

RHEL8.5から登場した Red Hat Connector

Solution Architect
森若和雄
2021-11-19

このスライドの目的

- 対象: RHEL運用管理者
- 目的: RHEL 8.5から登場したrhc(Red Hat Connector)の目的を理解して要不要の判断ができるようにする

Red Hat Connectorが解決しようとしている課題は何？

- Red Hat Enterprise Linuxの初期登録が煩雑
 - rhc connectコマンドだけで以下を処理
 - subscription-manager register
 - insights-client register
 - Red Hat InsightsへのOpenSCAPスキャン結果登録
- Red Hat Insightsの機能強化
 - Red Hat Insightsは1日1回情報をスキャンして診断情報を提供するSaaS
 - Red Hat ConnectorはRed Hat InsightsからのRemediation(Ansible playbook)実行を可能にする
 - 関連パッケージ更新、設定の自動修正など
 - 従来もできたが、別売のRed Hat Smart Managementが必要だった

Red Hat Connector利用のおおまかな流れ

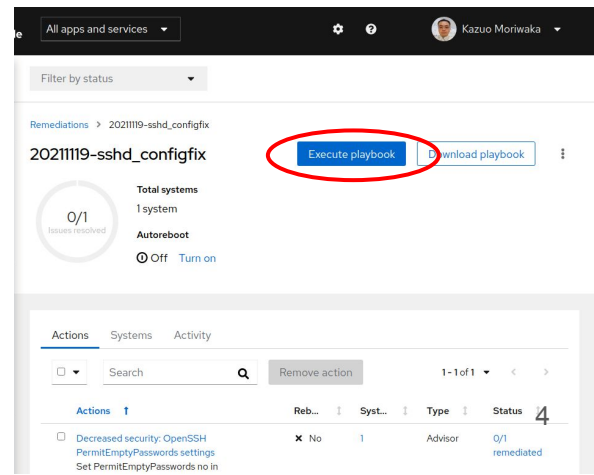
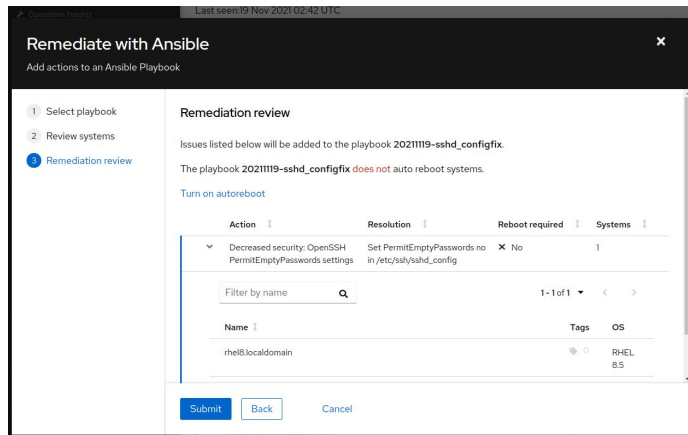
1. 各システム上で、`rhc connect`コマンドを実行して**アカウントへ登録**する
(1日1回、Red Hat Insightsが自動的に情報収集と診断)
2. 管理者がRed Hat Insights上で**Remediation**を作成
3. Remediationの**Execute playbook**ボタンを押すとシステムが修正される

```
[root@rhel8 ~]# rhc connect
Connecting rhel8.localdomain to Red Hat.
This might take a few seconds.

Username: kmoriwak
Password:

● Connected to Red Hat Subscription Management
● Activated the Red Hat connector daemon

Manage your Red Hat connector systems: https://red.ht/connector
[root@rhel8 ~]#
```



