



Red Hat Insights 1-latest

FedRAMP 準拠のポリシーを使用した設定変更に対する監視および対応

インベントリ設定の変更を検出してメール通知を送信するポリシーを作成する方法

Red Hat Insights 1-latest FedRAMP 準拠のポリシーを使用した設定変更に対する監視および対応

インベントリー設定の変更を検出してメール通知を送信するポリシーを作成する方法

Red Hat Customer Content Services

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

このドキュメントでは、FedRAMP[®] に準拠した Policy サービスの概要と、システム設定の変更を検出して電子メールで通知するポリシーを作成する方法を説明します。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 RED HAT INSIGHTS ポリシーサービスの概要	3
1.1. RED HAT HYBRID CLOUD CONSOLE のユーザーアクセス設定	3
第2章 通知およびメール通知の設定	5
2.1. ポリシーサービスの通知と統合の有効化	5
2.2. ユーザー設定	5
第3章 ポリシーの作成	7
3.1. パブリッククラウドプロバイダーがオーバープロビジョニングされないようにするポリシーの作成	7
3.2. システムが RHEL の古いバージョンを実行しているかどうかを検出するポリシーの作成	8
3.3. 最新の CVE をもとに脆弱なパッケージバージョンを検出するポリシーの作成	8
第4章 ポリシーの確認および管理	10
第5章 付録	11
5.1. システムファクト	11
5.2. 演算子	14
RED HAT ドキュメントへのフィードバック (英語のみ)	16

第1章 RED HAT INSIGHTS ポリシーサービスの概要

ポリシーは環境内のシステム設定を評価し、変更が発生したときに通知を送信できます。作成するポリシーは、Insights インベントリ内のすべてのシステムに適用できます。Red Hat Hybrid Cloud Console の Red Hat Insights for Red Hat Enterprise Linux ユーザーインターフェイス、または Insights API を使用して、ポリシーを作成および管理できます。

ポリシーは、以下のようなタスクの管理に役立ちます。

- システム設定で特定の条件が発生した場合にアラートを生成する。
- システムでセキュリティーパッケージが古くなった場合にチームに電子メールを送信する。

ポリシーを使用してインベントリの設定変更を監視し、電子メールで通知するには、以下が必要です。

- ユーザーの電子メール設定を設定する (まだ設定されていない場合)。
- ポリシーを作成して、設定変更をトリガーとして検出し、トリガーアクションとして電子メールを選択する。



注記

- User Access は、[Red Hat Hybrid Cloud Console > Settings アイコン \(⚙️\) > Identity & Access Management > User Access > Users](#) で設定します。
- この機能の詳細と使用例は、[FedRAMP を使用したロールベースのアクセス制御 \(RBAC\) で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. RED HAT HYBRID CLOUD CONSOLE のユーザーアクセス設定

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。

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。

1.1.2. ポリシーサービスの User Access ロール

Red Hat Hybrid Cloud Console の次の事前定義済みロールを使用すると、Insights for Red Hat Enterprise Linux のポリシー機能にアクセスできます。

- **ポリシー管理者ロール**。ポリシー管理者ロールは、ポリシーリソースに対する利用可能な操作の実行をユーザーに許可する、読み取りおよび書き込みアクセスを提供します。この事前定義済みロールは、**デフォルトの管理者アクセスグループ** に属しています。
- **ポリシー閲覧者ロール**。ポリシー閲覧者ロールは、読み取り専用アクセスを提供します。ポリシー閲覧者ロールのデフォルト設定が不十分であると判断される場合は、**User Access 管理者** が、必要な特定のパーミッションを持つカスタムロールを作成できます。この事前定義済みロールは、**デフォルトのアクセスグループ** に属しています。



注記

2023年4月より前にグループを設定した場合、組織管理者ではないユーザーのポリシー管理者ロールは、ポリシー閲覧者ロールに置き換えられます。4月より前にデフォルトのアクセスグループに加えられた変更は、反映されません。

関連情報

- 「ロールベースアクセス制御 (RBAC) の User Access 設定ガイド」の [User Access の使用方法](#)
- [事前定義された User Access ロール](#)

第2章 通知およびメール通知の設定

Red Hat Insights は、Red Hat Hybrid Cloud Console で通知とユーザー設定を指定すると、Red Hat Enterprise Linux システムに対するポリシーの変更を通知します。

2.1. ポリシーサービスの通知と統合の有効化

Red Hat Hybrid Cloud Console で通知サービスを有効にすると、ポリシーサービスが問題を検出してアラートを生成するたびに、通知を送信できます。通知サービスを使用すると、Red Hat Insights ダッシュボードでアラートを継続的にチェックする必要がなくなります。

