



Red Hat Advanced Cluster Security for Kubernetes 3.73

アーキテクチャー

システムアーキテクチャー

法律上の通知

Copyright © 2023 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

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
1.2. セントラルサービス	5
1.3. 安全なクラスターサービス	5
1.4. 外部コンポーネント	6
1.5. OPENSIFT CONTAINER PLATFORM と KUBERNETES にインストールした場合のアーキテクチャーの違い	6
1.6. サービス間の対話	7

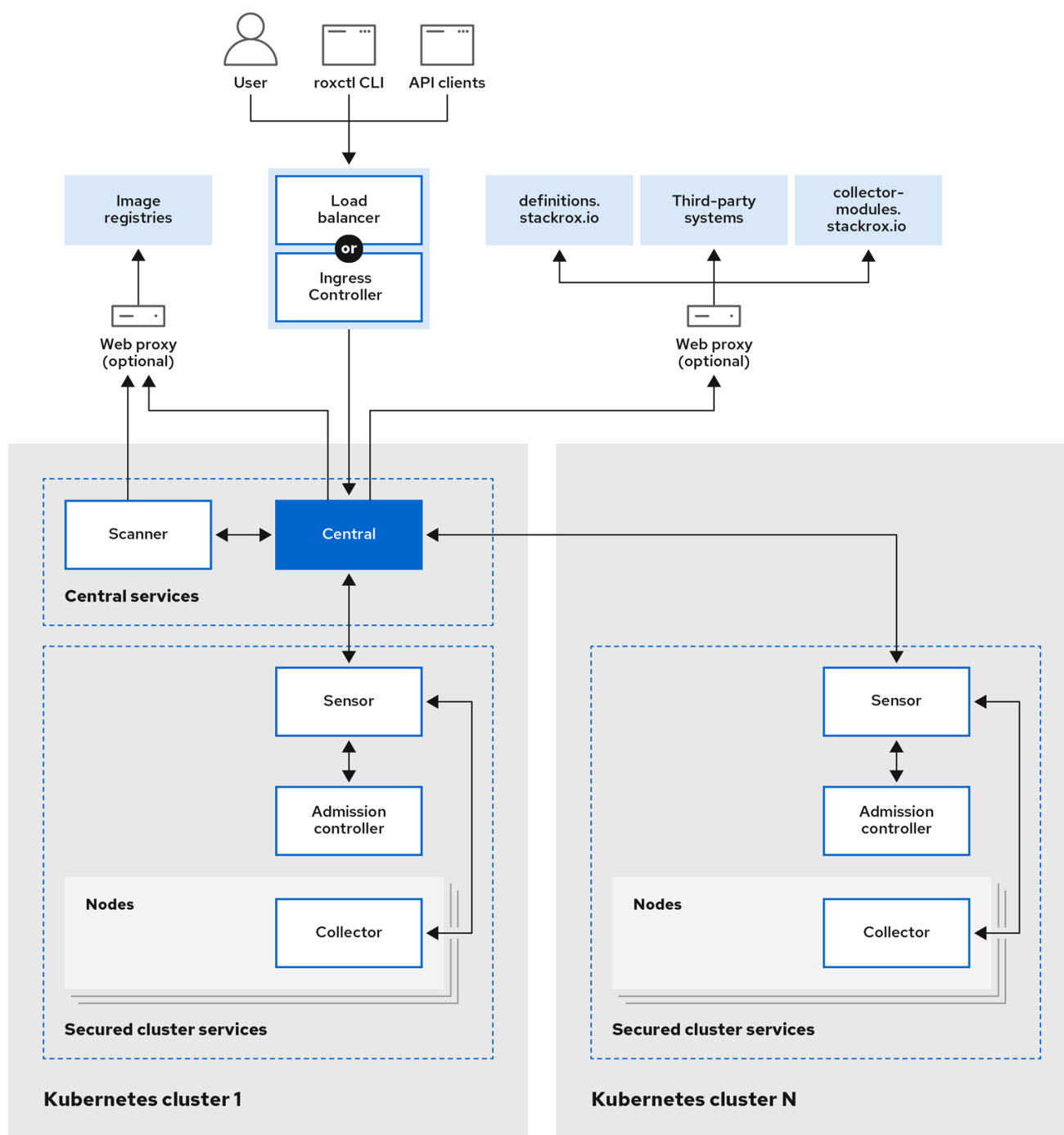
第1章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES アーキテクチャー