Red Hat Connector

Red Hat Connector はrhccommandとrhcdサービスからなります。

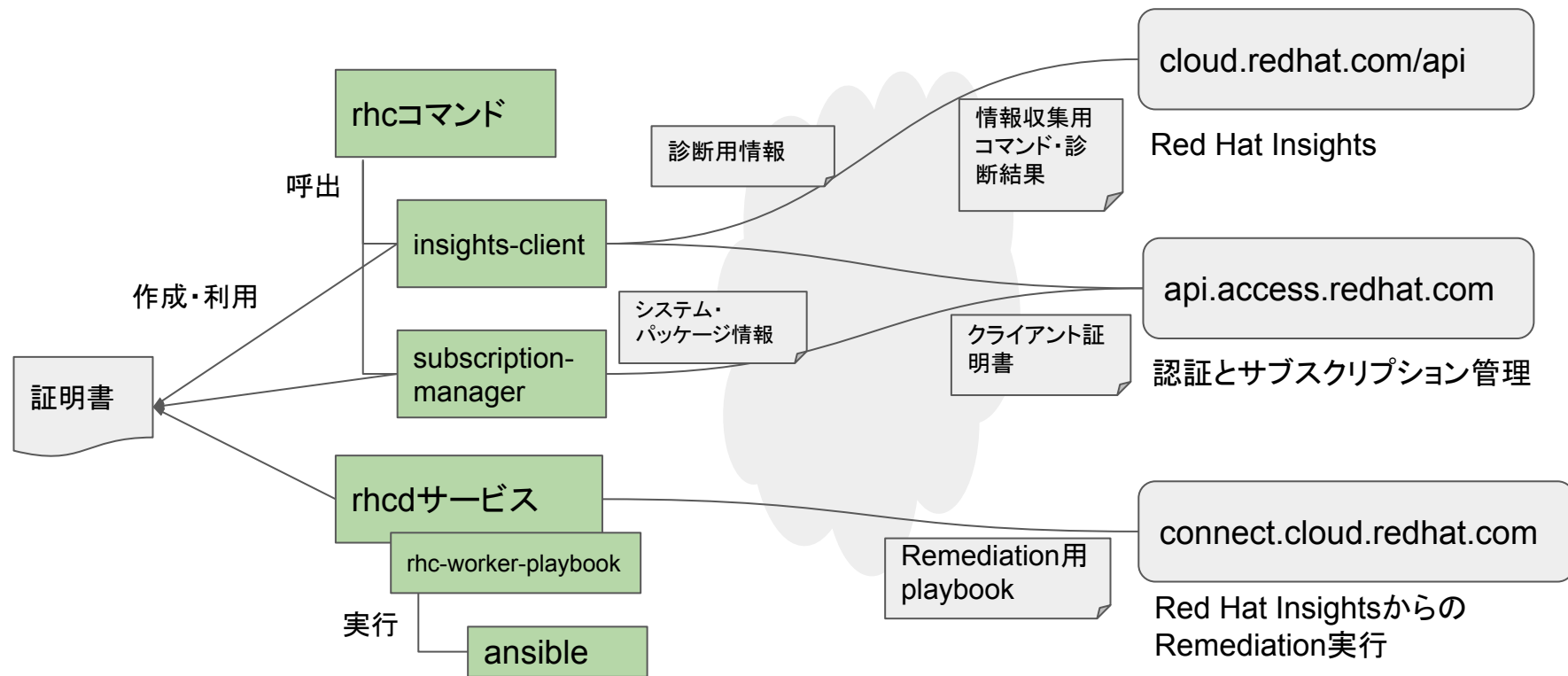
rhccommand

- Red Hat Insightsへ登録
- Red Hat Subscription Managementの登録
- Red Hat Connector Daemon(rhcd)の有効化

rhcdサービス

- Red Hat InsightsからのRemediation(Ansible playbook)の受け付けと実行

概要図



Cloud ConnectorとRed Hat Connectorの比較

Red Hat InsightsからRemediationを実行するための仕組みとしては以前からCloud Connectorがありました。簡単に比較します。

	Red Hat Connector	Cloud Connector
対象RHELバージョン	8.5以降	Insightsに対応した全バージョン
登録するもの	各RHELシステム	Red Hat Satellite Server
Smart Management 必要?	不要	必要
通信の仕組み	各RHELのrhcd	Satellite Serverのreceptor

rhcコマンドの使い方

- 事前設定 (Remediation実行をしたい場合)

```
# subscription-manager register
```

```
# subscription-manager repos --enable ansible-2.9-for-rhel-8-x86_64-rpms
```

```
# dnf -y install ansible rhc-worker-playbook
```

- アクティベーションキーを使って登録

```
# rhc connect -a <activation-key> -o <organization-id>
```

- アカウント情報を使って登録

```
# rhc connect -u <username> -p <password>
```

- 登録を削除

```
# rhc disconnect
```


Red Hat Connectorの設定

<https://red.ht/connector> で、登録したときの機能の利用有無を設定

- Red Hat Insightsの利用有無
 - Insights内でのOpenSCAPの利用有無
 - InsightsからのRemediation実行の利用有無

「Insightsのレポートは見たいけれど
リモート実行はNG」のようなケースに対応

The screenshot displays the 'Red Hat connector Dashboard' with a 'Tech preview' label and a 'Connect systems' button. It shows '1' system connected with a 'View in Inventory' link. Below, the 'Services' tab is active, showing 'Red Hat Insights' with 'Save changes' and 'View log' buttons. A descriptive paragraph follows. The 'Settings' section contains three toggle switches, all of which are turned on: 'Connect to Red Hat Insights', 'Use OpenSCAP for Compliance policies', and 'Enable Cloud Connector to fix issues directly from Insights'.

