

Managing vulnerabilities

Security vulnerabilities in your environment may be exploited by an attacker to perform unauthorized actions such as denial of service, remote code execution, or unauthorized access to sensitive data. Therefore, the management of vulnerabilities is a foundational step towards a successful Kubernetes security program.

Vulnerability management process

vulnerability management process

Vulnerability management is a continuous process to identify and remediate vulnerabilities. Red Hat Advanced Cluster Security for Kubernetes helps you to facilitate a vulnerability management process.

A successful vulnerability management program often includes the following critical tasks:

- Performing asset assessment
- Prioritizing the vulnerabilities
- Assessing the exposure
- Taking action
- Continuously reassessing assets

Red Hat Advanced Cluster Security for Kubernetes helps organizations to perform continuous assessments on their OpenShift Container Platform and Kubernetes clusters. It provides organizations with the contextual information they need to prioritize and act on vulnerabilities in their environment more effectively.

Performing asset assessment

Performing an assessment of an organization's assets involve the following actions:

- Identifying the assets in your environment.
- Scanning these assets to identify known vulnerabilities.
- Reporting on the vulnerabilities in your environment to impacted stakeholders.

When you install Red Hat Advanced Cluster Security for Kubernetes on your Kubernetes or OpenShift Container Platform cluster, it first aggregates the assets running inside of your cluster to help you identify those assets. Red Hat Advanced Cluster Security for Kubernetes allows organizations to perform continuous assessments on their OpenShift Container Platform and Kubernetes clusters. It provides organizations with the contextual information to prioritize and act on vulnerabilities in their environment more effectively.

Important assets that should be monitored by the organization's vulnerability management process using Red Hat Advanced Cluster Security for Kubernetes include:

- **Components:** Components are software packages that may be used as part of an image or run on a node. Components are the lowest level where vulnerabilities are present. Therefore organizations must upgrade, modify or remove software

components in some way to remediate vulnerabilities.

- **Image:** A collection of software components and code that create an environment to run an executable portion of code. Images are where you upgrade components to fix vulnerabilities.
- **Nodes:** A server used to manage and run applications using OpenShift or Kubernetes and the components that make up the OpenShift Container Platform or Kubernetes service.

Red Hat Advanced Cluster Security for Kubernetes groups these assets into the following structures:

- **Deployment:** A definition of an application in Kubernetes that may run pods with containers based on one or many images.
- **Namespace:** A grouping of resources such as Deployments that support and isolate an application.
- **Cluster:** A group of nodes used to run applications using OpenShift or Kubernetes.

Red Hat Advanced Cluster Security for Kubernetes scans the assets for known vulnerabilities and uses the Common Vulnerabilities and Exposures (CVE) data to assess the impact of a known vulnerability.

Viewing application vulnerabilities

You can view application vulnerabilities in Red Hat Advanced Cluster Security for Kubernetes.

Procedure

1. On the RHACS portal, navigate to **Vulnerability Management** → **Dashboard**.
2. On the **Dashboard** view header, select **Application & Infrastructure** → **Namespaces** or **Deployments**.
3. From the list, search for and select the **Namespace** or **Deployment** you want to review.
4. To get more information about the application, select an entity from **Related entities** on the right.

Viewing image vulnerabilities

You can view image vulnerabilities in Red Hat Advanced Cluster Security for Kubernetes.

Procedure

1. On the RHACS portal, navigate to **Vulnerability Management** → **Dashboard**.
2. On the **Dashboard** view header, select **Images**.
3. From the list of images, select the image you want to investigate. You can also filter the list.
 - a. Enter **Image** in the search bar and then select the **Image** attribute.
 - b. Enter the image name in the search bar.
4. In the image details view, review the listed CVEs and prioritize taking action to address the impacted components.
5. Select **Components** from **Related entities** on the right to get more information about all the components that are impacted by the selected image. Or select **Components** from the **Affected components** column under the **Image findings** section for finding components affected by specific CVEs.

Additional resources

- [Using local page filtering](#)

Viewing infrastructure vulnerabilities

You can view vulnerabilities in nodes by using Red Hat Advanced Cluster Security for Kubernetes.

