Red Hat Advanced Cluster Security for Kubernetes 4.4

架构

系统架构

Last Updated: 2024-06-28

Red Hat Advanced Cluster Security for Kubernetes 4.4 架构

系统架构

法律通告

摘要

提供有关 Red Hat Advanced Cluster Security for Kubernetes 架构的概述和描述。

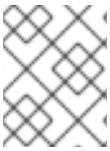
目录

第 1 章 RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 架构

发现 Red Hat Advanced Cluster Security for Kubernetes 架构和概念。

1.1. RED HAT ADVANCED CLUSTER SECURITY FOR KUBERNETES 架构概述

Red Hat Advanced Cluster Security for Kubernetes (RHACS)使用分布式架构来支持大规模部署，并进行了优化，以最大程度降低对底层 OpenShift Container Platform 或 Kubernetes 节点的影响。



注意

当您在 Kubernetes 和 OpenShift Container Platform 上安装 RHACS 时，架构略有不同。但是，底层组件及其之间的交互保持不变。

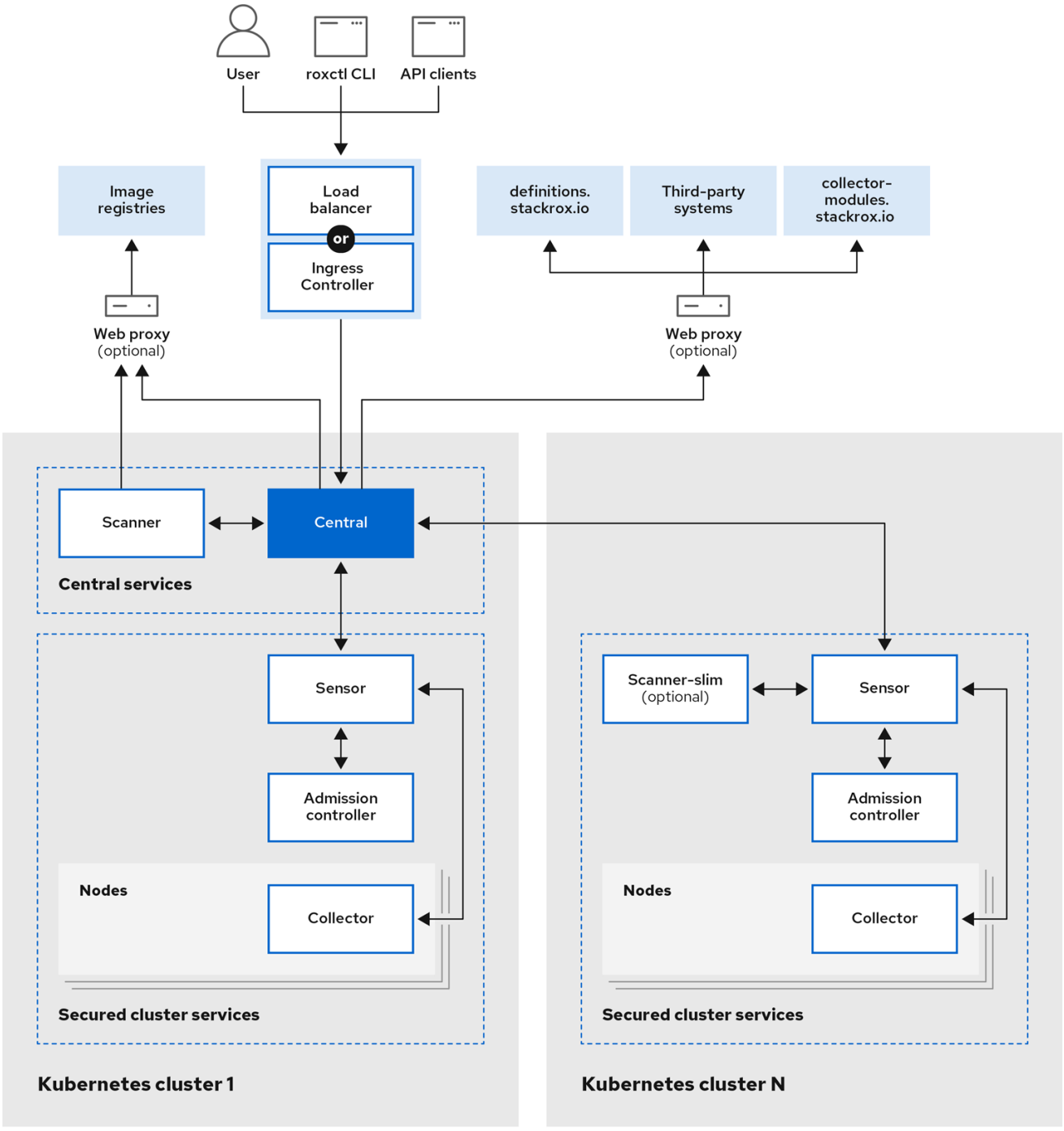
用于 Kubernetes 的 RHACS 架构

下图显示了带有 StackRox Scanner 的架构。对于版本 4.4，Scanner V4 可用。Scanner V4 的安装是可选的，但提供了额外的优点。

重要

扫描程序 V4 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。



367_RHACS_0923

您可以将 RHACS 作为 OpenShift Container Platform 或 Kubernetes 集群中的一组容器安装。RHACS 包括以下服务：

- 您在一个集群中安装的中央服务
- 在您要由 RHACS 保护的每个集群中安装的安全集群服务

除了这些主要服务外，RHACS 也与其他外部组件交互，以增强集群的安全性。

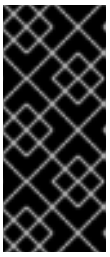
其他资源

- 在 OpenShift Container Platform 和 Kubernetes 上安装之间的架构区别
- 外部组件

1.2. 中央服务

您可以在单个集群中安装 Central 服务。这些服务包括以下组件：