たとえば、サーバーのセキュリティソフトウェアが古くなっていることをポリシーサービスが検出したときに自動的に電子メールメッセージを送信するように、またはポリシーサービスが毎日生成するすべてのアラートの電子メールダイジェストを送信するように通知サービスを設定できます。

通知サービスは、電子メールメッセージだけでなく、以下に示す他の方法でポリシーイベントデータを送信するように設定することもできます。

- 認証済みクライアントを使用して Red Hat Insights API にイベントデータをクエリーする
- Webhook を使用して受信要求を受け入れるサードパーティーのアプリケーションにイベントを送信する
- Splunk などのアプリケーションと通知を統合してポリシーイベントをアプリケーションダッシュボードにルーティングする

通知サービスを有効にするには、以下の3つの主要なステップが必要です。

- まず、組織管理者が通知管理者ロールを持つ User Access グループを作成し、そのグループにアカウントメンバーを追加します。
- 次に、通知管理者が通知サービス内のイベントの動作グループを設定します。動作グループは、通知ごとに配信方法を指定します。たとえば、動作グループは、電子メール通知をすべてのユーザーに送信するか、組織の管理者にのみ送信するかを指定できます。
- 最後に、イベントから電子メール通知を受信するユーザーは、各イベントの個別電子メールを受け取るようにユーザー設定する必要があります。

関連情報

- 発生済みで組織に影響を与える可能性がある特定されたイベントを確認するための Hybrid Cloud Console 通知の設定に関する詳細は、[Red Hat Hybrid Cloud Console with FedRAMP での通知の設定](#) を参照してください。
- サードパーティーアプリケーションと統合する Hybrid Cloud Console 通知の設定に関する詳細は、[Red Hat Hybrid Cloud Console とサードパーティーアプリケーションのインテグレーション](#) を参照してください。

2.2. ユーザー設定

メール通知を受け取るには、以下の手順に従ってメール設定を指定したり、更新したりできます。

手順

1. [Operations > Policies](#) に移動します。

2. **Open user preferences** をクリックします。My Notifications ページが表示されます。
3. 左側のメニューから **Red Hat Enterprise Linux > Policies** を選択します。
4. ポリシーの通知設定を定義するには、適切なボックスにチェックを入れます。
5. 電子メール通知の設定によっては、トリガーされたポリシーを含む各システムに関する **即時通知** 電子メールや、トリガーされたアプリケーションイベントを 24 時間単位でまとめた **日次ダイジェスト** をサブスクライブできます。すべての通知のサブスクライブを解除するには、**Unsubscribe from all** を選択します。



注記

即時通知をサブスクライブすると、大規模なインベントリで多数のメールを受信する可能性があります。メールの量を減らすには、Daily digest オプションを選択することを検討してください。

6. **Submit** をクリックします。

第3章 ポリシーの作成

以下のワークフローの例では、複数のタイプのポリシーを作成し、システム設定の変更を検出して変更通知の電子メールを送信する方法を説明します。



注記

ポリシーの作成時に、メールのアラートにオプトインしていない旨の警告メッセージが表示される場合は、ポリシーからメールを受信するようにユーザー設定を行います。

3.1. パブリッククラウドプロバイダーがオーバープロビジョニングされないようにするポリシーの作成

以下の手順を使用してポリシーを作成します。

手順

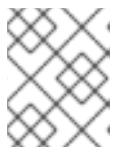
1. [Red Hat Hybrid Cloud Console](#) で、[Operations > Policies](#) に移動します。
2. **Create policy** をクリックします。
3. 必要に応じて、Create a policy ページで **From scratch** または **As a copy of existing Policy** をクリックします。**As a copy of existing Policy** オプションでは、開始点として使用する既存のポリシーリストからポリシーを選択するように求められます。
4. **Next** をクリックします。
5. **Condition** を入力します。この場合は、`['alibaba', 'aws', 'azure', 'google'] and(facts.number_of_cpus >= 8 or facts.number_of_sockets >= 2)` と入力します。この条件では、指定のパブリッククラウドプロバイダーで実行中のインスタンスが許容範囲を超える CPU ハードウェアで実行されているかどうかを検出します。



注記

What condition can I define? または **Review available system facts** をデプロイメントして、使用可能な条件の説明を表示し、利用可能なシステムファクトをそれぞれ表示できます。このセクションでは、使用できる構文の例を示します。

6. **Validate condition** をクリックします。
7. 条件を検証したら、**Next** をクリックします。
8. Trigger actions ページで **Add trigger actions** をクリックします。通知がグレイアウトされたら、通知ボックスの **Notification settings** を選択します。ここで、通知とその動作をカスタマイズできます。
9. **Next** をクリックします。



