とセキュリティーの向上

Red Hat Insights advisor サービスの推奨事項は、すべてのシステムを同等に扱います。ただし、システムによっては、他のシステムよりも高いレベルのセキュリティーが必要な場合や、異なるネットワークパフォーマンスレベルが必要な場合があります。カスタムタグを追加する機能に加えて、Red Hat Insights for Red Hat Enterprise Linux は定義済みタグを提供します。advisor サービスはこれを使用して、より注意が必要な可能性のあるシステムに的を絞った推奨事項を作成できます。

定義済みタグによって提供される拡張されたセキュリティー強化と強化された検出および修復機能をオプトインして取得するには、タグを設定する必要があります。設定後、advisor サービスは、調整された重大度レベルと、システムに適用されるネットワークパフォーマンス設定に基づいて推奨事項を提供します。

タグを設定するには、**/etc/insights-client/tags.yaml** ファイルを使用して、インベントリーサービスでシステムにタグを付ける場合と同様の方法で、定義済みタグを使用してシステムにタグを付けます。定義済みタグは、カスタムタグの作成に使用されるのと同じ **key=value** 構造を使用して設定されます。Red Hat の定義済みタグの詳細を次の表に示します。

表4.1 サポートされている定義済みタグのリスト

キー	値	注記
security	**normal** (デフォルト) / **strict**	**default** を使用すると、advisor サービスは、システムのリスクプロファイルを、RHEL の最新バージョンのデフォルト設定および頻繁に使用される使用パターンから導出されたベースラインと比較します。これにより、推奨事項の焦点があっており、アクション可能で、数を減らすことができます。**strict** 値を使用すると、advisor サービスはセキュリティーが重要なシステムであると見なし、特定の推奨事項でより厳密なベースラインが使用されるようになり、新しい最新の RHEL インストールでも推奨事項が表示される可能性があります。

キー	値	注記
network_performance	**null** (デフォルト) / **latency** / **throughput**	ネットワークパフォーマンス設定 (ビジネス要件に応じたレイテンシーまたはスループット) は、システムに対する advisor サービスの推奨事項の重大度に影響します。

注記

定義済みタグのキー名は予約されています。定義済みの値とは異なる値を持つキー **security** をすでに使用している場合、推奨事項に変更は加えられません。既存の **key=value** がいずれかの定義済みのキーと同じ場合にのみ、推奨事項に変更が加えられます。たとえば、**key=value** が **security: high** の場合、Red Hat の定義済みタグが原因で、推奨事項は変更されません。**key=value** ペアが **security: strict** である場合は、システムの推奨事項に変更が加えられます。

関連情報

- システムタグを使用して、拡張セキュリティー強化の推奨事項を有効にする
- タグを活用して Red Hat Insights Advisor の推奨機能の環境認識を向上させる
- システムタグ付けのカスタム

4.5.5. 定義済みタグの設定

Red Hat Insights for Red Hat Enterprise Linux advisor サービスの定義済みタグを使用すると、システムの推奨事項の動作を調整し、拡張されたセキュリティー強化と強化された検出および修復機能を得ることができます。以下の手順に従って、事前定義されたタグを設定できます。

前提条件

- システムへのルートレベルのアクセスがある。
- Insights クライアントがインストールされている。
- Insights クライアント内にシステムが登録されている。
- すでに **tags.yaml** ファイルを作成している。tags.yaml ファイルの作成とカスタムグループの追加 を参照してください。

手順

1. コマンドラインと任意のエディターを使用して、**/etc/insights-client/tags.yaml** を開きます。(次の例では Vim を使用しています。)

```
[root@server ~]# vi /etc/insights-client/tags.yaml
```

2. **/etc/insights-client/tags.yaml** ファイルを編集して、タグの定義済みの **key=value** ペアを追加します。この例は、**security: strict** および **network_performance: latency** タグを追加する方法を示しています。

```
# cat /etc/insights-client/tags.yaml
group: redhat
location: Brisbane/Australia
description:
- RHEL8
- SAP
security: strict
network_performance: latency
```

3. 変更を保存します。
4. エディターを終了します。
5. **オプション: Insights-client** コマンドを実行して、Red Hat Insights for Red Hat Enterprise Linux へのアップロードを生成するか、次のスケジュールされた Red Hat Insights アップロードまで待ちます。

