

Compliance Reporting and Remediation with Red Hat ACS

Install the OpenShift Compliance Operator

From the Web interface of OpenShift, navigate to **Operators** -> **OperatorHub** on the left hand side menu.

In the **Filter by keyword** box, search for "compliance operator"

Click on the Compliance Operator logo, click Install on the Popup, and on the confirmation page, Install. Installation should take only a few minutes.

Create a ScanSettingBinding to run a Compliance Scan

To perform a scan, we need to create an object in the **openshift-compliance** namespace to describe the scan jobs we want to run. This sample YAML will create two scan jobs, one for OCP4-cis and one for OCP4-cis-node.

```
apiVersion: compliance.openshift.io/v1alpha1
kind: ScanSettingBinding
metadata:
  name: cis-compliance
profiles:
  - name: ocp4-cis-node
    kind: Profile
    apiGroup: compliance.openshift.io/v1alpha1
  - name: ocp4-cis
    kind: Profile
    apiGroup: compliance.openshift.io/v1alpha1
settingsRef:
  name: default
  kind: ScanSetting
  apiGroup: compliance.openshift.io/v1alpha1
```

Sample of ScanSettingBinding

With this YAML saved as a file called "sscan.yaml", create the object using the OpenShift command-line:

```
oc -n openshift-compliance create -f sscan.yaml
```

If successful, you should see this response:

```
scansettingbinding.compliance.openshift.io/cis-compliance created
```

You can also create this object by pasting the YAML into the OpenShift web Console.

1. Change the active project to "openshift-compliance"
2. Click the + Icon in the top right of the interface
3. Paste the YAML from the example above and click "Create"

Ingest the Compliance Scan Results in ACS

If ACS was installed prior to the Compliance Operator, we'll need to restart the ACS sensor in the OpenShift cluster to see these results.

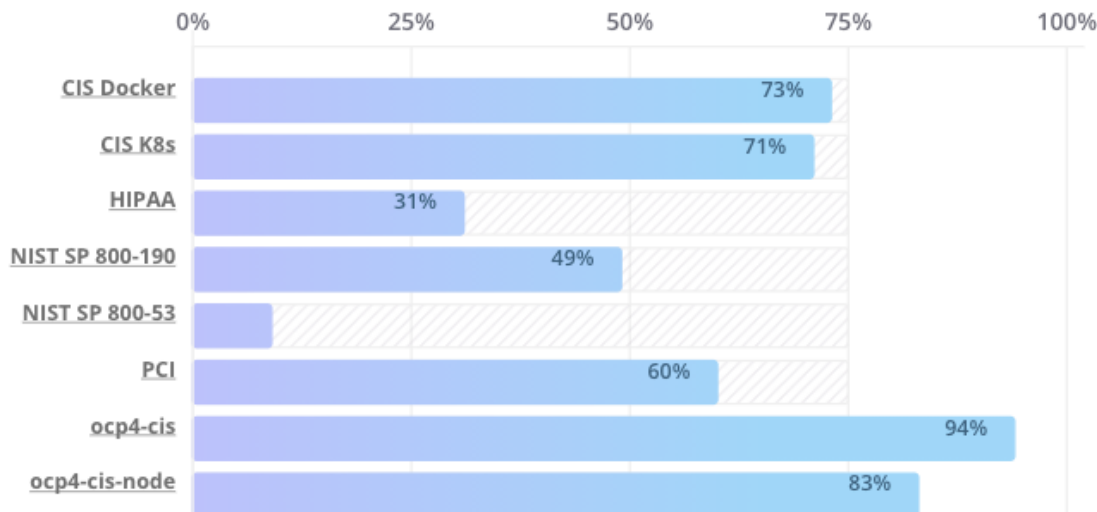
1. In the OpenShift console, change the active project to "**stackrox**"
2. Navigate to **Workloads** -> **Pods**
3. Find the Pod with name starting with "sensor-" and from the right-hand side three-dot menu, choose Delete Pod

Examine Compliance Results for Workloads in ACS

With the Sensor restarted, kick off a compliance scan in ACS to see the updated results:

1. In the ACS User Interface, select **Compliance** from the left menu, and click **Scan Environment** in the top menu bar.
2. The scan should only take a few seconds; once it's complete you should see entries for both the ACS built-in and compliance operator standards:

PASSING STANDARDS ACROSS CLUSTERS



To see the detailed results, click on the name or bar of any of the standards. To investigate the results of the OpenShift CIS benchmark scan, for example, click **ocp4-cis**:

