



Red Hat Advanced Cluster Security for Kubernetes 3.70

アーキテクチャー

システムアーキテクチャー

Red Hat Advanced Cluster Security for Kubernetes 3.70 アーキテクチャー

システムアーキテクチャー

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

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Architecture.ent file |.

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

では、Red Hat Advanced Cluster Security for Kubernetes アーキテクチャーの概要および詳細を説明します。

目次

第1章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES アーキテクチャー	3
1.1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES アーキテクチャーの概要	3
Red Hat Advanced Cluster Security for Kubernetes バージョン 3.69.1 以降	3
Red Hat Advanced Cluster Security for Kubernetes version 3.69 以前	3
一元化されたサービス	3
Red Hat Advanced Cluster Security for Kubernetes バージョン 3.69.1 以降の Scanner アーキテクチャー	4
安全なクラスターサービス	4
1.2. 外部コンポーネント	5

第1章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES アーキテクチャー

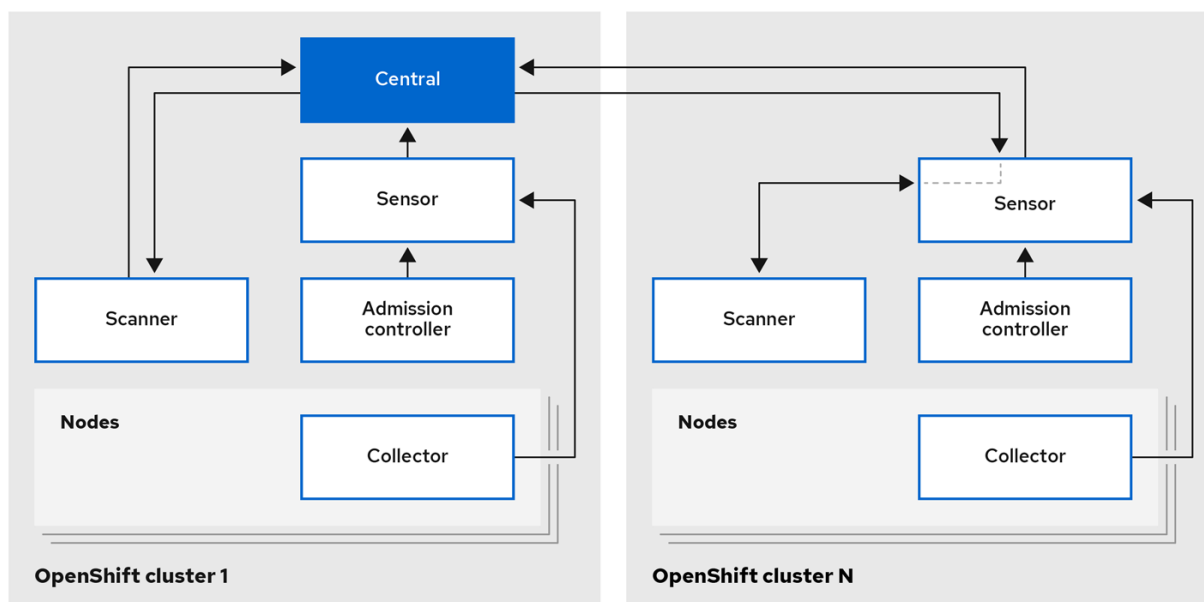
Red Hat Advanced Cluster Security for Kubernetes アーキテクチャーおよび概念をご覧ください。

1.1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES アーキテクチャーの概要

Red Hat Advanced Cluster Security for Kubernetes (RHACS) は、大規模なデプロイメントをサポートし、基盤となる OpenShift Container Platform ノードまたは Kubernetes ノードへの影響を最小限に抑えるように最適化された分散アーキテクチャーを使用します。OpenShift Container Platform または Kubernetes クラスターにコンテナセットとして RHACS をインストールします。RHACS には、RHACS によって保護された各クラスターにインストールするサービスと、1つのクラスターにインストールする集中型サービスが含まれます。

Red Hat Advanced Cluster Security for Kubernetes バージョン 3.69.1 以降

図1.1 OpenShift Container Platform 用のハイレベル Red Hat Advanced Cluster Security for Kubernetes アーキテクチャー



214_RHACS_0322

Red Hat Advanced Cluster Security for Kubernetes version 3.69 以前

Red Hat Advanced Cluster Security for Kubernetes バージョン 3.69 以前の場合、Scanner は、Central がインストールされているクラスターにのみインストールされます。

一元化されたサービス

一元化されたサービスを単一のクラスター (図1および2のクラスター1) にインストールします。これらのサービスには、Central と Scanner の2つの主要コンポーネントが含まれます。

- **Central:** Central セントラルは、RHACS アプリケーション管理インターフェイスおよびサービスです。データの永続性、API インタラクション、およびユーザーインターフェイス (RHACS ポータル) アクセスを処理します。同じ Central インスタンスを使用して、複数の OpenShift Container Platform または Kubernetes クラスターをセキュリティー保護できます。
- **Scanner:** Scanner は、コンテナイメージとそれに関連するデータベースをスキャンするため