- **Central** ： Central 是 RHACS 应用程序管理界面和服务。它处理 API 交互和用户界面 (RHACS Portal) 访问。您可以使用同一中实例来保护多个 OpenShift Container Platform 或 Kubernetes 集群。
- **Central DB** ： Central DB 是 RHACS 的数据库，并处理所有数据持久性。它目前基于 PostgreSQL 13。
- scanner **V4** （技术预览）：从版本 4.4 开始，RHACS 包含扫描程序 V4 漏洞扫描程序来扫描容器镜像。扫描程序 V4 基于 ClairCore 构建，同时还支持 Clair 扫描程序。扫描程序 V4 支持扫描语言和特定于操作系统的镜像组件。对于版本 4.4，您必须将这个扫描程序与 StackRox Scanner 结合使用，以提供节点和平台扫描功能，直到 Scanner V4 支持这些功能。scanner V4 包含 Indexer、Matcher 和 DB 组件。



重要

扫描程序 V4 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

  - **scanner V4 Indexer**: Scanner V4 Indexer 执行镜像索引，之前被称为镜像分析。根据镜像和 registry 凭证，索引程序会从 registry 中拉取镜像。它找到基础操作系统（如果存在），并查找软件包。它存储和输出索引报告，其中包含给定镜像的查找。
  - **scanner V4 Matcher**: Scanner V4 Matcher 执行漏洞匹配。如果中央服务扫描器 V4 Indexer 对镜像进行索引，则 Matcher 会从 Indexer 获取索引报告，并与 Scanner V4 数据库中存储的漏洞匹配。如果 Secured Cluster services Scanner V4 Indexer 执行索引，则 Matcher 会使用从该索引程序发送的索引报告，然后与漏洞匹配。Matcher 还获取漏洞数据，并使用最新的漏洞数据更新 Scanner V4 数据库。Scanner V4 Matcher 输出漏洞报告，其中包含镜像的最终结果。
  - **扫描程序 V4 DB** ：此数据库存储扫描程序 V4 的信息，包括所有漏洞数据和索引报告。安装了 Central 的集群上 Scanner V4 DB 需要 PVC。
- **stackrox Scanner**: StackRox Scanner 是 RHACS 中的默认扫描程序。版本 4.4 添加了一个新的扫描程序 Scanner V4。StackRox 扫描程序源自 Clair v2 开源扫描程序的分叉。您必须继续使用此扫描程序进行 RHCOS 节点扫描和平台扫描。
- **scanner-DB** ：此数据库包含 StackRox Scanner 的数据。