CONTROLS

Resource List

Standard: X

ocp4-cis X

195 CONTROLS ACROSS 1 CLUSTER

development

Control ↑

etcd-unique-ca - Configure A Unique CA Certificate for etcd

file-groupowner-cni-conf - Verify Group Who Owns The OpenShift Container Network Interface Files

file-groupowner-controller-manager-kubeconfig - Verify Group Who Owns The OpenShift Controller Manager Kubeconfig File

file-groupowner-etcd-data-dir - Verify Group Who Owns The Etcd Database Directory

file-groupowner-etcd-data-files - Verify Group Who Owns The Etcd Write-Ahead-Log Files

file-groupowner-etcd-member - Verify Group Who Owns The etcd Member Pod Specification File

file-groupowner-etcd-pki-cert-files - Verify Group Who Owns The Etcd PKI Certificate Files

file-groupowner-ip-allocations - Verify Group Who Owns The OpenShift SDN Container Network Interface Plugin IP Address Allocations

Partial view of ACS compliance results for OCP4

Examine Compliance Reports for Non-OpenShift Kubernetes Clusters

For Kubernetes clusters like GKE, AKS, and EKS, where ACS is running, compliance results for the configuration of the Docker engine and the Kubernetes cluster itself are provided in the Compliance page in the UI.

Navigate back to the ACS **Compliance** page.

1. In the section labeled "PASSING STANDARDS ACROSS CLUSTERS", click on **CIS Docker**.
2. Scroll down to view the list of configuration checks and their pass / fail status.
3. Each cluster has its own section for results; you can scroll through all of the clusters, or use the Filter Bar at the top to choose a particular cluster with the key "Cluster:"

gke-prod-1
Control ↑
1.1.1 - Ensure the container host has been Hardened
1.1.2 - Ensure that the version of Docker is up to date
1.2.1 - Ensure a separate partition for containers has been created
1.2.2 - Ensure only trusted users are allowed to control Docker daemon
1.2.3 - Ensure auditing is configured for the docker daemon
1.2.4 - Ensure auditing is configured for Docker files and directories - /var/lib/docker
1.2.5 - Ensure auditing is configured for Docker files and directories - /etc/docker
CIS Docker Results

Many of the controls in CIS Docker refer to the configuration of the Docker engine on each Kubernetes nodes, but a significant number of CIS Docker controls are best practices for building and using containers, and ACS has policies to enforce their use.

Examine CIS Docker Benchmark Policies in ACS

To see the built-in ACS policies for CIS compliance,

1. Navigate to **Platform Configuration -> System Policies**
2. In the filter bar at the top, type the word **CIS** to filter the view down to the CIS Docker related policies.

To see all of the running workloads that violate CIS Docker best practices,

1. Navigate to the **Violations** page
2. In the filter bar at the top, click and choose the key Policy:
3. For the search value, type the word **CIS** to see current deployments that violate any CIS related policy

VIOLATIONS			
Filtered View			
64 VIOLATIONS MATCHED			
<input type="checkbox"/> Entity	Type	Policy	Enforced
<input type="checkbox"/> redis-cart in "gke-prod-1/hipster"	Deployment	Docker CIS 4.1: Ensure That a User for the Container Has Been Created	No
<input type="checkbox"/> adservice in "gke-prod-1/hipster"	Deployment	Docker CIS 4.1: Ensure That a User for the Container Has Been Created	No
<input type="checkbox"/> shippingservice in "gke-prod-1/hipster"	Deployment	Docker CIS 4.1: Ensure That a User for the Container Has Been Created	No
<input type="checkbox"/> currencyservice in "gke-prod-1/hipster"	Deployment	Docker CIS 4.1: Ensure That a User for the Container Has Been Created	No
<input type="checkbox"/> loadgenerator in "gke-prod-1/hipster"	Deployment	Docker CIS 4.1: Ensure That a User for the Container Has Been Created	No
Violations of CIS Docker benchmark policies			

Configure Policy in ACS to Invoke Compliance related Controls

The Built-in standards in ACS Compliance provide guidance on required configurations to meet each individual control. Standards like PCI, HIPAA, and NIST 800-190 are focused on workloads visible to ACS, and apply to all workloads running in any Kubernetes cluster that ACS is installed in.

Much of the control guidance can be implemented using ACS policies, and providing appropriate policy with enforcement in ACS can change compliance scores.

As an example, we'll look at a control in the NIST 800-190 that requires that container images be kept up to date, and to use meaningful version tags: "practices should emphasize accessing images using immutable names that specify discrete versions of images to be used."

WARNING: This configuration will change the behavior of your Kubernetes clusters and possibly result in preventing new deployments from being created. After testing, you can quickly revert the changes using the instructions at the end of this section.