に Red Hat が開発および認定した脆弱性 Scanner です。すべてのイメージレイヤーを分析して、Common Vulnerabilities and Exposures (CVE) リストから既知の脆弱性をチェックします。Scanner は、パッケージマネージャーによってインストールされたパッケージおよび複数のプログラミング言語の依存関係の脆弱性も識別します。

Red Hat Advanced Cluster Security for Kubernetes バージョン 3.69.1以降の Scanner アーキテクチャー

Red Hat Advanced Cluster Security for Kubernetes バージョン 3.69.1以降を OpenShift Container Platform にインストールする場合は、セキュリティーで保護された各クラスターに軽量バージョンの Scanner をインストールして (図 1)、統合された OpenShift Container Registry (OCR) でイメージをスキャンできるようにします。

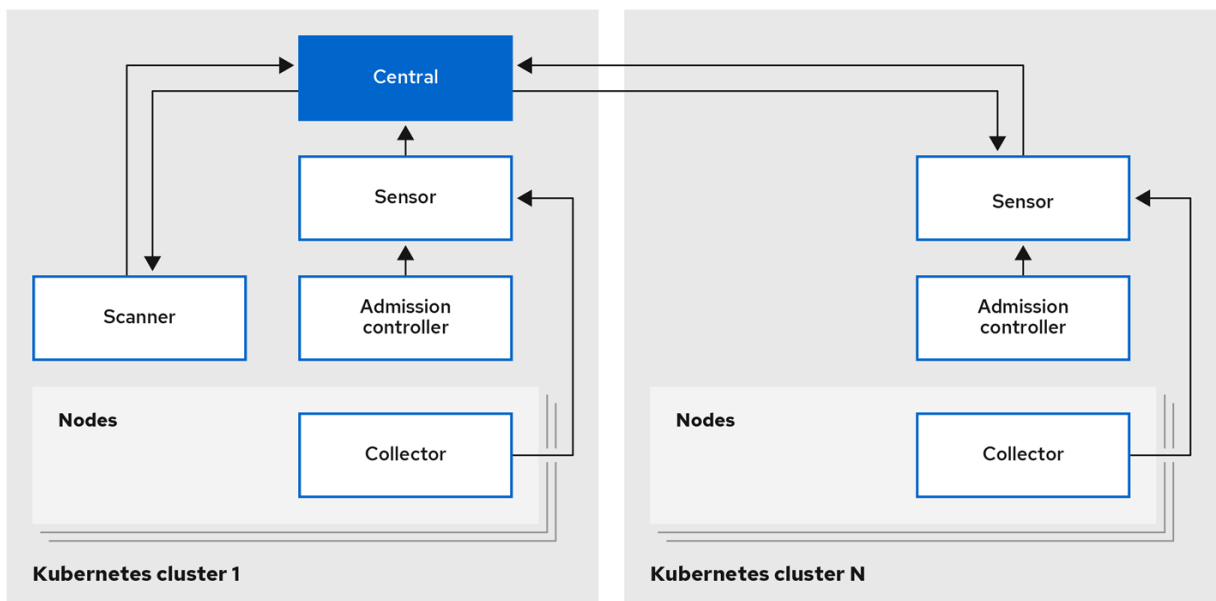
安全なクラスターサービス

Red Hat Advanced Cluster Security for Kubernetes (図 1 および 2 の **Cluster N**) を使用して、保護する各クラスターに保護されたクラスターサービスをインストールします。Central をインストールするクラスターも保護されており、これらのサービスが含まれています。

- **Sensor:** Sensor は、クラスターの分析と監視を担当するサービスです。これは、ポリシーの検出と適用のために OpenShift Container Platform または Kubernetes API サーバーとの対話を処理し、Collector と連携します。
- **管理コントローラー:** 管理コントローラーは、ユーザーが RHACS のセキュリティーポリシーに違反するワークロードを作成するのを防ぎます。
- **Collector:** Collector は、クラスターノード上のコンテナアクティビティーを分析および監視します。コンテナの実行時間とネットワークアクティビティーに関する情報を収集し、収集したデータを Sensor に送信します。
- **Scanner (OpenShift Container Platform バージョン 3.69.1以降のみ):** OpenShift Container Platform では、RHACS は各セキュアクラスターに軽量バージョンの Scanner をインストールし (図 1)、統合された OCR でイメージをスキャンできるようにします。