Red Hat connector Dashboard Tech preview Connect systems

Systems connected with Red Hat connector
1
[View in Inventory](#)

Services Activation keys

Red Hat Insights Save changes View log

Red Hat Insights is a proactive operational efficiency and security risk management solution in Red Hat Enterprise Linux (RHEL) subscriptions for versions 6.4 and higher, as well as public cloud versions of RHEL. It helps identify, prioritize, and resolve risks to security, compliance, performance, availability, and stability before they become urgent issues. Insights also enables users to monitor for adherence to internal policies and understand configuration changes over time.

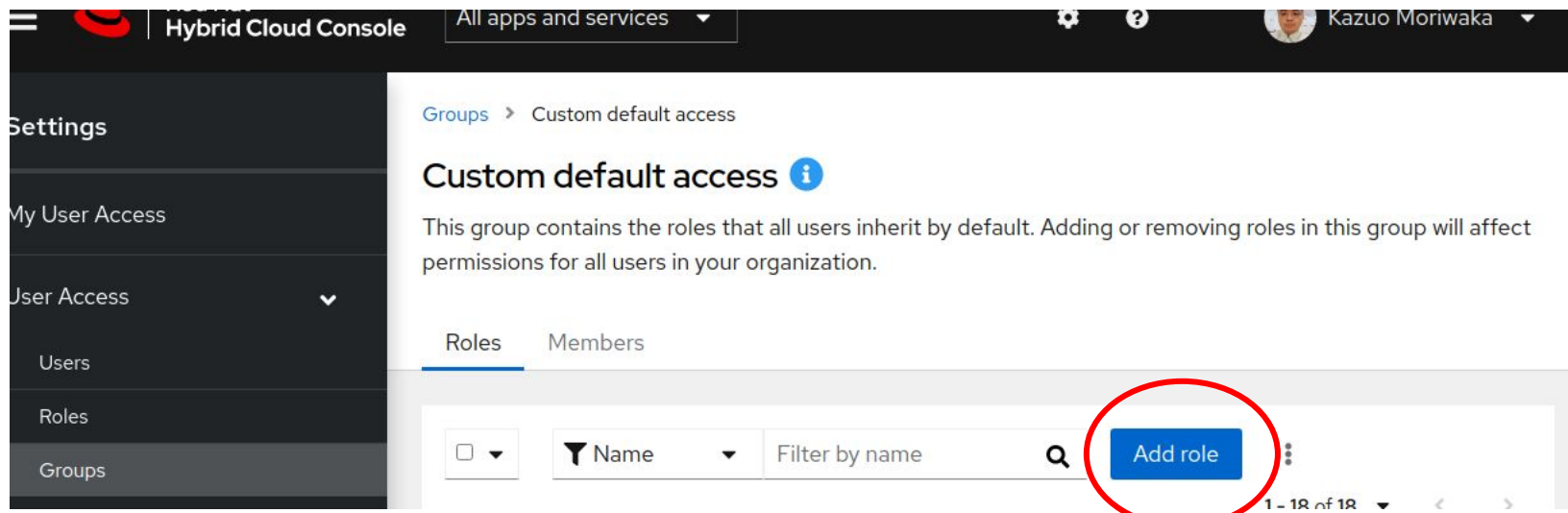
Settings

- ☒ **Connect to Red Hat Insights**
Required to use Insights applications. Enables Advisor, Drift, Patch, Vulnerability and Policies applications.
- ☒ **Use OpenSCAP for Compliance policies**
Required to use Compliance application
- ☒ **Enable Cloud Connector to fix issues directly from Insights**
Cloud Connector allows you to push Remediation Ansible Playbooks directly from Insights to your systems.