注記

Trigger actions ページで、電子メールアラートを有効にし、電子メール設定を開くこともできます。

10. Review and enable ページで、切り替えスイッチをクリックしてポリシーを有効にし、詳細を確認します。
11. **Finish** をクリックします。

新しいポリシーが作成されました。システムのチェックインでポリシーが評価されたときに、ポリシーの条件が満たされている場合、ポリシーは、ユーザーの電子メール設定に応じて、ポリシーにアクセスできるアカウントのすべてのユーザーに電子メールを自動的に送信します。

3.2. システムが RHEL の古いバージョンを実行しているかどうかを検出するポリシーの作成

システムが古いバージョンの RHEL を実行しているかどうかを検出し、検出内容について電子メールで通知を送信するポリシーを作成できます。

手順

1. [Red Hat Hybrid Cloud Console](#) で、[Operations > Policies](#) に移動します。
2. **Create policy** をクリックします。
3. Create Policy ページで、必要に応じて **From scratch** または **As a copy of existing Policy** をクリックします。**As a copy of existing Policy** オプションでは、開始点として使用する既存のポリシーリストからポリシーを選択するように求められます。
4. **Next** をクリックします。
5. ポリシーの **Name** および **Description** を入力します。
6. **Next** をクリックします。
7. **Condition** を入力します。この場合は、**facts.os_release <8.1** と入力します。この条件は、システムが、RHEL 8.1 をベースとした以前のバージョンのオペレーティングシステムを実行しているかどうかを検出します。
8. **Validate condition** をクリックして、**Next** をクリックします。
9. Trigger actions ページで **Add trigger actions** をクリックし、**Email** を選択します。
10. **Next** をクリックします。
11. Review and activate ページで、切り替えスイッチをクリックしてポリシーを有効にし、詳細を確認します。
12. **Finish** をクリックします。

新しいポリシーが作成されました。システムのチェックインでポリシーが評価されたときに、ポリシーの条件がトリガーされると、ポリシーサービスは、ユーザーの電子メール設定に応じて、ポリシーにアクセスできるアカウントのすべてのユーザーに電子メールを自動的に送信します。

3.3. 最新の CVE をもとに脆弱なパッケージバージョンを検出するポリシーの作成

最新の CVE をもとに脆弱なパッケージバージョンを検出し、検出内容を電子メールで通知するポリシーを作成できます。

手順

1. [Red Hat Hybrid Cloud Console](#) で、[Operations > Policies](#) に移動します。
2. **Create policy** をクリックします。
3. Create Policy ページで、必要に応じて **From scratch** または **As a copy of existing Policy** をクリックします。**As a copy of existing Policy** オプションでは、開始点として使用する既存のポリシーリストからポリシーを選択するように求められます。
4. **Next** をクリックします。
5. ポリシーの **Name** および **Description** を入力します。
6. **Next** をクリックします。
7. **Condition** を入力します。この場合は、**facts.installed_packages contains ['openssh-4.5']** と入力します。この条件は、システムが、最新の CVE に基づいて **openssh** パッケージの脆弱なバージョンを実行しているかどうかを検出します。
8. **Validate condition** をクリックして、**Next** をクリックします。
9. Trigger actions ページで **Add trigger actions** をクリックし、**Email** を選択します。
10. **Next** をクリックします。
11. Review and activate ページで、切り替えスイッチをクリックしてポリシーを有効にし、詳細を確認します。
12. **Finish** をクリックします。


新しいポリシーが作成されました。システムのチェックインでポリシーが評価されたときに、ポリシーの条件が満たされている場合、ポリシーは、ユーザーの電子メール設定に応じて、ポリシーにアクセスできるアカウントのすべてのユーザーに電子メールを自動的に送信します。

第4章 ポリシーの確認および管理

[Operations > Policies](#) に移動すると、作成されたすべての (有効化および無効化された) ポリシーを確認および管理できます。

ポリシーのリストは、名前別およびアクティブ状態でフィルタリングできます。ポリシーの横にあるオプションメニューをクリックして、以下の操作を実行できます。

- 有効化および無効化
- 編集
- 複製
- 削除

また、ポリシー一覧から複数のポリシーを選択し、上部のポリシーの **Create policy** ボタンの横にあるオプションメニュー  をクリックすると、以下の操作を一括で実行できます。