Procedure

1. On the RHACS portal, navigate to **Vulnerability Management** → **Dashboard**.
2. On the **Dashboard** view header, select **Application & Infrastructure** → **Cluster**.
3. From the list of clusters, select the cluster you want to investigate.
4. Review the clusters vulnerabilities and prioritize taking action on the impacted nodes on the cluster.

Viewing node vulnerabilities

You can view vulnerabilities in specific nodes by using Red Hat Advanced Cluster Security for Kubernetes.

Procedure

1. On the RHACS portal, navigate to **Vulnerability Management** → **Dashboard**.
2. On the **Dashboard** view header, select **Nodes**.
3. From the list of nodes, select the node you want to investigate.
4. Review vulnerabilities for the selected node and prioritize taking action.
5. To get more information about the affected components in a node, select **Components** from **Related entities** on the right.

Prioritizing the vulnerabilities

Answer the following questions to prioritize the vulnerabilities in your environment for action and investigation:

- How important is an affected asset for your organization?
- How severe does a vulnerability need to be for investigation?
- Can the vulnerability be fixed by a patch for the affected software component?
- Does the existence of the vulnerability violate any of your organization's security policies?

The answers to these questions help security and development teams decide if they want to gauge the exposure of a vulnerability.

Red Hat Advanced Cluster Security for Kubernetes provides you the means to facilitate the prioritization of the vulnerabilities in your applications and components.

Assessing the exposure

To assess your exposure to a vulnerability, answer the following questions:

- Is your application impacted by a vulnerability?
- Is the vulnerability mitigated by some other factor?
- Are there any known threats that could lead to the exploitation of this vulnerability?
- Are you using the software package which has the vulnerability?
- Is spending time on a specific vulnerability and the software package worth it?

Take some of the following actions based on your assessment:

- Consider marking the vulnerability as a false positive if you determine that there is no exposure or that the vulnerability does not apply in your environment.
- Consider if you would prefer to remediate, mitigate or accept the risk if you are exposed.
- Consider if you want to remove or change the software package to reduce your attack surface.

Taking action

Once you have decided to take action on a vulnerability, you can take one of the following actions:

- Remediate the vulnerability
- Mitigate and accept the risk
- Accept the risk
- Mark the vulnerability as a false positive

You can remediate vulnerabilities by performing one of the following actions:

- Remove a software package
- Update a software package to a non-vulnerable version.

Additional resources

- [Reviewing a false positive or deferred CVE](#)

Finding a new component version

The following procedure finds a new component version to upgrade to.

Procedure

1. On the RHACS portal, navigate to **Vulnerability Management** → **Dashboard**.
2. On the **Dashboard** view header, select **Images**.
3. From the list of images, select the image you already assessed.
4. Under the **Image findings** section, select the CVE.

5. Select the Affected components of the CVE you want to take action on.
6. Review the version of the component that the CVE is fixed in and update your image.

Accepting risks


Follow the instructions in this section to accept the risks in Red Hat Advanced Cluster Security for Kubernetes.

Prerequisites

- You must have `write` permission for the `VulnerabilityManagementRequests` resource.

To accept risk with or without mitigation:

Procedure

1. On the RHACS portal, navigate to **Vulnerability Management** → **Dashboard**.
2. On the **Dashboard** view header, select **Images**.
3. From the list of images, select the image you already assessed.
4. Find the row which lists the CVE you would like to take action on.
5. Click  on the right for the CVE you identified and click **Defer CVE**.
6. Select the date and time till you want to defer the CVE.
7. Select if you want to defer the CVE for the selected image tag or all tags for this image.
8. Enter the reason for the deferral.
9. Click **Request approval**. Select the blue information icon on the right of the CVE and copy the approval link to share with your organization's deferral approver.

Marking vulnerabilities as false positive


The following procedure marks a vulnerability as a false positive.

Prerequisites

- You must have the `write` permission for the `VulnerabilityManagementRequests` resource.

