Red Hat Advanced Cluster Security for Kubernetes 4.4

Architecture

System architecture

Last Updated: 2024-06-27

Red Hat Advanced Cluster Security for Kubernetes 4.4 Architecture

System architecture

Legal Notice

Abstract

Provides an overview and description of the Red Hat Advanced Cluster Security for Kubernetes architecture.

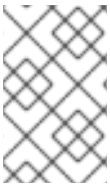
Table of Contents

CHAPTER 1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES ARCHITECTURE

Discover Red Hat Advanced Cluster Security for Kubernetes architecture and concepts.

1.1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES ARCHITECTURE OVERVIEW

Red Hat Advanced Cluster Security for Kubernetes (RHACS) uses a distributed architecture that supports high-scale deployments and is optimized to minimize the impact on the underlying OpenShift Container Platform or Kubernetes nodes.

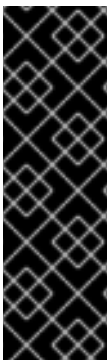


NOTE

The architecture is slightly different when you install RHACS on Kubernetes and in OpenShift Container Platform. However, the underlying components and the interactions between them remain the same.

RHACS architecture for Kubernetes

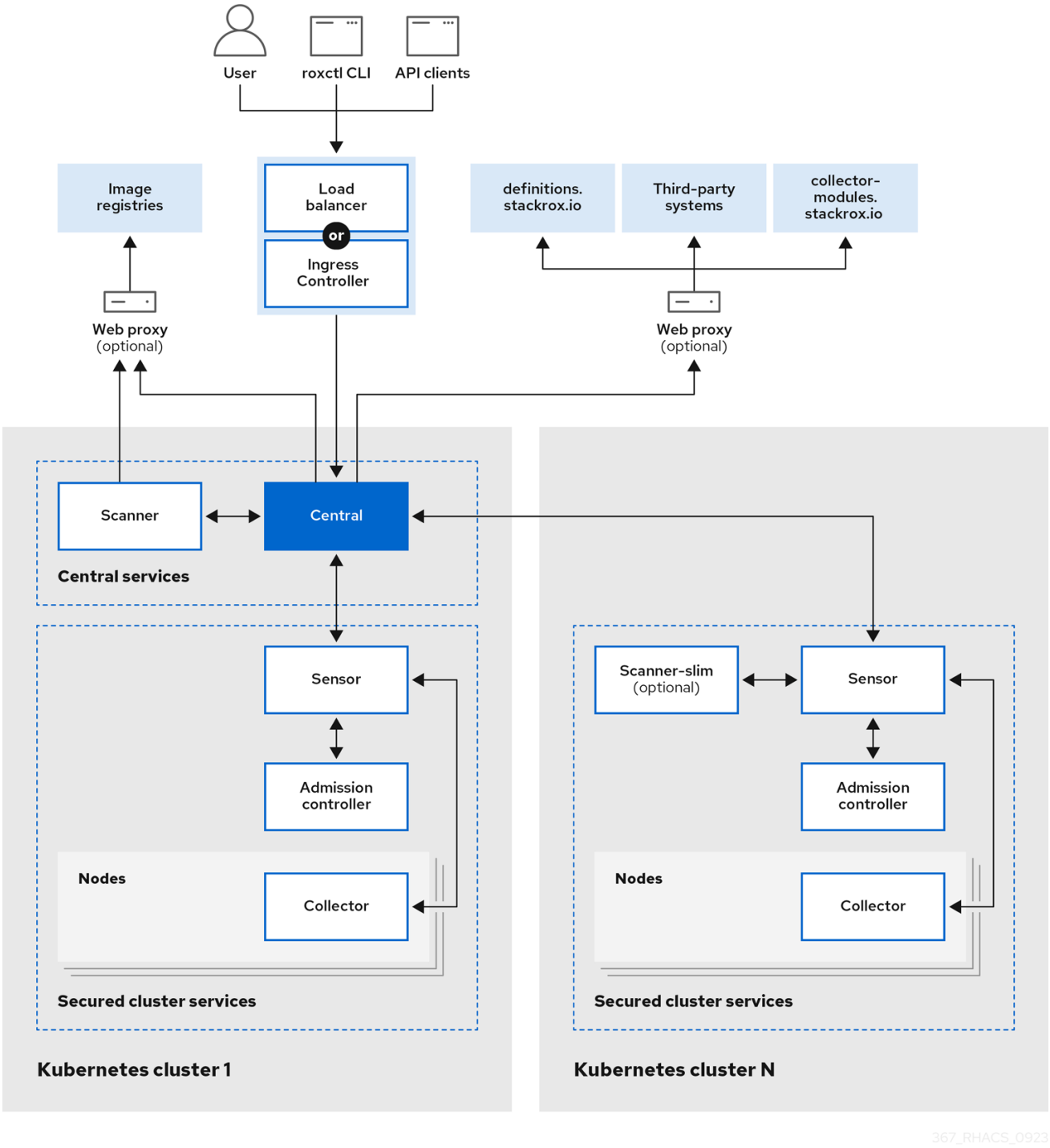
The following graphic shows the architecture with the StackRox Scanner. For version 4.4, Scanner V4 is available. Installation of Scanner V4 is optional, but provides additional benefits.