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。

図1.1 Kubernetes 向け Red Hat Advanced Cluster Security for Kubernetes アーキテクチャー



214_RHACS_0123



注記

RHACS を Kubernetes 上と OpenShift Container 上にインストールする場合、アーキテクチャーはわずかに異なります。ただし、基礎となるコンポーネントとそれらの間のインタラクションは同じままです。

OpenShift Container Platform または Kubernetes クラスターにコンテナーセットとして RHACS をインストールします。RHACS には以下が含まれます。

- 1つのクラスターにインストールするセントラルサービス。

- RHACS によりセキュリティ保護する各クラスターにインストールするセキュアなクラスターサービス。

これらの主要サービスに加え、RHACS は他の外部コンポーネントとも対話して、クラスターのセキュリティを強化します。

関連情報

- [OpenShift Container Platform と Kubernetes にインストールした場合のアーキテクチャーの違い](#)
- [外部コンポーネント](#)

1.2. セントラルサービス

単一のクラスターにセントラルサービスを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保護できます。
- **Scanner:** Scanner は、Red Hat が開発および認定した、コンテナイメージをスキャンするための脆弱性スキャナーです。Scanner は次の機能を実行します。
 - 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。
 - インストールされているパッケージの脆弱性と、複数のプログラミング言語の依存関係を特定します。コンテナイメージのスキャンに加えて、Scanner はノードのオペレーティングシステムとオーケストレーターの脆弱性を特定します。たとえば、ノードをスキャンして、Kubernetes、OpenShift Container Platform、Istio の脆弱性を特定します。

1.3. 安全なクラスターサービス

Red Hat Advanced Cluster Security for Kubernetes を使用してセキュリティ保護するすべてのクラスター (Central をインストールしたクラスターを含む) に、セキュアなクラスターサービスをインストールします。セキュリティで保護されたクラスターサービスには、次のコンポーネントが含まれます。

- **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。Sensor は、OpenShift Container Platform または Kubernetes API および Collector イベントをリッスンして、クラスターの現在の状態を報告します。Sensor は、RHACS ポリシーに基づいてデプロイタイムおよびランタイムの違反もトリガーします。さらに、Sensor は、ネットワークポリシーの適用、RHACS ポリシーの再処理の開始、Admission コントローラーとの対話など、すべてのクラスターの対話を担当します。
- **Admission コントローラー:** Admission コントローラーは、ユーザーが RHACS のセキュリティ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を分析および監視します。コンテナのランタイムとネットワークアクティビティの情報を収集し、収集したデータを Sensor に送信します。
- **Scanner:** Kubernetes では、セキュアなクラスターサービスに Scanner は含まれません。ただし、OpenShift Container Platform では、RHACS は統合された OpenShift Container Platform