Procedure

Procedure

1. On the RHACS portal, navigate to **Vulnerability Management** → **Dashboard**.
2. On the **Dashboard** view header, select **Images**.
3. From the list of images, select the image you already assessed.
4. Find the row which lists the CVE you would like to take action on.
5. Click the  on the right for the CVE you identified and click **Defer CVE**.
6. Select the date and time you want to defer the CVE.
7. Select if you want to defer the CVE for the selected image tag or all tags for this image.
8. Enter the reason for the deferral.
9. Click **Request approval**.
10. Select the blue information icon on the right of the CVE and copy the approval link to share with your organization's deferral approver.

Reviewing a false positive or deferred CVE


Use the following procedure to review a false positive or deferred CVE.

Prerequisites

- You must have the `write` permission for the `VulnerabilityManagementApprovals` resource.

You can review a false positive or deferred CVE:

Procedure

1. Open the approval link in your browser or in the RHACS portal.
2. Navigate to **Vulnerability Management** → **Risk Acceptance** and search for the CVE.
3. Review the vulnerabilities comments, scope, and action to decide if you would like to approve it.
4. Click on the  at the far right of the CVE and approve or deny the request for approval.

Reporting vulnerabilities to teams

Reporting vulnerabilities to teams

As organizations must constantly reassess and report on their vulnerabilities, some organizations find it helpful to have scheduled communications to key stakeholders to help in the vulnerability management process.

You can use Red Hat Advanced Cluster Security for Kubernetes to schedule these reoccurring communications through e-mail. These communications should be scoped to the most relevant information that the key stakeholders need.

For sending these communications, you must consider the following questions:

- What schedule would have the most impact when communicating with the stakeholders?
- Who is the audience?
- Should you only send specific severity vulnerabilities in your report?
- Should you only send fixable vulnerabilities in your report?

Scheduling vulnerability management reports

The following procedure creates a scheduled vulnerability report.


Procedure

1. On the RHACS portal, navigate to **Vulnerability Management** → **Reporting**.
2. Click **Create report**.
3. Enter a name for your report in the **Report name** field.
4. Select a weekly or monthly cadence for your report under **Repeat report...**
5. Enter **Description** for the report.
6. Select the scope for the report by selecting if you want to report fixable vulnerabilities, vulnerabilities of a specific severity, or vulnerabilities that only appeared since the last scheduled report.
7. For **Configure resource scope**, select the scope of resources the vulnerabilities apply to.
8. Select or create an e-mail notifier to send your report by e-mail and configure your distribution list under **Notification and distribution**.
9. Select **Create** to schedule the report.

Sending a vulnerability report

The following procedure sends a vulnerability report.


Procedure

1. On the RHACS portal, navigate to **Vulnerability Management** → **Reporting**.
2. From the list of reports, select the report.
3. Select the  on the right of the report and click **Run report now**.

Editing a vulnerability report

The following procedure edits a vulnerability report.


Procedure

1. On the RHACS portal, navigate to **Vulnerability Management** → **Reporting**.
2. From the list of reports, select the report.
3. Select the  on the right of the report and click **Edit**.
4. Modify the report as required.
5. Click **Save**.

Deleting a vulnerability report

The following procedure deletes a vulnerability report.

Procedure

1. On the RHACS portal, navigate to **Vulnerability Management** → **Reporting**.
2. From the list of reports, select the report.
3. Select the  on the right of the report and click **Delete report**.

Common tasks

This section lists some common tasks you can perform from the **Vulnerability Management** → **Dashboard** view.

Finding critical CVEs impacting your infrastructure

Finding critical CVEs impacting your infrastructure

Use the **Vulnerability Management** view for identifying CVEs that are impacting your platform the most.

Procedure

1. Navigate to the RHACS portal and click **Vulnerability Management** from the navigation menu.
2. Select CVEs on the **Vulnerability Management** view header.
3. In the **CVEs** view, select the **Env Impact** column header to arrange the CVEs in descending order (highest first) based on the environment impact.

Finding the most vulnerable image components

Use the **Vulnerability Management** view for identifying highly vulnerable image components.