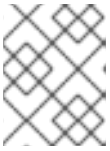
RHACS 扫描程序会分析每个镜像层，以确定基础操作系统，并确定操作系统软件包管理器安装的编程语言软件包和软件包。它们与来自各种漏洞来源的已知漏洞匹配。另外，StackRox Scanner 会识别节点的操作系统和平台中的漏洞。这些功能计划在以后的版本中为 Scanner V4。

1.2.1. 漏洞源

RHACS 使用以下漏洞源：

- alpine 安全数据库
- Amazon Linux 安全中心跟踪的数据

- Debian 安全跟踪器
- Oracle OVAL
- Photon OVAL
- Red Hat OVAL
- Red Hat CVE Map ：这用于 Red Hat Container Catalog 中显示的镜像。
- SUSE OVAL
- Ubuntu OVAL
- OSV ：这用于与语言相关的漏洞，如 Go、Java、Node.js (JavaScript)、Python 和 Ruby。这个源可能会为漏洞提供 GitHub 安全公告(GHSA) ID 而不是 CVE 号。



注意

RHACS Scanner V4 使用此许可证的 OSV.dev 上可用的 OSV 数据库。https://github.com/google/osv.dev/blob/master/LICENSE

- NVD ：这用于各种目的，如在供应商不提供信息时填补信息差距。例如，Alpine 不提供描述、CVSS 分数、严重性或发布日期。

注意

此产品使用 NVD API，但不由 NVD 结束或认证。

- stackrox: 上游 StackRox 项目维护一组漏洞，这些漏洞可能会因为来自其他源的数据格式或数据不存在而被发现。

Scanner V4 Indexer 使用以下源：

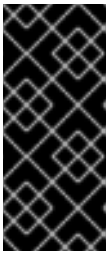
- repository-to-cpe.json ：将 RPM 存储库映射到其相关的 cps，这是匹配基于 RHEL 的镜像的漏洞所必需的。
- container-name-repos-map.json ：这与提供它们的存储库匹配。

1.3. 安全的集群服务

您可以使用 RHACS Cloud Service 在您要保护的每个集群中安装安全集群服务。安全的集群服务包括以下组件：

- **Sensor** ：传感器是负责分析和监控集群的服务。Sensor 侦听 OpenShift Container Platform 或 Kubernetes API 和 Collector 事件来报告集群的当前状态。Sensor 还根据 RHACS 云服务策略触发部署时间和运行时违反情况。另外，Sensor 负责所有集群交互，如应用网络策略、启动 RHACS 云服务策略的重新处理以及与 Admission 控制器交互。
- **准入控制器** ： Admission 控制器可防止用户创建在 RHACS 云服务中违反安全策略的工作负载。
- **Collector** ：收集器分析和监控集群节点上的容器活动。它收集容器运行时和网络活动信息，并将收集的数据发送到 Sensor。

- **stackrox Scanner**: 在 Kubernetes 中，安全集群服务包括 Scanner-slim 作为可选组件。但是，在 OpenShift Container Platform 上，RHACS 云服务在每个安全集群中安装 Scanner-slim 版本，以便在 OpenShift Container Platform 集成 registry 和其他 registry 中扫描镜像。
- **scanner-DB** ：此数据库包含 StackRox Scanner 的数据。
- **scanner V4**: Scanner V4 组件会在安全集群中安装（如果启用）。

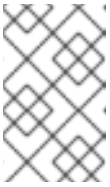


重要

扫描程序 V4 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

  - **scanner V4 Indexer**: Scanner V4 Indexer 执行镜像索引，之前被称为镜像分析。根据镜像和 registry 凭证，索引程序会从 registry 中拉取镜像。它找到基础操作系统（如果存在），并查找软件包。它存储和输出索引报告，其中包含给定镜像的查找。
  - **扫描程序 V4 DB** ：如果启用了 Scanner V4，则安装此组件。此数据库存储扫描程序 V4 的信息，包括索引报告。为获得最佳性能，请为 Scanner V4 DB 配置持久性卷声明(PVC)。