レジストリー内のイメージをスキャンするために、セキュアなクラスターごとに軽量 Scanner バージョンをインストールします。

1.4. 外部コンポーネント

Red Hat Advanced Cluster Security for Kubernetes (RHACS) は、以下の外部コンポーネントと対話します。

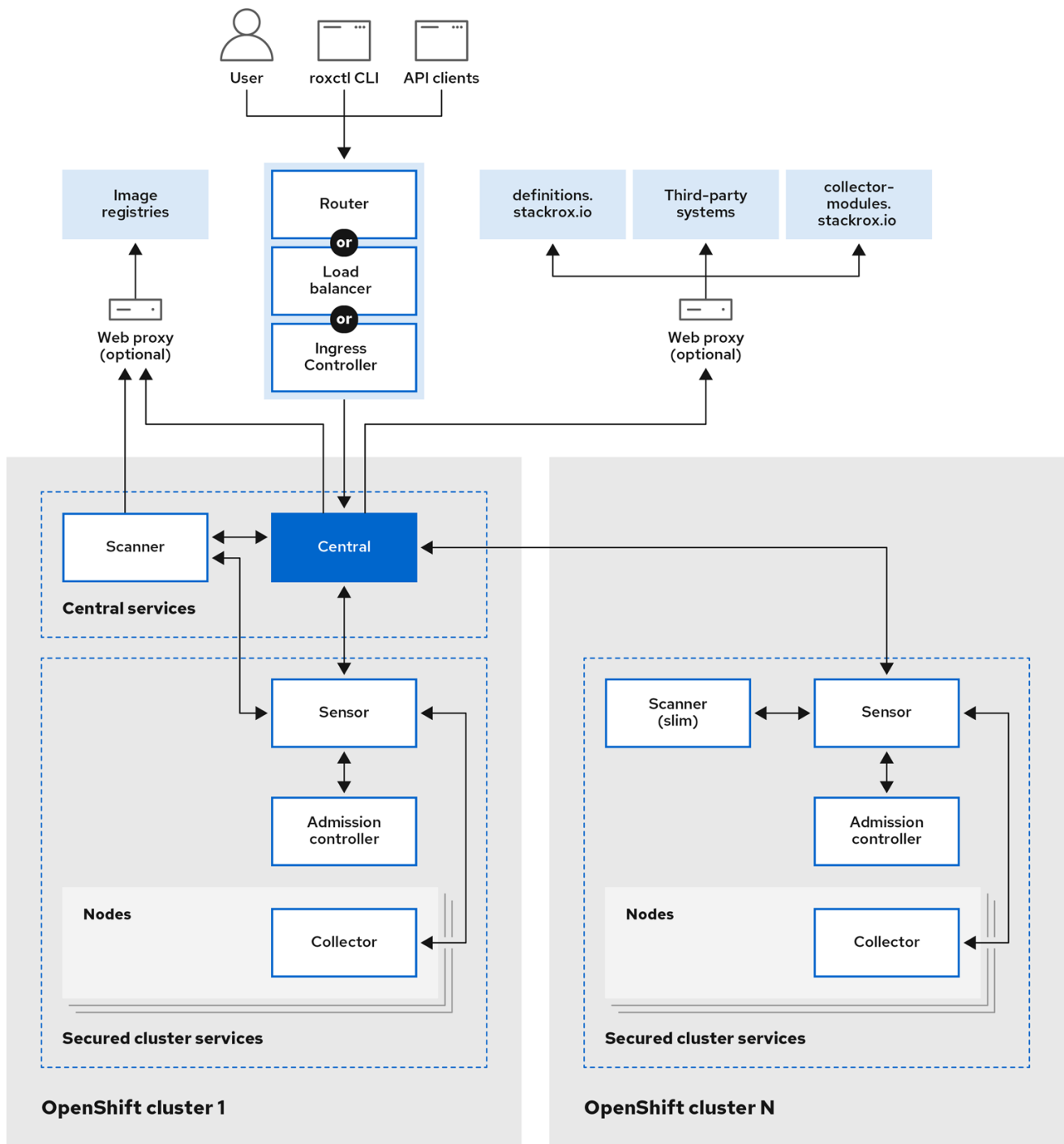
- **サードパーティーシステム:** RHACS を、CI/CD パイプライン、イベント管理 (SIEM) システム、ロギング、電子メールなどの他のシステムと統合できます。
- **roxctl:** roxctl は、RHACS でコマンドを実行するためのコマンドラインインターフェイス (CLI) です。
- **イメージレジストリー:** RHACS をさまざまなイメージレジストリーと統合し、RHACS を使用してイメージをスキャンおよび表示できます。RHACS は、セキュアなクラスターで検出されたイメージプルシークレットを使用して、アクティブなイメージのレジストリー統合を自動的に設定します。ただし、非アクティブなイメージをスキャンするには、レジストリー統合を手動で設定する必要があります。
- **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、一般的な National Vulnerability Database (NVD) データと、Alpine、Debian、Ubuntu などのディストリビューション固有のデータが含まれます。
- **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 Collector に渡します。