Procedure

1. Navigate to the RHACS portal and click **Vulnerability Management** from the navigation menu.
2. From the **Vulnerability Management** view header, select **Application & Infrastructure** → **Components**.
3. In the **Components** view, select the **CVEs** column header to arrange the components in descending order (highest first) based on the CVEs count.

Identifying the container image layer that introduces vulnerabilities

Use the **Vulnerability Management** view to identify vulnerable components and the image layer they appear in.

Procedure

1. Navigate to the RHACS portal and click **Vulnerability Management** from the navigation menu.
2. Select an image from the **Top Riskiest Images** widget.
3. In the **Image** details view, select the **Dockerfile** tab under the **Image Findings** section.
4. In the **Dockerfile** tab under the **Image Findings** section, select the expand icon to see

a summary of image components.

5. Select the expand icon for specific components to get more details about the CVEs affecting the selected component.

Viewing details only for fixable CVEs

Use the **Vulnerability Management** view to filter and show only the fixable CVEs.

Procedure

1. Navigate to the RHACS portal and click **Vulnerability Management** from the navigation menu.
2. From the **Vulnerability Management** view header, select **Filter CVEs** → **Fixable**.

Identifying the operating system of the base image

Use the **Vulnerability Management** view to identify the operating system of the base image.

Procedure

1. Navigate to the RHACS portal and click **Vulnerability Management** from the navigation menu.
2. From the **Vulnerability Management** view header, select **Images**.
3. View the base operating system (OS) and OS version for all images under the **Image OS** column.
4. Select an image to view its details. The base operating system is also available under the **Image Summary** → **Details and Metadata** section.



NOTEa

Red Hat Advanced Cluster Security for Kubernetes lists the **Image OS** as **unknown** when either:

- The operating system information is not available, or
- If the image scanner in use does not provide this information.

Docker Trusted Registry, Google Container Registry, and Anchore do not provide this information.

Identifying top risky objects

Use the **Vulnerability Management** view for identifying the top risky objects in your environment. The **Top Risky** widget displays information about the top risky images, deployments, clusters, and namespaces in your environment. The risk is determined based on the number of vulnerabilities and their CVSS scores.

Procedure

1. Navigate to the RHACS portal and click **Vulnerability Management** from the navigation menu.
2. Select the **Top Risky** widget header to choose between riskiest images, deployments, clusters, and namespaces.

The small circles on the chart represent the chosen object (image, deployment, cluster, namespace). Hover over the circles to see an overview of the object they represent. And select a circle to view detailed information about the selected object, its related entities, and the connections between them.

For example, if you are viewing **Top Risky Deployments by CVE Count and CVSS score**, each circle on the chart represents a deployment.

- When you hover over a deployment, you see an overview of the deployment, which includes deployment name, name of the cluster and namespace, severity, risk priority, CVSS, and CVE count (including fixable).
 - When you select a deployment, the **Deployment** view opens for the selected deployment. The **Deployment** view shows in-depth details of the deployment and includes information about policy violations, common vulnerabilities, CVEs, and riskiest images for that deployment.
3. Select **View All** on the widget header to view all objects of the chosen type. For example, if you chose **Top Risky Deployments by CVE Count and CVSS score**, you can select **View All** to view detailed information about all deployments in your infrastructure.

Identifying top riskiest images and components

Similar to the **Top Risky**, the **Top Riskiest** widget lists the names of the top riskiest images and components. This widget also includes the total number of CVEs and the number of fixable CVEs in the listed images.

Procedure

1. Navigate to the RHACS portal and click **Vulnerability Management** from the navigation menu.
2. Select the **Top Riskiest Images** widget header to choose between the riskiest images and components. If you are viewing **Top Riskiest Images**:
 - When you hover over an image in the list, you see an overview of the image, which includes image name, scan time, and the number of CVEs along with severity (critical, high, medium, and low).
 - When you select an image, the **Image** view opens for the selected image. The **Image** view shows in-depth details of the image and includes information about CVEs by CVSS score, top riskiest components, fixable CVEs, and Dockerfile for the image.
3. Select **View All** on the widget header to view all objects of the chosen type. For example, if you chose **Top Riskiest Components**, you can select **View All** to view detailed information about all components in your infrastructure.