注意

当在与 Central 服务相同的集群中安装安全集群服务并在同一个命名空间中安装时，安全的集群服务不会部署 Scanner V4 组件。相反，假设 Central 服务已包含 Scanner V4 部署。

1.4. 外部组件

Red Hat Advanced Cluster Security for Kubernetes (RHACS)与以下外部组件交互：

- **第三方系统** ：您可以将 RHACS 与其他系统（如 CI/CD 管道、事件管理(SIEM)系统、日志记录、电子邮件等）集成。
- **roxctl**: **roxctl** 是一个命令行界面 (CLI)，用于在 RHACS 上运行命令。
- **镜像 registry** ：您可以将 RHACS 与各种镜像 registry 集成，并使用 RHACS 扫描和查看镜像。RHACS 使用安全集群中发现的镜像 pull secret 为活跃镜像自动配置 registry 集成。但是，要扫描不活跃的镜像，您必须手动配置 registry 集成。
- **definitions.stackrox.io**：RHACS 聚合了来自 **definitions.stackrox.io** 端点中各种漏洞源的数据，并将这些信息传递给 Central。该源包括常规、国家漏洞数据库 (NVD) 数据和特定于分发的数据，如 Alpine、Debian 和 Ubuntu。
- **collector-modules.stackrox.io**: Central 到达 **collector-modules.stackrox.io**，以获取受支持的内核模块并将这些模块传递给 Collector。

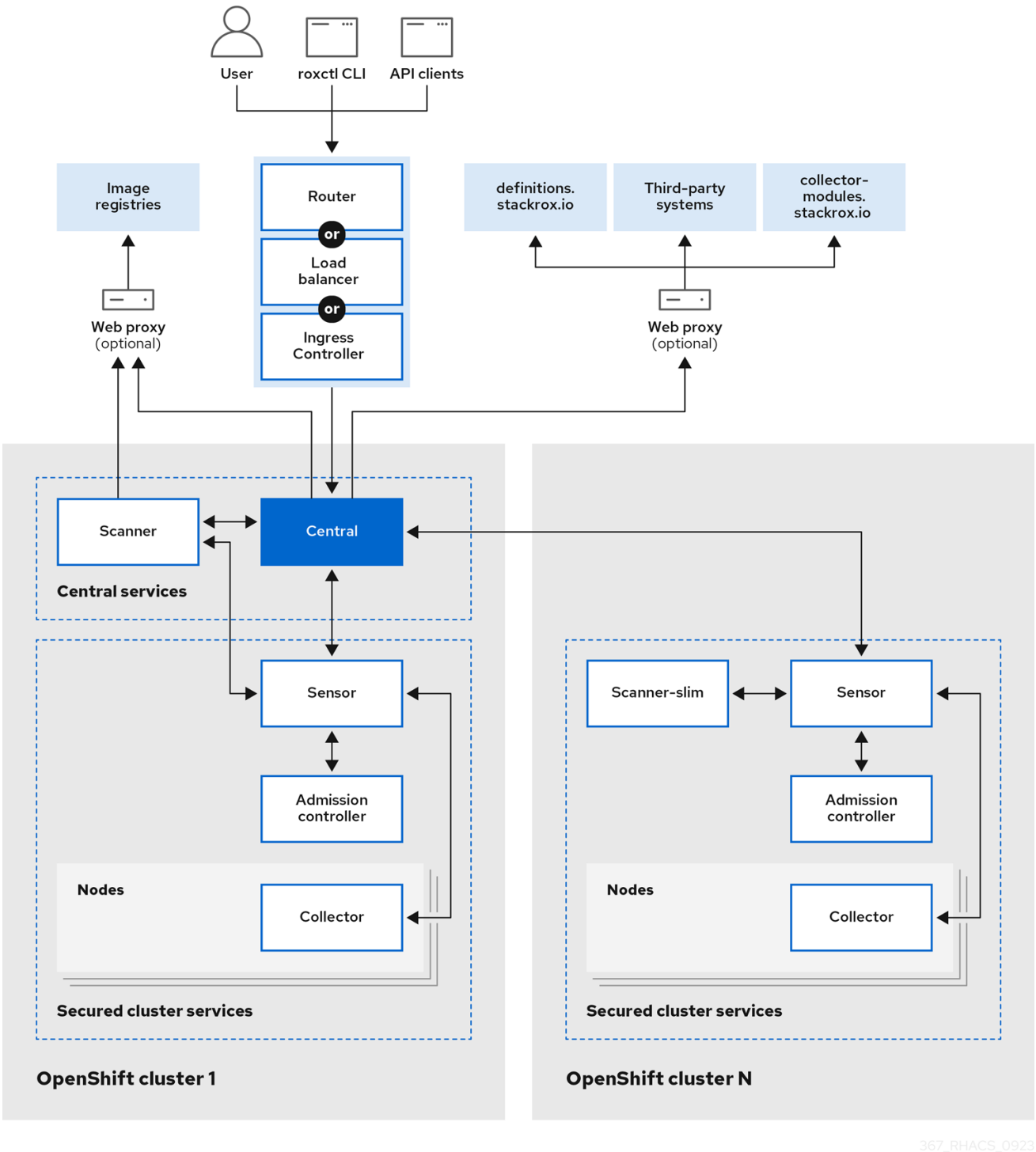
1.5. 在 OPENSHIFT CONTAINER PLATFORM 和 KUBERNETES 上安装之间的架构区别