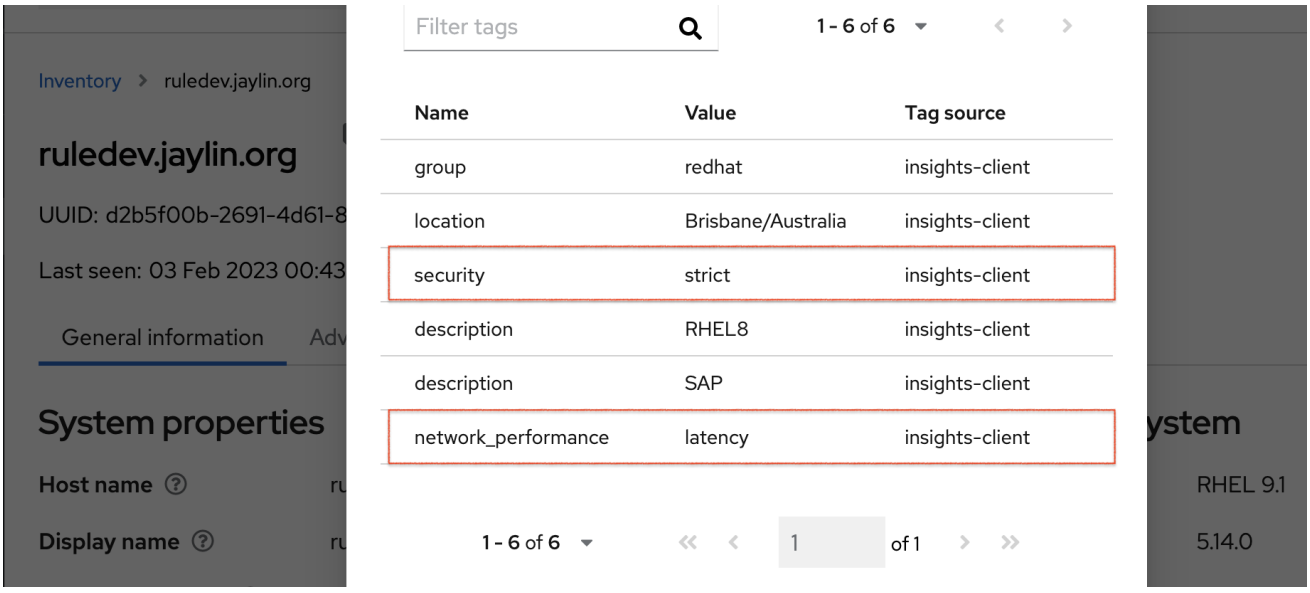
```
[root@server ~]# insights-client
```

定義済みタグが実稼働環境にあることの確認

Red Hat Insights へのアップロードを生成した後 (または、次の Insights アップロードのスケジュールを待った後)、Red Hat Insights > RHEL > Inventory にアクセスして、タグが実稼働環境にあるかどうかを確認できます。システムを見つけて、新たに作成されたタグを探します。次のことを示す表が表示されます。

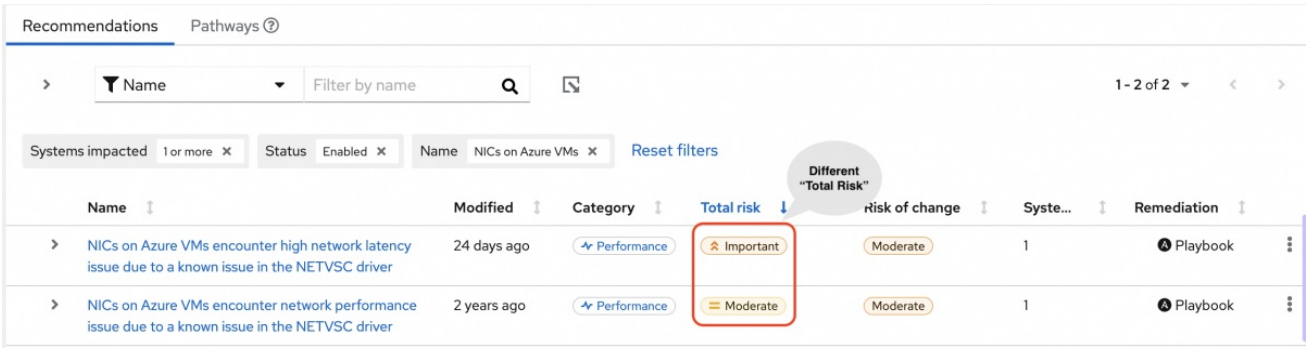
- 名前
- 値
- タグソース (例: insights-client)。

次のイメージは、タグを作成した後にインベントリーに表示される内容の例を示しています。



定義済みタグを適用した後の推奨事項の例

次の図では、advisor サービスは **network_performance: latency** タグが設定されたシステムを示しています。



システムは、総リスク (重要に分類) が高い推奨事項を表示します。**network_performance: latency** タグのないシステムの場合、総リスクは中程度に分類されます。総リスクの高さに基づいて、システムの優先順位付けに関する決定を行うことができます。

第5章 参考資料

詳細は、次の参考資料を参照してください。

5.1. 参考資料

Vulnerability サービスの詳細は、以下の資料を参照してください。

- **Vulnerability サービスレポートの生成**
- 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。