Red Hat Advanced Cluster Security for Kubernetes 3.74

Architecture

System architecture

Last Updated: 2023-03-21

Red Hat Advanced Cluster Security for Kubernetes 3.74 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 3
1.1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES ARCHITECTURE OVERVIEW 3
1.2. CENTRAL SERVICES 5
1.3. SECURED CLUSTER SERVICES 5
1.4. EXTERNAL COMPONENTS 5
1.5. ARCHITECTURAL DIFFERENCES BETWEEN INSTALLATION ON OPENSHIFT CONTAINER PLATFORM AND KUBERNETES 6
1.6. INTERACTION BETWEEN THE SERVICES 7

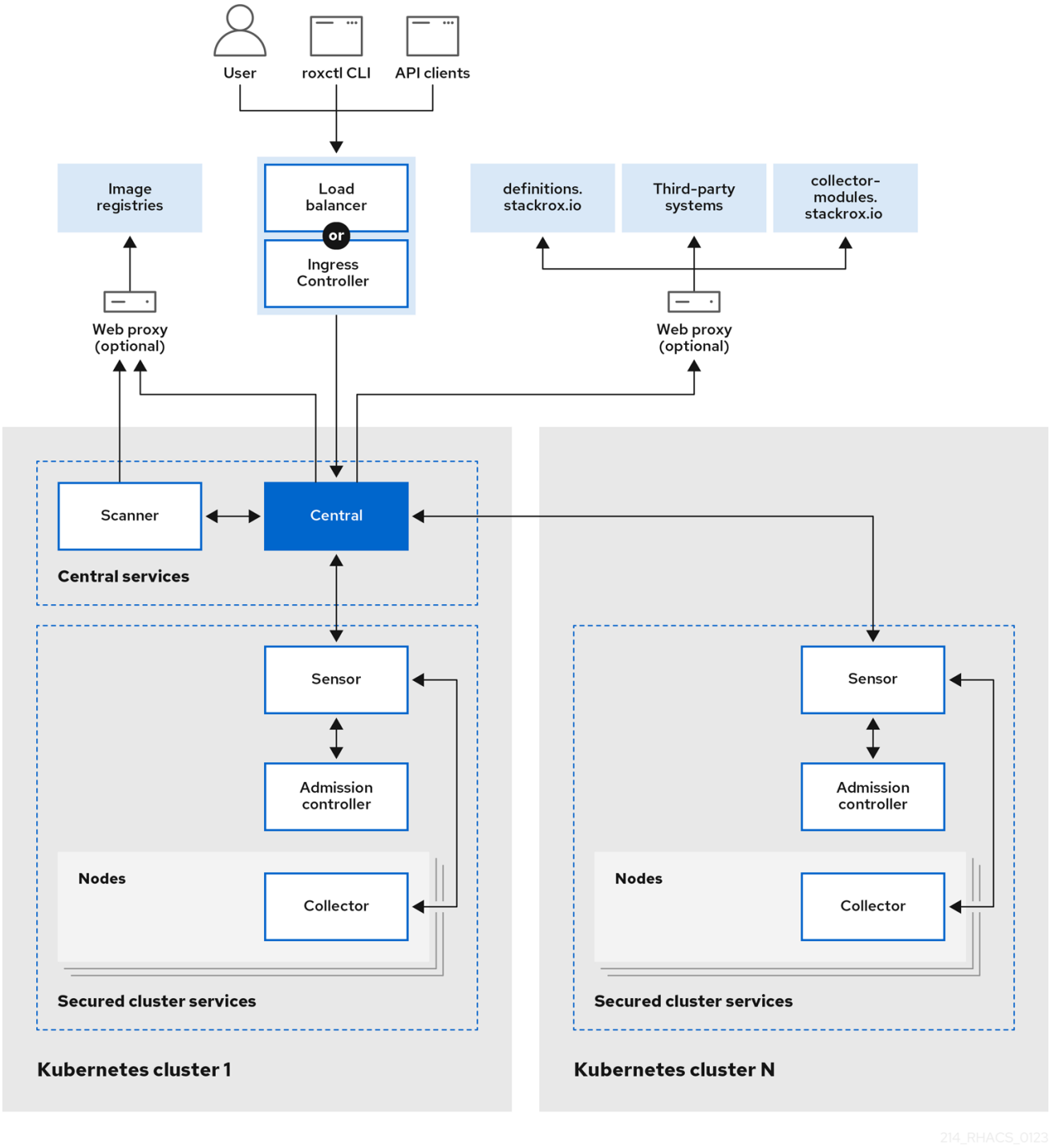
CHAPTER 1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES ARCHITECTURE

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.

Figure 1.1. Red Hat Advanced Cluster Security for Kubernetes architecture for Kubernetes



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.

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

- 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 two main components, Central and Scanner.

- **Central**: Central is the RHACS application management interface and services. It handles data persistence, API interactions, and user interface (RHACS Portal) access. You can use the same Central instance to secure multiple OpenShift Container Platform or Kubernetes clusters.
- **Scanner**: Scanner is a Red Hat-developed and certified vulnerability scanner for scanning container images. Scanner performs the following functions:
    - It analyzes all image layers and checks for known vulnerabilities from the Common Vulnerabilities and Exposures (CVEs) list.
    - It identifies vulnerabilities in installed packages and dependencies for multiple programming languages. In addition to scanning container images, Scanner identifies vulnerabilities in the node's operating system and orchestrators. For example, it scans nodes to identify Kubernetes, OpenShift Container Platform, and Istio vulnerabilities.

