Prerequisites for installing Red Hat Advanced Cluster Security for Kubernetes

General requirements

To install Red Hat Advanced Cluster Security for Kubernetes, you must have:

- OpenShift Container Platform version 4.5 or later.

  > **WARNINGa**
  > You must not install Red Hat Advanced Cluster Security for Kubernetes on:
  >
  > - Amazon Elastic File System (Amazon EFS). Use the Amazon Elastic Block Store (Amazon EBS) with the default **gp2** volume type instead.
  > - Older CPUs that do not have the Streaming SIMD Extensions (SSE) 4.2 instruction set. For example, Intel processors older than *Sandy Bridge* and AMD processors older than *Bulldozer*. (These processors were released in 2011.)

- Cluster nodes with a supported operating system. See the Red Hat Advanced Cluster Security for Kubernetes Support Policy for additional information.
  - **Operating system**: Amazon Linux, CentOS, Container-Optimized OS from Google, Red Hat Enterprise Linux CoreOS (RHCOS), Debian, Red Hat Enterprise Linux (RHEL), or Ubuntu.
  - **Processor and memory**: 2 CPU cores and at least 3GiB of RAM.

> **NOTEa**
> For deploying Central, use a machine type with 4 or more cores and apply scheduling policies to launch Central on such nodes.

- Persistent storage by using persistent volume claim (PVC).
    - Use Solid-State Drives (SSDs) for best performance. However, you can use another storage type if you do not have SSDs available.
- Helm command-line interface (CLI) v3.2 or newer. Use the `helm version` command to verify the version of Helm you have installed.
- The OpenShift Container Platform CLI (`oc`).
- You must have the required permissions to configure deployments in the Central cluster.
- You must have access to the Red Hat Container Registry. See Red Hat Container Registry Authentication for information about downloading images from `registry.redhat.io` .

> **NOTEa**
> If you are not a Red Hat customer and purchased the StackRox Kubernetes Security Platform before the acquisition, you can use StackRox's container registry at `stackrox.io` . Contact support@stackrox.com to enable access to the registry.

Prerequisites for installing Central

A single containerized service called Central handles data persistence, API interactions, and user interface (Portal) access.

Central requires persistent storage:

- You can provide storage with a persistent volume claim (PVC).

> **NOTEa**
> You can use a hostPath volume for storage only if all your hosts (or a group of hosts) mount a shared file system, such as an NFS share or a storage appliance. Otherwise, your data is only saved on a single node. Red Hat does not recommend using a hostPath volume.

- Use Solid-State Drives (SSD) for best performance. However, you can use another storage type if you do not have SSDs available.

- If you use a web proxy or firewall, you must configure bypass rules to allow traffic for the `definitions.stackrox.io` and `collector-modules.stackrox.io` domains and enable Red Hat Advanced Cluster Security for Kubernetes to trust your web proxy or firewall. Otherwise, updates for vulnerability definitions and kernel support packages will fail.

  Red Hat Advanced Cluster Security for Kubernetes requires access to:

  - `definitions.stackrox.io` for downloading updated vulnerability definitions. Vulnerability definition updates allow Red Hat Advanced Cluster Security for Kubernetes to maintain up-to-date vulnerability data when new vulnerabilities are discovered or additional data sources are added.
  - `collector-modules.stackrox.io` to download updated kernel support packages. Updated Kernel support packages ensure that Red Hat Advanced Cluster Security for Kubernetes can monitor the latest operating systems and collect data about the network traffic and processes running inside the containers. Without these updates, Red Hat Advanced Cluster Security for Kubernetes might fail to monitor containers if you add new nodes in your cluster or if you update your nodes' operating system.

NOTEa

For security reasons, you should deploy Central in a cluster with limited administrative access.

Memory and storage requirements

The following table lists the minimum memory and storage values required to install and run Central.

Central	CPU	Memory	Storage
Request	1.5 cores	4 GiB	100 GiB
Limit	4 cores	8 GiB	100 GiB

Sizing guidelines

Use the following compute resources and storage values depending upon the number of nodes in your cluster.

Nodes	Deployments	CPU	Memory	Storage
Up to 100	Up to 1000	2 cores	4 GiB	100 GiB
Up to 500	Up to 2000	4 cores	8 GiB	100 GiB
More than 500	More than 2000	8 cores	12 - 16 GiB	100 - 200 GiB

Prerequisites for installing Scanner

Red Hat Advanced Cluster Security for Kubernetes includes an image vulnerability scanner called Scanner. This service scans images that are not already scanned by scanners integrated into image registries.

Memory and storage requirements

Scanner	CPU	Memory
Request	1.2 cores	2700 MiB
Limit	5 cores	8000 MiB

Prerequisites for installing Sensor

Sensor monitors your Kubernetes and OpenShift Container Platform clusters. These services currently deploy in a single deployment, which handles interactions with the Kubernetes API and coordinates with Collector.

Memory and storage requirements

Sensor	CPU	Memory
Request	1 core	1 GiB
Limit	2 cores	4 GiB

Prerequisites for installing Admission Controller

The Admission controller prevents users from creating workloads that violate policies you configure.

Memory and storage requirements

By default, the admission control service runs 3 replicas. The following table lists the request

By default, the admission control service runs 3 replicas. The following table lists the request and limits for each replica.

Admission controller	CPU	Memory
Request	.05 cores	100 MiB
Limit	.5 cores	500 MiB

Prerequisites for installing Collector

Collector monitors runtime activity on each node in your secured clusters. It connects to Sensor to report this information.

CAUTIONa

To install Collector on systems configured with Unified Extensible Firmware Interface (UEFI) boot, you must use eBPF probes because kernel modules are unsigned, and the UEFI firmware cannot load unsigned packages.

Memory and storage requirements

Collector	CPU	Memory
Request	.05 cores	320 MiB
Limit	.75 cores	1 GiB

NOTEa

Collector uses a mutable image tag (`<version>-latest`), so you get support for newer Linux kernel versions more easily. There is no change in code, pre-existing kernel modules, or eBPF programs for image updates. Updates only add a single image layer with support for new kernel versions published after the initial release.