- ポリシーの削除
- ポリシーの有効化
- ポリシーの無効化



注記

オプトインされていないメールアラートに関する警告メッセージが表示された場合は、ポリシーからメールを受信するようにユーザー設定を指定してください。

第5章 付録

この付録には、以下の参考資料が含まれています。

- システムファクト
- 演算子

5.1. システムファクト

以下の表に、システム比較用のシステムファクトを示します。

表5.1 システムファクトおよび機能

ファクト名	説明	値の例
Ansible	Ansible 関連のファクトのリストを含むカテゴリー	値が 4.0.0 の controller_version
arch	システムアーキテクチャー	x86_64
bios_release_date	BIOS リリース日: 通常は MM/DD/YYYY	01/01/2011
bios_vendor	BIOS ベンダー名	LENOVO
bios_version	BIOS バージョン	1.17.0
cloud_provider	クラウドベンダー。値は google 、 azure 、 aws 、 alibaba 、または empty です。	google
cores_per_socket	ソケットあたりの CPU コア数	2
cpu_flags	CPU フラグのリストが含まれるカテゴリー。それぞれの名前は CPU フラグ (vmx など) で、値は常に enabled です。	値が enabled の vmx
enabled_services	有効なサービスのリストが含まれるカテゴリー。各カテゴリーの名前はサービス名 (crond など) で、値は常に enabled です。	値が enabled の crond
fqdn	システムの完全修飾ドメイン名	system1.example.com
infrastructure_type	システムインフラストラクチャー。一般的な値は virtual または physical です。	virtual
infrastructure_vendor	インフラストラクチャーベンダー。一般的な値は kvm 、 vmware 、 baremetal などです。	kvm

ファクト名	説明	値の例
installed_packages	インストールされている RPM パッケージのリスト。これはカテゴリです。	値が 4.2.46-33.el7.x86_64 の bash
installed_services	インストールされているサービスのリストが含まれるカテゴリ。各カテゴリの名前はサービス名 (crond など) で、値は常に installed です。	値が installed の crond
kernel_modules	カーネルモジュールのリスト。カテゴリの各名前はカーネルモジュール (例: nfs) で、値は enabled です。	値が enabled の nfs
last_boot_time	YYYY-MM-DDTHH:MM:SS 形式のブート時間。情報のみ。システム全体での起動時間は比較しません。	2019-09-18T16:54:56
mssql	MSSQL 関連のファクトのリストを含むカテゴリ	値が 15.0.4153.1 の mssql_version
network_interfaces	ネットワークインターフェイスに関連するファクトの一覧	
	各インターフェイスには、 ipv6_addresses 、 ipv4_addresses 、 mac_address 、 mtu 、 state 、 type のファクトが 6 つあります。2 つのアドレスフィールドは IP アドレスのコンマ区切りリストです。 state フィールドは UP または DOWN のいずれかになります。 type フィールドはインターフェイス種別です (例: ether 、 loopback 、 bridge など)。	
	各インターフェイス (例: lo 、 em1 など) は、ファクト名の前に付けられます。たとえば、em1 の MAC アドレスは em1.mac_address という名前のファクトになります。	
	多くのネットワークインターフェイスのファクトは、システム全体で等しいことを確認するために比較されます。ただし、 ipv4_addresses 、 ipv6_addresses 、および mac_address は、システム全体で異なることを確認するためにチェックされます。 lo のサブ例外 (subexception) は、すべてのシステムで常に同じ IP アドレスと MAC アドレスを持つ必要があります。	

ファクト名	説明	値の例
number_of_cpus	CPU の合計数	1
number_of_sockets	ソケットの合計数	1
os_kernel_version	カーネルバージョン	4.18.0
os_release	カーネルリリース	8.1
running_processes	実行中のプロセスのリスト。ファクト名はプロセスの名前で、値はインスタンス数です。	値が 1 の crond
sap_instance_number	SAP インスタンス番号	42
sap_sids	SAP システム ID (SID)	A42
sap_system	SAP がシステムにインストールされているかどうかを示すブール値フィールド	True
sap_version	SAP バージョン番号	2.00.052.00.1599 235305
satellite_managed	システムが Satellite Server に登録されているかどうかを示すブール値フィールド	FALSE
selinux_current_mode	現在の SELinux モード	enforcing
selinux_config_file	設定ファイルに設定されている SELinux モード	enforcing
systemd	失敗の数、キューに入れられている現在のジョブの数、および systemd の現在の状態	state with a value of degraded
system_memory	人が読める形式のシステムメモリーの合計	3.45 GiB
tuned_profile	tuned-adm active コマンドから生成された現在のプロファイル	desktop

ファクト名	説明	値の例
yum_repos	yum リポジトリーの一覧。リポジトリー名がファクトの最初に追加されます。各リポジトリーには、関連するファクト base_url 、 enabled 、および gpgcheck があります。	Red Hat Enterprise Linux 7 Server(RPMs).base_url の値は https://cdn.redhat.com/content/dist/rhel/server/7/\$releasever/\$basearch/os になります。

5.2. 演算子

表5.2 条件で利用可能な演算子

演算子	値
論理演算子	AND
	OR
ブール演算子	EQUAL
	NOTEQUAL
数値比較演算子	GT
	GTE
	LT
	LTE
文字列比較演算子	CONTAINS
配列演算子	IN
	CONTAINS
解析演算子	OR
	AND
	NOT

演算子	値
	EQUAL
	NOTEQUAL
	CONTAINS
	NEG

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。