ユーザにRoleを追加

Remediationを実行するには Remediations administrator ロールが必要。
デフォルトでは許可されていない。

<https://console.redhat.com/settings/rbac/groups> で、実行を許可したいユーザのグループにRemediations administratorを追加する。



Red Hat Insightsでシステムの状態を確認

console.redhat.com/insights/ で
システム状態を確認する。

検出した問題のうち、自動修正できるものはAnsible欄にチェックがつく。

The screenshot displays the Red Hat Hybrid Cloud Console interface. The left sidebar contains navigation links for Red Hat Enterprise Linux, Dashboard, Operations Insights, Advisor, Drift, Inventory, Security Insights, Vulnerability, Compliance, Policies, Patch, Business Insights, Subscriptions, Register Systems, and Remediations. The main content area shows the 'Inventory' section for the host 'rhel8.localdomain'. It includes details like UUID and last seen time. Below this, there are tabs for General information, Advisor (selected), Vulnerability, Compliance, and Patch. The 'Advisor' tab shows a table of detected issues. One issue is listed: 'Decreased security: OpenSSH PermitEmptyPasswords settings', which is 5 years old and has a 'Moderate' risk level. A green checkmark in the 'Ansible' column indicates that this issue can be automatically remediated. Below the table, there is a section titled 'Detected issues' with a detailed explanation of the OpenSSH settings issue and a recommendation to review and revise the settings.

Red Hat Hybrid Cloud Console

All apps and services

Filter by status

Inventory > rhel8.localdomain

rhel8.localdomain

UUID: 2e5d425d-889d-4c42-b8db-7fce0436b498

Last seen: 19 Nov 2021 02:46 UTC

General information | **Advisor** | Vulnerability | Compliance | Patch

2 Recommendations

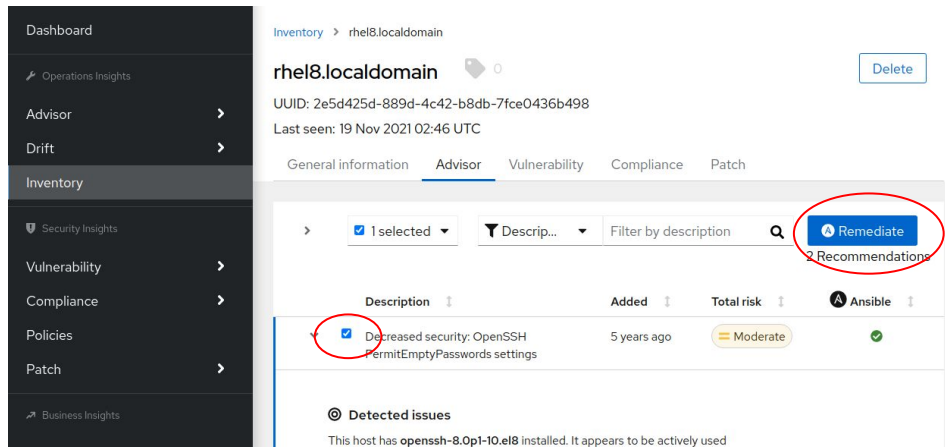
Description	Added	Total risk	Ansible
Decreased security: OpenSSH PermitEmptyPasswords settings	5 years ago	Moderate	✓

Detected issues

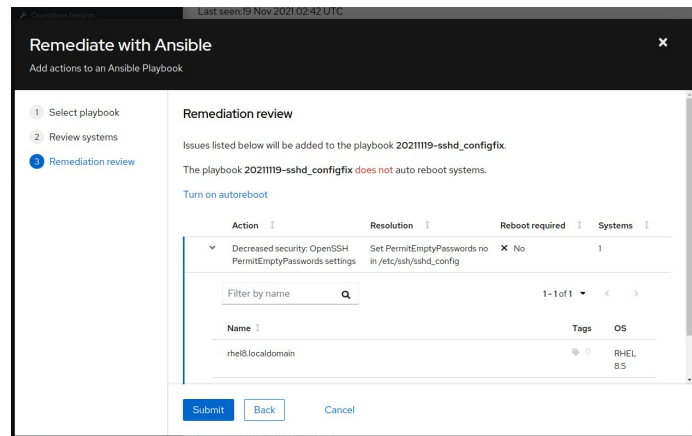
This host has **openssh-8.0p1-10.el8** installed. It appears to be actively used because the **sshd** service is enabled and an **sshd** process is running. The current settings might be required by your use case or needed for your other software configurations. However, **any deviation from the recommended practices should be carefully considered**. Red Hat recommends that you review the OpenSSH settings for all your reported servers, revise them, and leave detected, potentially problematic settings only where necessary.