在 OpenShift Container Platform 上安装 RHACS 时，只有两个架构区别：

1. 当您使用 Operator 或 Helm 安装方法在 OpenShift Container Platform 上安装 RHACS 时，RHACS 会在每个安全集群中安装 RHACS 版本。轻量级扫描器启用扫描集成的 OpenShift Container Registry (OCR) 中的镜像。

2. 在安装了 Central 的集群中，Sensor 与 Scanner 通信。此连接允许访问附加到集群的内部 registry。

图 1.1. Red Hat Advanced Cluster Security for Kubernetes 架构 for OpenShift Container Platform



1.6. 服务间的交互

本节介绍 RHACS 服务如何相互交互。

表 1.1. 带有 Scanner V4 的 RHACS

组件	方向	组件	描述
Central	▮	scanner V4 Indexer	中央请求索引器下载和索引(analyze)给定镜像。这个过程会产生索引报告。扫描程序 V4 Indexer 从 Central 请求映射文件，以帮助索引过程。
Central	▮	scanner V4 Matcher	Central 请求 Scanner V4 Matcher 与给定镜像匹配到已知漏洞。这个过程会产生最终扫描结果：漏洞报告。扫描程序 V4 Matcher 从 Central 请求最新的漏洞。
Sensor	▮	scanner V4 Indexer	在使用 Operator 或使用委派扫描时部署的 Red Hat OpenShift 环境中默认启用 **SecuredCluster** 扫描。启用 **SecuredCluster** 扫描时，Sensor 会请求 Scanner V4 来索引镜像。扫描程序 V4 Indexer 从 Sensor 请求映射文件，以帮助索引过程，除非在同一命名空间中存在 Central。在这种情况下，会联系 Central。
scanner V4 Indexer	→	镜像 registry	Indexer 从 registry 中拉取镜像元数据以确定镜像的层，并下载之前未索引的层。
scanner V4 Matcher	→	scanner V4 Indexer	扫描程序 V4 Matcher 从 Indexer 请求镜像索引（索引报告）的结果。然后，它会使用报告来确定相关的漏洞。只有在 Central 集群中索引镜像时，才会发生此交互。当 Scanner V4 与安全集群中索引的镜像的漏洞匹配时，不会发生此交互。
scanner V4 Indexer	→	扫描程序 V4 DB	Indexer 存储与索引结果相关的数据，以确保镜像层仅下载并索引一次。这可以防止不必要的网络流量和其他资源利用率。
scanner V4 Matcher	→	扫描程序 V4 DB	扫描程序 V4 Matcher 将它的所有漏洞数据存储在数据库中，并定期更新这些数据。扫描程序 V4 索引程序还会在漏洞匹配过程中查询此数据。
Sensor	▮	Central	Central 和 Sensor 之间有双向通信。Sensor 定期轮询 Central 以下载传感器捆绑包配置的更新。它还会为安全集群观察到的活动发送事件，并观察到的策略违反情况。Central. 与 Sensor 通信，以强制针对启用的策略对所有部署进行重新处理。