1.3. SECURED CLUSTER SERVICES

You install the secured cluster services on every cluster you want to secure by using the Red Hat Advanced Cluster Security for Kubernetes, including the cluster where you have installed Central. 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 policies. Additionally, Sensor is responsible for all cluster interactions, such as applying network policies, initiating reprocessing of RHACS policies, and interacting with the Admission controller.
- **Admission controller**: The Admission controller prevents users from creating workloads that violate security policies in RHACS.
- **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.
- **Scanner**: On Kubernetes, the Secured cluster services do not include Scanner. However, on the OpenShift Container Platform, RHACS installs a lightweight Scanner version on each secured cluster to scan images in the integrated OpenShift Container Platform registry.

1.4. EXTERNAL COMPONENTS

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

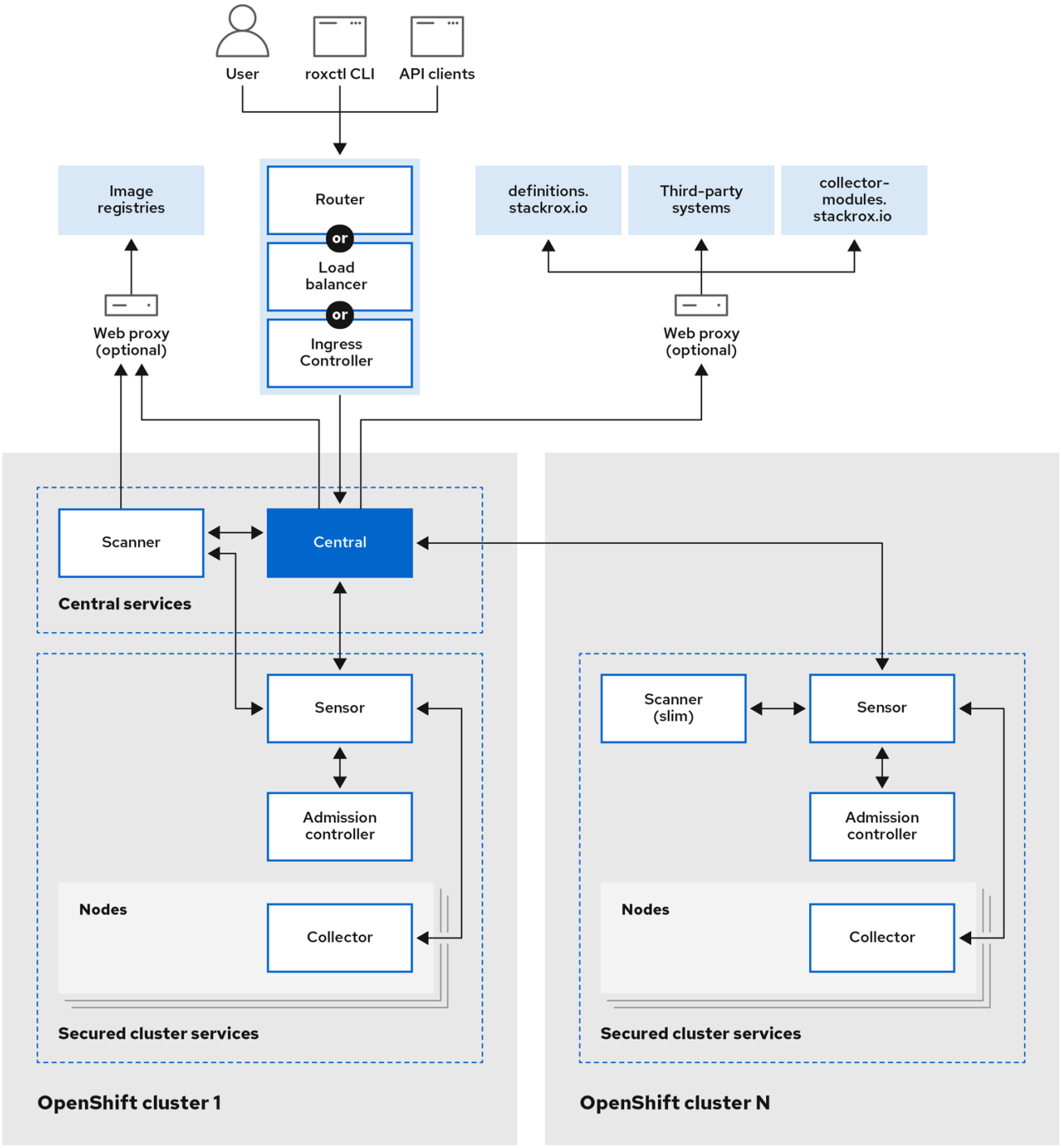
- **Third-party systems**: You can integrate RHACS with other systems such as CI/CD pipelines, event management (SIEM) systems, logging, email, and more.
- **roxctl**: **roxctl** is a command-line interface (CLI) for running commands on RHACS.
- **Image registries**: You can integrate RHACS with various 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 1.2. 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.

Component	Direction	Interacts with	Description

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. 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 the Collector.

Component	Direction	Interacts with	Description
Admission controller	▮	Sensor	Sensors send the list of security policies to enforce to the 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.