Red Hat Insights 2022

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

Last Updated: 2022-06-20

Red Hat Insights 2022 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

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

本書では、Policy サービスの概要と、システム設定の変更を検出してメールで通知するポリシーを作成する方法について説明します。

目次

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。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、弊社の CTO、Chris Wright のメッセージ 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

弊社のドキュメントに関するご意見やご感想をお寄せください。フィードバックを提供するには、ドキュメントのテキストを強調表示し、コメントを追加します。

前提条件

- Red Hat カスタマーポータルにログインしている。
- Red Hat カスタマーポータルでは、このドキュメントは **Multi-page HTML** 表示形式です。

手順

フィードバックを提供するには、以下の手順を実施します。

1. ドキュメントの右上隅にある **フィードバック** ボタンをクリックして、既存のフィードバックを確認します。

注記

フィードバック機能は、**マルチページ HTML** 形式でのみ有効です。

2. フィードバックを提供するドキュメントのセクションを強調表示します。
3. ハイライトされたテキスト近くに表示される **Add Feedback** ポップアップをクリックします。ページの右側のフィードバックセクションにテキストボックスが表示されます。
4. テキストボックスにフィードバックを入力し、**Submit** をクリックします。ドキュメントに関する問題が作成されます。
5. 問題を表示するには、フィードバックビューで問題リンクをクリックします。

第1章 INSIGHTS FOR RHEL インベントリーの変更についてポリシーから自動通知を受け取る手順

Policies サービスを使用すると、通知設定を指定し、発生する可能性のあるセキュリティーの問題や、システムへの変更をユーザーに通知できます。

1.1. インベントリー設定の変更に関するポリシーの検出および通知

作成するポリシーは、Insights for RHEL インベントリー内のすべてのシステムに適用できます。Insights for RHEL ユーザーインターフェースまたは 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メールを送信する。

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

- ユーザーの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メールを選択する。

注記

- Insights for Red Hat Enterprise Linux > Settings > User Access で User Access を設定します。
- この機能およびユースケースの詳細は、**User Access Configuration Guide for Role-based Access Control (RBAC)** を参照してください。

1.2. ポリシーサービスの通知と統合を有効にする

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、Red Hat Hybrid Cloud Console の通知サービスを有効にして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ー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。

メールメッセージの送信に加え、他の方法でポリシーイベントデータを送信するように通知サービスを設定できます。

- 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、組織管理者は通知管理者ロールを持つユーザーアクセスグループを作成し、そのグループにアカウントメンバーを追加します。
- 次に、通知管理者は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、メール通知をすべてのユーザーに送信するか、組織の管理者のみ送信するかを指定できます。
- 最後に、イベントからメール通知を受信するユーザーは、各イベントの個別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

ポリシーアラートの通知を設定する方法の詳細は、Red Hat Insights Notifications を参照してください。

第2章 ユーザー設定

情報を更新し、ユーザープリファレンスで Red Hat Hybrid Cloud Console サービスの E メールプリファレンスを設定します。

2.1. ユーザー設定

メールの設定は、以下のように設定または更新できます。

手順

1. 右上のユーザーメニューをクリックし、User preferences > Notifications > Red Hat Enterprise Linux https://console.redhat.com/user-preferences/email に移動します。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。
2. メール通知の設定によっては、ポリシーがトリガーされた各システムに関する **Instant notification** メールや、24 時間単位でアプリケーションイベントがトリガーされた全システムに関する **Daily digest** (まとめ) にサブスクライブできます。

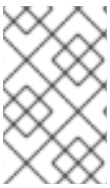
注記

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ーで多量のメールを受け取る可能性があります。つまり、システムのチェックごとにメールを 1 件受け取ります。

3. **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に、ポリシーからメールを受信するように設定します。詳細は、第 2 章の「ユーザー設定」を参照してください。

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

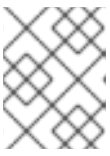
手順

1. Red Hat Hybrid Cloud Console で、 Red Hat Enterprise Linux > 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一覧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** を展開して、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。通知がグレーアウトされたら、通知ボックスの **Notification settings** を選択します。ここでは、notificaitons および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、メールアラートを有効にし、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て詳細を確認します。
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を評価する時に、ポリシー内の条件が満たされると、メールの設定に合わせて、ポリシーは自動的にポリシーへのアクセスのあるアカウント内の全ユーザーにメールを送信します。

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、 Red Hat Enterprise Linux > 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一覧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** と **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、トグルスイッチをクリックしてポリシーをアクティブにし、その詳細を確認します。
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を評価する時に、ポリシー内の条件がトリガーされると、メールの設定に合わせて、ポリシーサービスはポリシーへのアクセスのあるアカウントの全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、 Red Hat Enterprise Linux > 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一覧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** と **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、トグルスイッチをクリックしてポリシーをアクティブにし、その詳細を確認します。
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を評価する時に、ポリシー内の条件が満たされると、メールの設定に合わせて、ポリシーは自動的にポリシーへのアクセスのあるアカウント内の全ユーザーにメールを送信します。

第4章 ポリシーの確認および管理

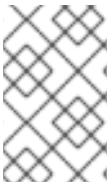
Red Hat Enterprise Linux > Policies に移動すると、作成されたすべてのポリシー (有効および無効) を確認および管理できます。

ポリシーの一覧は、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。

- Enable and disable
- Edit
- Duplicate
- Delete

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
- ポリシーを無効にする



注記

メール通知がオプトインされていないことを示す警告メッセージが表示される場合は、2章「ユーザー設定」の説明に従って、ポリシーからメールを受信するように設定を行います。

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

以下の表は、システム比較で使用するシステムファクトを表示します。

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 フラグの一覧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	有効なサービスの一覧が含まれるカテゴリー。カテゴリーの各名前はサービス名 (**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 パッケージの一覧。これはカテゴリーです。	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一覧が含まれるカテゴリー。カテゴリーの各名前はサービス名 (**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一覧。カテゴリー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ー	15.0.4153.1 の値を持つ mssql_version
network_interfaces	ネットワークインターフェースに関連するファクトの一覧。	
	各インターフェースには、**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ース種別です (例: **ether**、**loopback**、**bridge** など)。	
	各インターフェース (例: **lo**、**em1** など) がファクト名にプレフィックスが付けられます。たとえば、em1 の mac address は、**em1.mac_address** という名前のファクトになります。	

ファクト名	説明	値の例
	多くのネットワークインターフェースのファクトは、システム全体で同等である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よう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。	
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一覧。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。。	**crond**: 値が **1** です。
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	**2.00.052.00.1599235305**
satellite_managed	示すブーリアンフィールドは、Satellite サーバーに登録されているシステムです。	**FALSE**
selinux_current_mode	現在の SELinux モード	**enforcing**
selinux_config_file	設定ファイルに設定した SELinux モード	**enforcing**
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
ブール値の演算子	EQUAL
	NOTEQUAL
数値比較演算子	GT
	GTE
	LT
	LTE
文字列比較演算子	CONTAINS
アレイ演算子	IN
	CONTAINS
パーサー演算子	OR
	AND
	NOT

演算子	値
	EQUAL
	NOTEQUAL
	CONTAINS
	NEG