IMPORTANT

Scanner V4 is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope .



You install RHACS as a set of containers in your OpenShift Container Platform or Kubernetes cluster. RHACS includes the following services:

- Central services you install on one cluster
- Secured cluster services you install on each cluster you want to secure by RHACS

In addition to these primary services, RHACS also interacts with other external components to enhance your clusters' security.

Additional resources

- Architectural differences between installation on OpenShift Container Platform and Kubernetes

- External components

1.2. CENTRAL SERVICES

You install Central services on a single cluster. These services include the following components:

- **Central**: Central is the RHACS application management interface and services. It handles API interactions and user interface (RHACS Portal) access. You can use the same Central instance to secure multiple OpenShift Container Platform or Kubernetes clusters.
- **Central DB**: Central DB is the database for RHACS and handles all data persistence. It is currently based on PostgreSQL 13.
- **Scanner V4** (Technology Preview): Beginning with version 4.4, RHACS contains the Scanner V4 vulnerability scanner for scanning container images. Scanner V4 is built on ClairCore, which also powers the Clair scanner. Scanner V4 supports scanning of language and OS-specific image components. For version 4.4, you must use this scanner in conjunction with the StackRox Scanner to provide node and platform scanning capabilities until Scanner V4 support those capabilities. Scanner V4 contains the Indexer, Matcher, and DB components.

IMPORTANT

Scanner V4 is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope .

  - **Scanner V4 Indexer**: The Scanner V4 Indexer performs image indexing, previously known as image analysis. Given an image and registry credentials, the Indexer pulls the image from the registry. It finds the base operating system, if it exists, and looks for packages. It stores and outputs an index report, which contains the findings for the given image.
  - **Scanner V4 Matcher**: The Scanner V4 Matcher performs vulnerability matching. If the Central services Scanner V4 Indexer indexed the image, then the Matcher fetches the index report from the Indexer and matches the report with the vulnerabilities stored in the Scanner V4 database. If a Secured Cluster services Scanner V4 Indexer performed the indexing, then the Matcher uses the index report that was sent from that Indexer, and then matches against vulnerabilities. The Matcher also fetches vulnerability data and updates the Scanner V4 database with the latest vulnerability data. The Scanner V4 Matcher outputs a vulnerability report, which contains the final results of an image.
  - **Scanner V4 DB**: This database stores information for Scanner V4, including all vulnerability data and index reports. A persistent volume claim (PVC) is required for Scanner V4 DB on the cluster where Central is installed.
- **StackRox Scanner**: The StackRox Scanner is the default scanner in RHACS. Version 4.4 adds a new scanner, Scanner V4. The StackRox Scanner originates from a fork of the Clair v2 open source scanner. You must continue using this scanner for RHCOS node scanning and platform scanning.

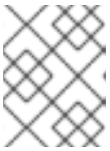
- **Scanner-DB**: This database contains data for the StackRox Scanner.

RHACS scanners analyze each image layer to determine the base operating system and identify programming language packages and packages that were installed by the operating system package manager. They match the findings against known vulnerabilities from various vulnerability sources. In addition, the StackRox Scanner identifies vulnerabilities in the node's operating system and platform. These capabilities are planned for Scanner V4 in a future release.

1.2.1. Vulnerability sources

RHACS uses the following vulnerability sources:

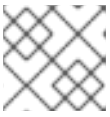
- Alpine Security Database
- Data tracked in Amazon Linux Security Center
- Debian Security Tracker
- Oracle OVAL
- Photon OVAL
- Red Hat OVAL
- Red Hat CVE Map: This is used for images which appear in the Red Hat Container Catalog.
- SUSE OVAL
- Ubuntu OVAL
- OSV: This is used for language-related vulnerabilities, such as Go, Java, Node.js (JavaScript), Python, and Ruby. This source might provide GitHub Security Advisory (GHSA) IDs rather than CVE numbers for vulnerabilities.