Viewing the Dockerfile for an image

Use the **Vulnerability Management** view to find the root cause of vulnerabilities in an image. You can view the Dockerfile and find exactly which command in the Dockerfile introduced the vulnerabilities and all components that are associated with that single command.

The Dockerfile tab shows information about:

- All the layers in the Dockerfile
- The instructions and their value for each layer
- The components included in each layer
- The number of CVEs in components for each layer

When there are components introduced by a specific layer, you can select the expand icon to see a summary of its components. If there are any CVEs in those components, you can select the expand icon for an individual component to get more details about the CVEs affecting that component.

Procedure

1. Navigate to the RHACS portal and click **Vulnerability Management** from the navigation menu.

2. Select an image from the **Top Riskiest Images** widget.
3. In the **Image** details view, select the **Dockerfile** tab under the **Image Findings** section.

Disabling identifying vulnerabilities in nodes

Identifying vulnerabilities in nodes is enabled by default. You can disable it from the RHACS portal.

Procedure

1. On the RHACS portal, navigate to **Platform Configuration** → **Integrations**.
2. Under **Image Integrations**, select **StackRox Scanner**.
3. From the list of scanners, select **StackRox Scanner** to view its details.
4. Remove the **Node Scanner** option from **Types**.
5. Select **Save**.

Scanning inactive images

Red Hat Advanced Cluster Security for Kubernetes scans all active (deployed) images every 4 hours and updates the image scan results to reflect the latest vulnerability definitions.

You can also configure Red Hat Advanced Cluster Security for Kubernetes to scan inactive (not deployed) images automatically.

Procedure

1. Select **Images** on the **Vulnerability Management** view header to view a list of all the images.
2. On the **Images** view header, select **Watch Images**.
3. In the **Manage Inactive Images** dialog, enter the inactive image's name (and not the image `id`) for which you want to enable scanning.
4. Select **Add Image**. Red Hat Advanced Cluster Security for Kubernetes then scans the image and shows the error or success message.
5. Select **Return to Image list** to view the **Images** view.

Creating policies to block specific CVEs

You can create new policies or add specific CVEs to an existing policy from the **Vulnerability Management** view.

Procedure

1. Click **CVEs** from the **Vulnerability Management** view header.
2. Select the checkboxes (leftmost column) for one or more CVEs and then click **Add selected CVEs to Policy** (add icon). Or, move the mouse over a CVE in the list, and select the **Add** icon on the right side.
3. For **Policy Name**:
 - To add the CVE to an existing policy, select an existing policy from the drop-down list box.
 - To create a new policy, enter the name for the new policy, and select **Create <policy_name>**.
4. Select a value for **Severity**, either **Critical**, **High**, **Medium**, or **Low**.
5. Choose the **Lifecycle Stage** to which your policy is applicable, from **Build**, or **Deploy**. You can also select both life-cycle stages.
6. Enter details about the policy in the **Description** box.
7. Turn off the **Enable Policy** toggle if you want to create the policy but enable it later. The **Enable Policy** toggle is on by default.
8. Verify the listed CVEs which are included in this policy.
9. Click **Save Policy**.

Viewing recently detected vulnerabilities

The **Recently Detected Vulnerabilities** widget on the **Vulnerability Management** view shows a list of recently discovered vulnerabilities in your scanned images, based on the scan time and CVSS score. It also includes information about the number of images affected by the CVE and its impact (percentage) on your environment.

- When you hover over a CVE in the list, you see an overview of the CVE, which includes scan time, CVSS score, description, impact, and whether it's scored by using CVSS v2 or v3.
- When you select a CVE, the **CVE** details view opens for the selected CVE. The **CVE**

details view shows in-depth details of the CVE and the components, images, and deployments and deployments in which it appears.

- Select **View All** on the **Recently Detected Vulnerabilities** widget header to view a list of all the CVEs in your infrastructure. You can also filter the list of CVEs.