Remediationを作成する

修正したい問題のチェックボックスを選択すると **Remediate** ボタンが有効化



ウィザード形式でRemediationを作成

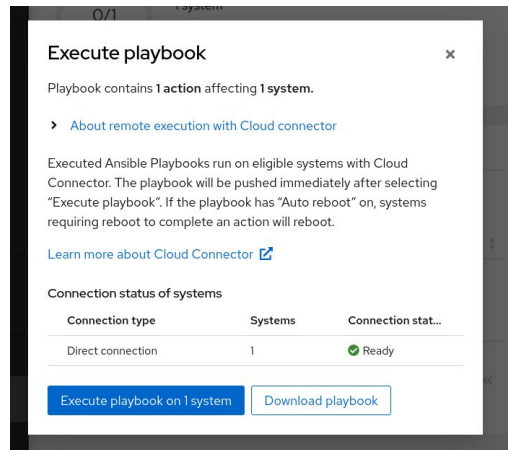
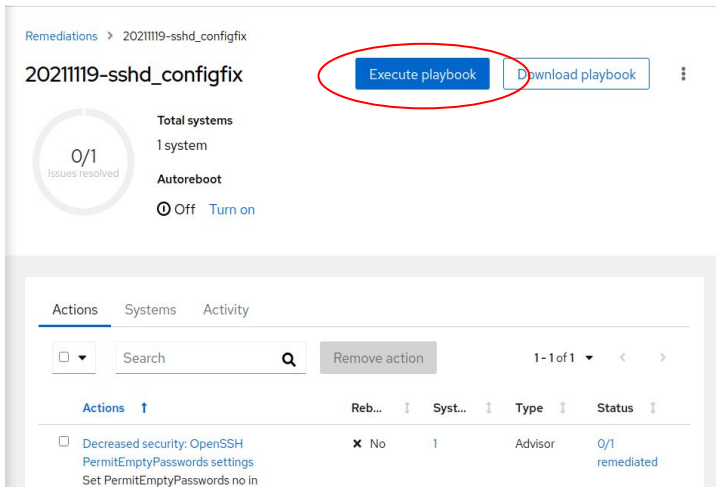


Remediationを実行する

作成したRemediation内で
Execute playbookボタンを押すと
実行確認のダイアログを表示

Execute playbook on X system ボタンを押すと
rhcd経由で修正用のansible playbookを実行

各システムのrhcdのログに実行の詳細が記録される



関連資料

公式ドキュメント

[Red Hat Connector Configuration Guide Red Hat Insights 2021](#)

Red Hat InsightsのGitHub

<https://github.com/RedHatInsights>

yggdrasil(rhcのupstream project)

<https://github.com/RedHatInsights/yggdrasil>

既知の問題

この資料を書いている間に気付いたものをメモしておきます。

- rhcdのエラーメッセージ
 - 起動時にcannot start watching '/etc/rhc/tags.toml': lstat /etc/rhc/tags.toml: no such file or directoryのようなメッセージが出る → optionalなファイルで安全に無視できる。ログのレベルを下げる予定。
 - ansible playbookを実行したあと cannot send message b8b503de-9ae3-4983-9a3d-12cf3dfa83f0: rpc error: code = Internal desc = Failed to serialize response! のようなメッセージが出る →調査中 [#2020426](#)
- ドキュメント
 - Red Hat ConnectのドキュメントにRemediation administrator roleが紹介されていないので不親切 → バグレポート済

想定Q&A

Q: rhcコマンドの利用は必須ですか？

A: いいえ。Red Hat Insightsを利用しない場合、問題なく無視することができます。

Q: rhcの利用にはSimple Content Access(SCA)が必須ですか？

A: SCAの利用が推奨されますが、必須ではありません。SCAを利用しない場合は別途subscription-managerでのサブスクリプションのattach操作が必要です。

Q: rhcを利用するとsubscription-managerは使わなくてよいですか？

A: rhcはRed Hat Subscription Managementへの登録だけを行います。リポジトリの有効化・無効化や、SCA無効時のサブスクリプションattachなどにはsubscription-managerの利用が必要です。

Thank you

Red Hat is the world's leading provider of
enterprise open source software solutions.
Award-winning support, training, and consulting
services make
Red Hat a trusted adviser to the Fortune 500.



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos



facebook.com/redhatinc



twitter.com/RedHat