NOTE

The RHACS Scanner V4 uses the OSV database available at OSV.dev under this license.

- NVD: This used for various purposes such as filling in information gaps when vendors do not provide information. For example, Alpine does not provide a description, CVSS score, severity, or published date.



NOTE

This product uses the NVD API but is not endorsed or certified by the NVD.

- StackRox: The upstream StackRox project maintains a set of vulnerabilities that might not be discovered due to data formatting from other sources or absence of data.

The Scanner V4 Indexer uses the following sources:

- repository-to-cpe.json: Maps RPM repositories to their related CPEs, which is required for matching vulnerabilities for RHEL-based images.

- container-name-repos-map.json: This matches container names to the repositories to which they are shipped.

1.3. SECURED CLUSTER SERVICES

You install the secured cluster services on each cluster that you want to secure by using the RHACS Cloud Service. Secured cluster services include the following components:

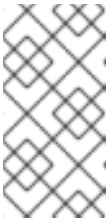
- **Sensor**: Sensor is the service responsible for analyzing and monitoring the cluster. Sensor listens to the OpenShift Container Platform or Kubernetes API and Collector events to report the current state of the cluster. Sensor also triggers deploy-time and runtime violations based on RHACS Cloud Service policies. In addition, Sensor is responsible for all cluster interactions, such as applying network policies, initiating reprocessing of RHACS Cloud Service policies, and interacting with the Admission controller.
- **Admission controller**: The Admission controller prevents users from creating workloads that violate security policies in RHACS Cloud Service.
- **Collector**: Collector analyzes and monitors container activity on cluster nodes. It collects container runtime and network activity information and sends the collected data to Sensor.
- **StackRox Scanner**: In Kubernetes, the secured cluster services include Scanner-slim as an optional component. However, on OpenShift Container Platform, RHACS Cloud Service installs a Scanner-slim version on each secured cluster to scan images in the OpenShift Container Platform integrated registry and optionally other registries.
- **Scanner-DB**: This database contains data for the StackRox Scanner.
- **Scanner V4**: Scanner V4 components are installed on the secured cluster if enabled.

IMPORTANT

Scanner V4 is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope .

  - **Scanner V4 Indexer**: The Scanner V4 Indexer performs image indexing, previously known as image analysis. Given an image and registry credentials, the Indexer pulls the image from the registry. It finds the base operating system, if it exists, and looks for packages. It stores and outputs an index report, which contains the findings for the given image.
  - **Scanner V4 DB**: This component is installed if Scanner V4 is enabled. This database stores information for Scanner V4, including index reports. For best performance, configure a persistent volume claim (PVC) for Scanner V4 DB.



NOTE

When secured cluster services are installed on the same cluster as Central services and installed in the same namespace, secured cluster services do not deploy Scanner V4 components. Instead, it is assumed that Central services already include a deployment of Scanner V4.

1.4. EXTERNAL COMPONENTS

Red Hat Advanced Cluster Security for Kubernetes (RHACS) interacts with the following external components:

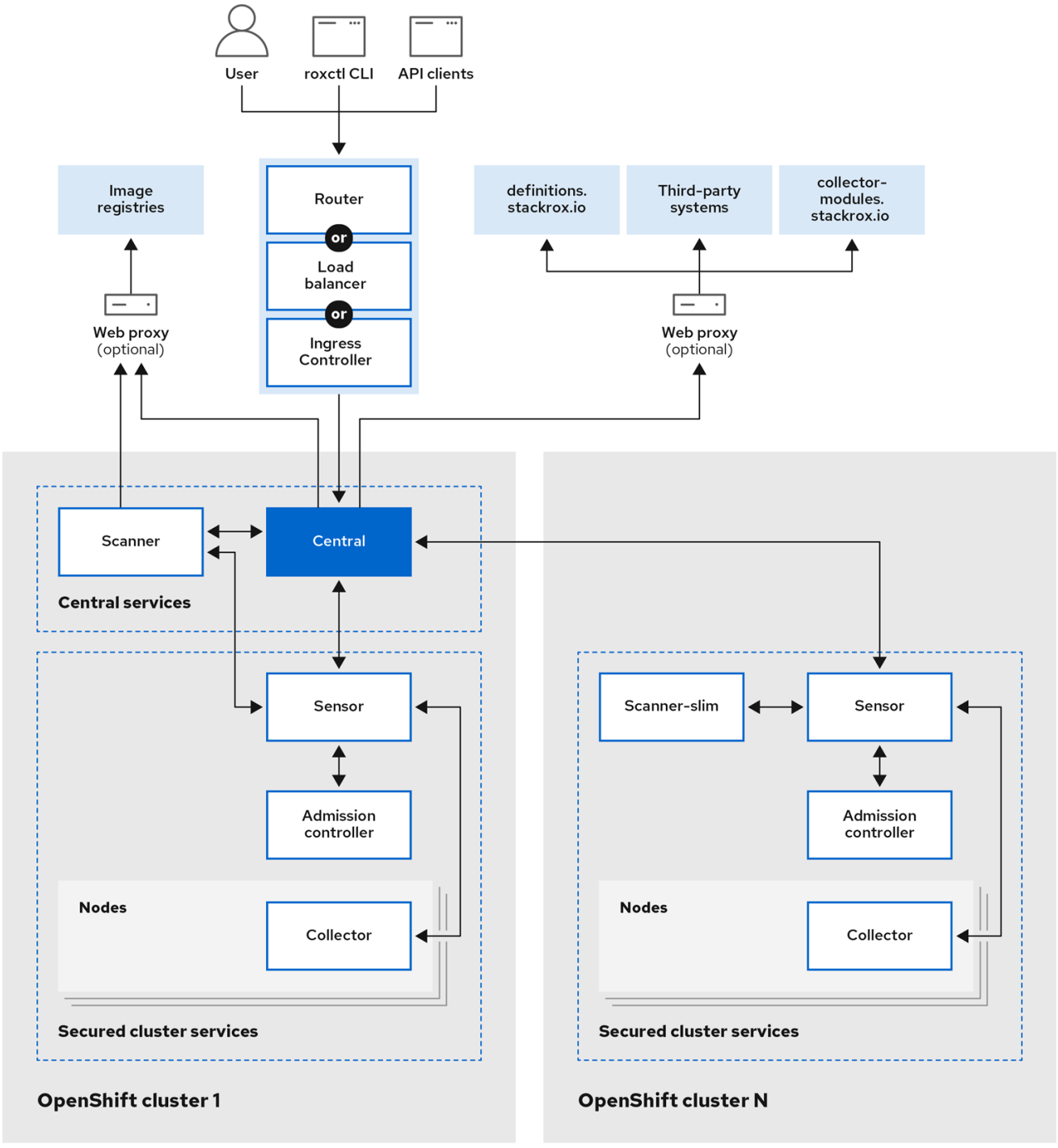
- **Third-party systems**: You can integrate RHACS with other systems such as CI/CD pipelines, event management (SIEM) systems, logging, email, and more.
- **roxctl**: **roxctl** is a command-line interface (CLI) for running commands on RHACS.
- **Image registries**: You can integrate RHACS with various image registries and use RHACS to scan and view images. RHACS automatically configures registry integrations for active images by using the image pull secrets discovered in secured clusters. However, for scanning inactive images, you must manually configure registry integrations.
- **definitions.stackrox.io**: RHACS aggregates the data from various vulnerability feeds at the **definitions.stackrox.io** endpoint and passes this information to Central. The feeds include general, National Vulnerability Database (NVD) data, and distribution-specific data, such as Alpine, Debian, and Ubuntu.
- **collector-modules.stackrox.io**: Central reaches out to **collector-modules.stackrox.io** to obtain supported kernel modules and passes on these modules to Collector.

1.5. ARCHITECTURAL DIFFERENCES BETWEEN INSTALLATION ON OPENSHIFT CONTAINER PLATFORM AND KUBERNETES

When you install RHACS on the OpenShift Container Platform, there are only two architectural differences:

1. RHACS installs a lightweight version of Scanner on every secured cluster when you install RHACS on the OpenShift Container Platform using the Operator or the Helm install method. The lightweight Scanner enables the scanning of images in the integrated OpenShift Container Registry (OCR).
2. Sensor communicates with Scanner in the cluster where you have installed Central. This connection allows accessing internal registries attached to the cluster.

Figure 1.1. Red Hat Advanced Cluster Security for Kubernetes architecture for OpenShift Container Platform



1.6. INTERACTION BETWEEN THE SERVICES

This section explains how RHACS services interact with each other.