Inspect the NIST 800-190 Guidance for Control 4.2.2

4. Navigate back to the ACS **Compliance** page.
5. In the section labeled "PASSING STANDARDS ACROSS CLUSTERS", click on **NIST 800-190**.
6. Scroll down to control **4.2.2** and examine the control guidance on the right.

The control guidance reads:

"StackRox continuously monitors the images being used by active deployments. StackRox provides built-in policies that detects if images with insecure tags are being used or if the image being used is pretty old. Therefore, the cluster is compliant if there are policies that are being enforced that discourages such images from being deployed."

Enforce Policies that Meet Guidance for NIST Control 4.2.2

There are two separate default system policies that, together, meet this control's guidance, "90-day Image Age," and "Latest tag". Both must have enforcement enabled for this control to be satisfied.

- 3. Navigate to **Platform Configuration -> System Policies**
- 4. Find and click on the policy named, **"90-day Image Age"** which by default is second in the list. We're not going to change this policy other than to enable enforcement.
- 5. Click **Edit** to get to the Policy settings.
- 6. Click **Next** at the upper right to get to the Policy Criteria page.
- 7. Click **Next** at the upper right to get to the Violations Preview page.
- 8. Click **Next** at the upper right to get to the Enforcement Options page.
- 9. On the enforcement options, click **On** for both Build and Deploy enforcement. Click **Save**, and then **X** to close.
- 10. At the main System Policies page, find the Policy named, **"Latest tag"** and repeat steps 3 - 7 to enable enforcement and save the policy.


90-DAY IMAGE AGE

← PREVIOUS

SAVE

×

BASED ON THE FIELDS SELECTED IN YOUR POLICY CONFIGURATION, YOU MAY CHOOSE TO APPLY ENFORCEMENT AT THE FOLLOWING STAGES:




BUILD

ON

OFF

Enforcement Behavior

If enabled, StackRox will fail your CI builds when images match the conditions of this policy. Download the CLI above to get started.




DEPLOY

ON

OFF

Enforcement Behavior

If enabled, StackRox will automatically block creation of deployments that match the conditions of this policy. In clusters with the StackRox Admission Controller enabled, the Kubernetes API server will block noncompliant deployments. In other clusters, StackRox will edit noncompliant deployments to prevent pods from being scheduled.



RUNTIME

ON

OFF

Enforcement Behavior

If enabled, StackRox will either kill the offending pod or block the action taken on the pod. Executions within a pod that match the conditions of the policy will result in the pod being killed. Actions taken through the API server that match policy criteria will be blocked.

90-Day Image Age enforcement

View Updated Compliance Scan Results in ACS

In order to see the impact on NIST 800-190 scores:

1. Navigate back to the compliance page.
2. Click "Scan Environment" in the upper right.
3. In the section labeled "PASSING STANDARDS ACROSS CLUSTERS", click on NIST 800-190.
4. Scroll down to control 4.2.2 and verify that the control now reports 100% compliance.

<p>4.2.2 - Stale images in registries The risk of using stale images can be mitigated through two primary methods. First, organizations can prune registries of unsafe, vulnerable images that should no longer be used. This process can be automated based on time triggers and labels associated with images. Second, operational practices should emphasize accessing images using immutable names that specify discrete versions of images to be used. For example, rather than configuring a deployment job to use the image called my-app, configure it to deploy specific versions of the image, such as my-app:2.3 and my-app:2.4 to ensure that specific, known good instances of images are deployed as part of each job. Another option is using a "latest" tag for images and referencing this tag in deployment automation. However, because this tag is only a label attached to the image and not a guarantee of freshness, organizations should be cautious to not overly trust it. Regardless of whether an organization chooses to use discrete names or to use a "latest" tag, it is critical that processes be put in place to ensure that either the automation is using the most recent unique name or the images tagged "latest" actually do represent the most up-to-date versions.</p>	100%
NIST 800-190 Control 4.2.2	

Revert the Policy Changes

To avoid rejecting any other deployments to the cluster, you should disable the enforcement after viewing the updated ACS results.

1. Navigate to **Platform Configuration -> System Policies**
2. Find and click on the policy named, "90-day Image Age" which by default is second in the list. Click **Edit** to get to the Policy settings.
3. Click **Next** at the upper right to get to the Policy Criteria page.
4. Click **Next** at the upper right to get to the Violations Preview page.
5. Click **Next** at the upper right to get to the Enforcement Options page.
6. On the enforcement options, click **Off** for both Build and Deploy enforcement. Click **Save**, and then **X** to close.
7. At the main System Policies page, find the Policy named, "Latest tag" and repeat steps 3 - 7 to disable enforcement and save the policy.