図 2 は、Scanner のみを中央にインストールする Kubernetes 環境のアーキテクチャーを示しています。

図1.2 Kubernetes 向け高レベル Red Hat Advanced Cluster Security for Kubernetes



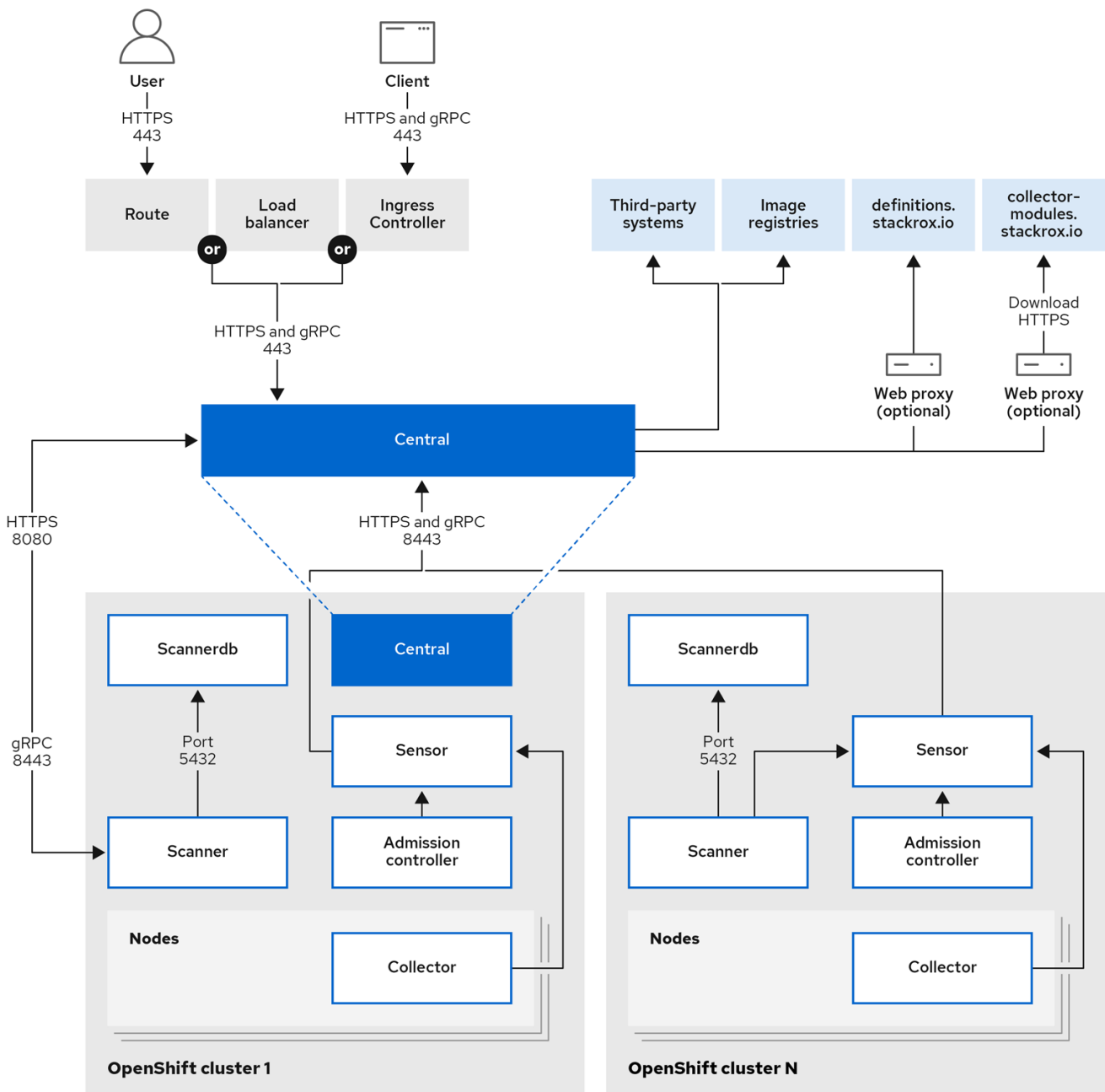
1.2. 外部コンポーネント

プライマリーサービスに加えて、Red Hat Advanced Cluster Security for Kubernetes は他のエンティティとも相互作用して、クラスターのセキュリティーを強化します。

図 3 は、OpenShift Container Platform の RHACS アーキテクチャーを示していますが、以下の例外に注意する必要があります。

- RHACS バージョン 3.69 以前では、Scanner サービスは集中型サービスで一度だけインストールされます。
- 他の Kubernetes ベースの環境では、Scanner サービスは集中型サービスで一度だけインストールされます。

図1.3 外部コンポーネント



214_RHACS_0322

Red Hat Advanced Cluster Security for Kubernetes は、以下の外部コンポーネントを使用します。

- **サードパーティーシステム:** RHACS を、CI/CD パイプライン、イベント管理 (SIEM) システム、ロギング、電子メールなどの他のシステムと統合できます。
- **イメージレジストリー:** RHACS をさまざまなイメージレジストリーと統合し、RHACS を使用してアクティブなイメージをスキャンおよび表示できます。保護されたクラスターで検出されたイメージプルシークレットを使用することにより、RHACS はこれらのレジストリー統合を自動的に設定します。
- **definitions.stackrox.io:** RHACS は、**definitions.stackrox.io** エンドポイントでさまざまな脆弱性フィードからのデータを集約し、この情報を Central に渡します。フィードには、一般、NVD、および Alpine、Debian、Ubuntu などのディストリビューション固有のものが含まれません。
- **collector-modules.stackrox.io:** Central は、**collector-modules.stackrox.io** にアクセスして、サポートされているカーネルモジュールを取得し、これらのモジュールを Sensor および Collector に渡します。

関連情報

- [イメージレジストリーとの統合](#)
- [CI システムとの統合](#)
- [syslog プロトコルを使用した統合](#)