Table 1.1. RHACS with Scanner V4

Component	Direction	Component	Description
Central	▮	Scanner V4 Indexer	Central requests the Indexer to download and index (analyze) given images. This process results in an index report. Scanner V4 Indexer requests mapping files from Central that assist the indexing process.
Central	▮	Scanner V4 Matcher	Central requests that the Scanner V4 Matcher match given images to known vulnerabilities. This process results in the final scan result: a vulnerability report. Scanner V4 Matcher requests the latest vulnerabilities from Central.
Sensor	▮	Scanner V4 Indexer	**SecuredCluster** scanning is enabled by default in Red Hat OpenShift environments deployed by using the Operator or when delegated scanning is used. When **SecuredCluster** scanning is enabled, Sensor requests Scanner V4 to index images. Scanner V4 Indexer requests mapping files from Sensor that assist the indexing process unless Central exists in the same namespace. In that case, Central is contacted instead.
Scanner V4 Indexer	→	Image Registries	The Indexer pulls image metadata from registries to determine the layers of the image, and downloads each previously unindexed layer.
Scanner V4 Matcher	→	Scanner V4 Indexer	Scanner V4 Matcher requests the results of the image indexing, the index report, from the Indexer. It then uses the report to determine relevant vulnerabilities. This interaction occurs only when the image is indexed in the Central cluster. This interaction does not occur when Scanner V4 is matching vulnerabilities for images indexed in secured clusters.
Scanner V4 Indexer	→	Scanner V4 DB	The Indexer stores data related to the indexing results to ensure that image layers are only downloaded and indexed once. This prevents unnecessary network traffic and other resource utilization.
Scanner V4 Matcher	→	Scanner V4 DB	Scanner V4 Matcher stores all of its vulnerability data in the database and periodically updates this data. Scanner V4 indexer also queries this data as part of the vulnerability matching process.

Component	Direction	Component	Description
Sensor	↕	Central	There is bidirectional communication between Central and Sensor. Sensor polls Central periodically to download updates for the sensor bundle configuration. It also sends events for the observed activity for the secured cluster and observed policy violations. Central communicates with Sensor to force reprocessing of all deployments against enabled policies.
Collector	↕	Sensor	Collector communicates with Sensor and sends all of the events to the respective Sensor for the cluster. On supported OpenShift Container Platform clusters, Collector analyzes the software packages installed on the nodes and sends them to Sensor so that Scanner can later scan them for vulnerabilities. Collector also requests missing drivers from Sensor. Sensor requests compliance scan results from Collector. Additionally, Sensor receives external Classless Inter-Domain Routing information from Central and pushes it to Collector.
Admission controller	↕	Sensor	Sensors send the list of security policies to enforce to Admission controller. Admission controller sends security policy violation alerts to Sensor. Admission controller can also request image scans from Sensor when required.
Admission controller	→	Central	It is not common; however, Admission controller can communicate with Central directly if the Central endpoint is known and Sensor is unavailable.

IMPORTANT

Scanner V4 is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope .

Table 1.2. RHACS with the StackRox Scanner

Component	Direction	Interacts with	Description
Central	↔	Scanner	There is bidirectional communication between Central and Scanner. Central requests image scans from Scanner, and Scanner requests updates to its CVE database from Central.
Central	→	**definitions.stackrox.io**	Central connects to the **definitions.stackrox.io** endpoint to receive the aggregated vulnerability information.
Central	→	**collector-modules.stackrox.io**	Central downloads supported kernel modules from **collector-modules.stackrox.io**.
Central	→	Image registries	Central queries the image registries to get image metadata. For example, to show Dockerfile instructions in the RHACS portal.
Scanner	→	Image registries	Scanner pulls images from the image registry to identify vulnerabilities.
Sensor	↔	Central	There is bidirectional communication between Central and Sensor. Sensor polls Central periodically for downloading updates for the sensor bundle configuration. It also sends events for the observed activity for the secured cluster and observed policy violations. Central communicates with Sensor to force reprocessing of all deployments against enabled policies.
Sensor	↔	Scanner	Only in OpenShift Container Platform, Sensor communicates with Scanner to access the local registry attached to the cluster. Scanner communicates with Sensor to request data from **definitions.stackrox.io**.
Collector	↔	Sensor	Collector communicates with Sensor and sends all of the events to the respective Sensor for the cluster. On supported OpenShift Container Platform clusters, Collector analyzes the software packages installed on the nodes and sends them to Sensor so that Scanner can later scan them for vulnerabilities. Collector also requests missing drivers from Sensor. Sensor requests compliance scan results from Collector. Additionally, Sensor receives external Classless Inter-Domain Routing information from Central and pushes it to Collector.

Component	Direction	Interacts with	Description
Admission controller	▮	Sensor	Sensors send the list of security policies to enforce to Admission controller. Admission controller sends security policy violation alerts to Sensor. Admission controller can also request image scans from Sensor when required.
Admission controller	→	Central	It is not common; however, Admission controller can communicate with Central directly if the Central endpoint is known and Sensor is unavailable.