组件	方向	组件	描述
Collector	▮	Sensor	收集器与 Sensor 通信，并将所有事件发送到集群的对应 Sensor。在支持的 OpenShift Container Platform 集群中，Collector 会分析节点上安装的软件包并将其发送到 Sensor，以便扫描程序稍后可以扫描它们以了解漏洞。收集器也请求 Sensor 中缺少的驱动程序。Sensor 从 Collector 请求合规性扫描结果。另外，Sensor 从 Central 接收外部无类别域间路由信息，并将其推送到 Collector。
准入控制器	▮	Sensor	传感器将安全策略列表发送到 Admission 控制器。准入控制器将安全策略违反警报发送到 Sensor。准入控制器也可以根据需要从 Sensor 请求镜像扫描。
准入控制器	→	Central	它并不常见；但是，如果知道 Central 端点且 Sensor 不可用，Admission 控制器可以直接与 Central 进行通信。

重要

扫描程序 V4 只是一个技术预览功能。技术预览功能不受红帽产品服务等级协议（SLA）支持，且功能可能并不完整。红帽不推荐在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。

有关红帽技术预览功能支持范围的更多信息，请参阅技术预览功能支持范围。

表 1.2. 使用 StackRox Scanner 的 RHACS

组件	方向	相互交互	描述
Central	▮	扫描程序	Central 和 Scanner 之间有双向通信。中央从扫描器请求镜像扫描，Scanner 从 Central 请求对其 CVE 数据库的更新。
Central	→	**definitions.stackrox.io**	Central 连接到 **definitions.stackrox.io** 端点，以接收聚合的漏洞信息。
Central	→	**collector-modules.stackrox.io**	Central 从 **collector-modules.stackrox.io** 下载支持的内核模块。
Central	→	镜像 registry	中央查询镜像 registry 以获取镜像元数据。例如，要在 RHACS 门户中显示 Dockerfile 指令。
扫描程序	→	镜像 registry	扫描程序从镜像 registry 拉取镜像以识别漏洞。

组件	方向	相互交互	描述
Sensor	▮	Central	Central 和 Sensor 之间有双向通信。Sensor 定期轮询 Central 以下载传感器捆绑包配置的更新。它还会为安全集群观察到的活动发送事件，并观察到的策略违反情况。Central. 与 Sensor 通信，以强制针对启用的策略对所有部署进行重新处理。
Sensor	▮	扫描程序	仅在 OpenShift Container Platform 中，Sensor 与 Scanner 通信以访问附加到集群的本地 registry。扫描程序与 Sensor 通信，以从 **definitions.stackrox.io** 请求数据。
Collector	▮	Sensor	收集器与 Sensor 通信，并将所有事件发送到集群的对应 Sensor。在支持的 OpenShift Container Platform 集群中，Collector 会分析节点上安装的软件包并将其发送到 Sensor，以便扫描程序稍后可以扫描它们以了解漏洞。收集器也请求 Sensor 中缺少的驱动程序。Sensor 从 Collector 请求合规性扫描结果。另外，Sensor 从 Central 接收外部无类别域间路由信息，并将其推送到 Collector。
准入控制器	▮	Sensor	传感器将安全策略列表发送到 Admission 控制器。准入控制器将安全策略违反警报发送到 Sensor。准入控制器也可以根据需要从 Sensor 请求镜像扫描。
准入控制器	→	Central	它并不常见；但是，如果知道 Central 端点且 Sensor 不可用，Admission 控制器可以直接与 Central 进行通信。