Viewing the most common vulnerabilities

The **Most Common Vulnerabilities** widget on the **Vulnerability Management** view shows a list of vulnerabilities that affect the largest number of deployments and images arranged by their CVSS score.

- When you hover over a CVE in the list, you see an overview of the CVE which includes, scan time, CVSS score, description, impact, and whether it is scored by using CVSS v2 or v3.
- When you select a CVE, the **CVE** details view opens for the selected CVE. The **CVE** details view shows in-depth details of the CVE and the components, images, and deployments and deployments in which it appears.
- Select **View All** on the **Most Common Vulnerabilities** widget header to view a list of all the CVEs in your infrastructure. You can also filter the list of CVEs. To export the CVEs as a CSV file, select **Export** → **Download CVES as CSV**.

Identifying deployments with most severe policy violations

The **Deployments with most severe policy violations** widget on the **Vulnerability Management** view shows a list of deployments and severity of vulnerabilities affecting that deployment.

- When you hover over a deployment in the list, you see an overview of the deployment, which includes the deployment name, the name of the cluster and the namespace in which the deployment exists, and the number of failing policies and their severity.
- When you select a deployment, the **Deployment** view opens for the selected deployment. The **Deployment** view shows in-depth details of the deployment and includes information about policy violations, common vulnerabilities, CVEs, and riskiest images for that deployment.
- Select **View All** on the **Most Common Vulnerabilities** widget header to view a list of all the CVEs in your infrastructure. You can also filter the list of CVEs. To export the CVEs as a CSV file, select **Export** → **Download CVES as CSV**.

Finding clusters with most Kubernetes and Istio vulnerabilities

Use the **Vulnerability Management** view for identifying the clusters with most Kubernetes and Istio vulnerabilities in your environment.

The **Clusters with most K8S & Istio Vulnerabilities** widget shows a list of clusters, ranked by the number of Kubernetes and Istio vulnerabilities in each cluster. The cluster on top of the list is the cluster with the highest number of vulnerabilities.

Procedure

1. Click on one of the clusters from the list to view details about the cluster. The **Cluster** view includes:
 - **Cluster Details** section, which shows cluster details and metadata, top risky objects (deployments, namespaces, and images), recently detected vulnerabilities, riskiest images, and deployments with the most severe policy violations.
 - **Cluster Findings** section, which includes a list of failing policies and list of fixable CVEs.
 - **Related Entities** section, which shows the number of namespaces, deployments, policies, images, components, and CVEs the cluster contains. You can select these entities to view more details.
2. Click **View All** on the widget header to view the list of all clusters.

Identifying vulnerabilities in nodes

You can use the **Vulnerability Management** view to identify vulnerabilities in your nodes. The identified vulnerabilities include vulnerabilities in:

- Core Kubernetes components.
- Container runtimes (Docker, CRI-O, runC, and containerd).



NOTEa

- Red Hat Advanced Cluster Security for Kubernetes does not support identifying vulnerabilities in nodes on OpenShift Container Platform.
- Red Hat Advanced Cluster Security for Kubernetes can identify vulnerabilities in the following operating systems:

- Amazon Linux 2
- CentOS
- Red Hat Enterprise Linux CoreOS (RHCOS)
- Debian
- Garden Linux (Debian 11)
- Red Hat Enterprise Linux (RHEL)
- Ubuntu (AWS, Azure, GCP, and GKE specific versions)

Procedure

1. Select **Nodes** on the **Vulnerability Management** view header to view a list of all the CVEs affecting your nodes.
2. Select a node from the list to view details of all CVEs affecting that node.
 - a. When you select a node, the **Node** details panel opens for the selected node. The **Node** view shows in-depth details of the node and includes information about CVEs by CVSS score and fixable CVEs for that node.
 - b. Select **View All** on the **CVEs by CVSS score** widget header to view a list of all the CVEs in the selected node. You can also filter the list of CVEs.
 - c. To export the fixable CVEs as a CSV file, select **Export as CSV** under the **Node Findings** section.