1.5. OPENSIFT CONTAINER PLATFORM と KUBERNETES にインストールした場合のアーキテクチャーの違い

RHACS を OpenShift Container Platform にインストールする場合、アーキテクチャー上の違いは 2 つだけです。

1. Operator または Helm インストール方法を使用して OpenShift Container Platform に RHACS をインストールすると、RHACS はすべてのセキュアなクラスターに Scanner の軽量バージョンをインストールします。軽量の Scanner は、統合された OpenShift Container Registry (OCR) 内のイメージのスキャンを可能にします。
2. Sensor は、Central をインストールしたクラスター内の Scanner と通信します。この接続により、クラスターに接続されている内部レジストリーにアクセスできます。

図1.2 OpenShift Container Platform 向け Red Hat Advanced Cluster Security for Kubernetes アーキテクチャー



214_RHACS_0123

1.6. サービス間の対話

このセクションでは、RHACS サービスがどのように対話するかについて説明します。

コンポーネント	方向	対話先	説明
---------	----	-----	----

コンポーネント	方向	対話先	説明
Central	■	Scanner	Central と Scanner の間に双方向通信があります。Central は Scanner にイメージスキャンを要求し、Scanner は Central に CVE データベースの更新を要求します。
Central	→	definitions.stackrox.io	Central は、 definitions.stackrox.io エンドポイントに接続して、集約された脆弱性情報を受信します。
Central	→	collector-modules.stackrox.io	Central は、サポートされているカーネルモジュールを collector-modules.stackrox.io からダウンロードします。
Central	→	イメージレジストリー	Central はイメージレジストリーにクエリーを実行して、イメージメタデータを取得します。たとえば、RHACS ポータルで Dockerfile の手順を表示します。
Scanner	→	イメージレジストリー	Scanner はイメージレジストリーからイメージをプルして、脆弱性を特定します。
Sensor	■	Central	Central と Sensor の間には双方向通信があります。Sensor は、センサーバンドル設定の更新をダウンロードするために定期的に Central をポーリングします。また、セキュアなクラスターで観察されたアクティビティと観察されたポリシー違反のイベントも送信します。Central は Sensor と通信して、有効なポリシーに対してすべてのデプロイメントの再処理を強制します。
Sensor	■	Scanner	OpenShift Container Platform でのみ、Sensor は Scanner と通信して、クラスターに接続されたローカルレジストリーにアクセスします。Scanner は Sensor と通信して、 definitions.stackrox.io からデータを要求します。
Collector	■	Sensor	Collector は Sensor と通信し、すべてのイベントをクラスターのそれぞれの Sensor に送信します。Collector は、不明ドライバーも Sensor に要求します。Sensor は、Collector にコンプライアンススキャン結果を要求します。さらに Sensor は、Central から外部の Classless Inter-Domain Routing 情報を受け取り、それを Collector にプッシュします。

コンポーネント	方向	対話先	説明
受付コントローラー	■	Sensor	Sensor は、適用するセキュリティーポリシーのリストを Admission コントローラーに送信します。Admission コントローラーは、セキュリティーポリシー違反アラートを Sensor に送信します。Admission コントローラーは、必要に応じて Sensor にイメージスキャンを要求することもできます。
受付コントローラー	→	Central	これは一般的ではありません。ただし、Central エンドポイントが判明しており、かつ Sensor が使用できない場合、Admission コントローラーは Central と直接通信できます。