**ELC - Runtime Policy with Block Non-compliant Images Control**

**Submitted to**

Text, logo

Description automatically generated

**By**

A logo with colorful dots

Description automatically generated

**Wipro Technologies**

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date of Revision** | **Description of Change** | **Reason for Change** | **Reviewed By** |
| 1.1 | 14-Feb-24 | Initial Draft | NA | Mihirkumar |
|  |  |  |  |  |
|  |  |  |  |  |

**Author/Reviewer/Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Designation** | **Responsibility** | **Date** |
| Mihirkumar Jani | Consultant | Author | 14-Feb-24 |
| Kannan Kuppusamy | Technical Lead | Reviewer | 29-Mar-24 |
| Felix Jebamani | Lead Consultant | Reviewer | 29-Mar-24 |
| Jamshid Abedi | Executive Director | Approver | 12-July-24 |

**Table of Contents**

[Objective of the Document 3](#_Toc162621374)

[1.0 Purpose and Scope 3](#_Toc162621375)

[2.0 AquaSec Enforcers Architecture 4](#_Toc162621376)

[2.1 AquaSec Runtime Policy 4](#_Toc162621377)

[3.0 The AKS cluster Kube Enforcer group Setting. 5](#_Toc162621378)

[4.0 Runtime Policy with Block Non-compliant Images control 6](#_Toc162621379)

[5.0 Testing of the control ‘Block Non-compliant Images’ 7](#_Toc162621380)

[5.2 Scenario 1: 8](#_Toc162621381)

[6.0 Reference links 9](#_Toc162621382)

[7.0 Appendix 9](#_Toc162621383)

[8.1 Abbreviations 9](#_Toc162621384)

# Objective of the Document

This document is regarding Runtime policy with Block Non-compliant Images control, which is help us to prevent the container from running non-compliant images.

# 1.0 Purpose and Scope

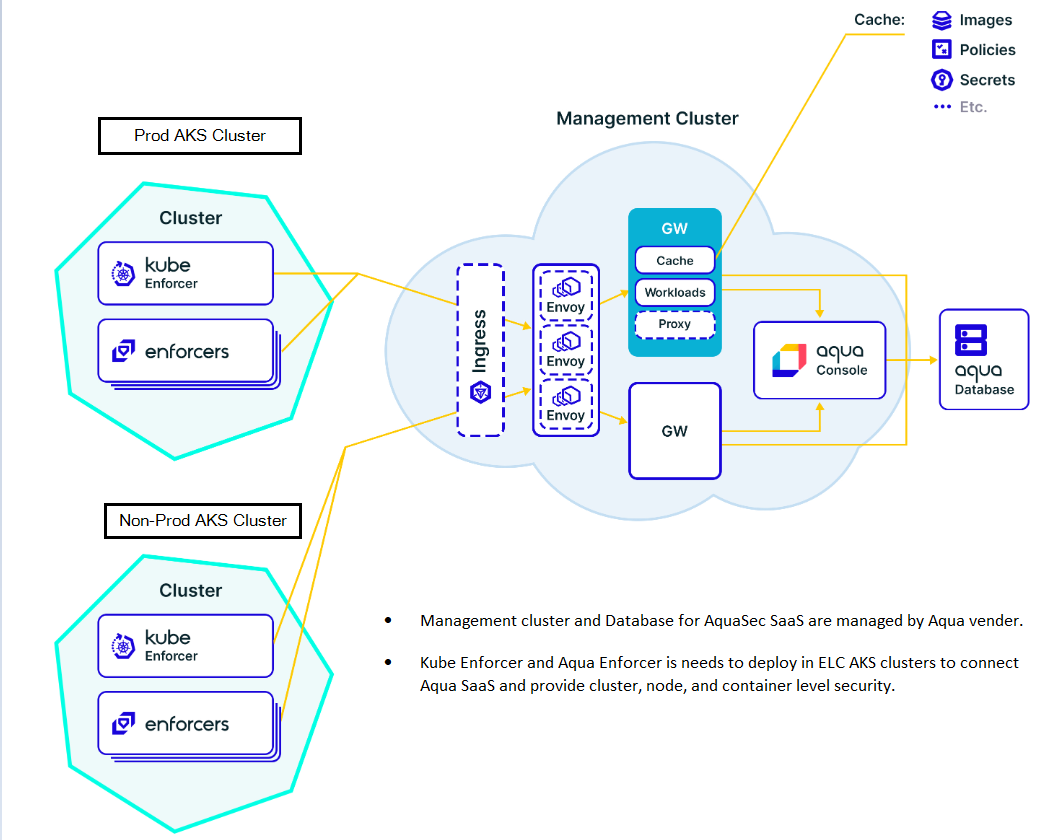
The purpose of Runtime policy is to strength and security in the Azure AKS clusters environment by setting up Block Non-compliant Images control.

This Policy applies to Estee Lauder Companies Inc. (the “Company”) whole Azure AKS clusters environment.

# 2.0 AquaSec Enforcers Architecture

Enforcers are the Aqua components that provide enforcement (securing your workloads and infrastructure during runtime) and other related functionality.

Figure 1: High-level architecture diagram



# 2.1 AquaSec Runtime Policy

* When the container orchestrator platform attempts to start a container, Aqua searches for all Container Runtime Policies whose scope includes the container.
* If any of these policies contains a control (security restriction) that prevents running the container, Aqua will cause deployment of the container to be blocked. Otherwise, the container is allowed to run and, during the runtime of the container, Aqua enforces the applicable Container Runtime Policies.
* When a container attempts to perform an activity that is prohibited by any such policy, and the relevant policy is in **Enforce** mode (not in Audit mode), Aqua will prevent the specific activity from occurring. However, Aqua will **not** terminate the container, or stop it from running.
* If the relevant policy is in either Enforce or Audit mode, Aqua will log an [audit event](https://docs.aquasec.com/v2022.4/platform/audit/view-audit-events/) with the "Runtime" event type.

# 3.0 The AKS cluster Kube Enforcer group Setting.

The Kube Enforcer uses native Kubernetes functionality to perform its functions, one Kube Enforcer can be deployed on each Kubernetes cluster.

Figure 2: The AKS cluster Kube Enforcer group (Navigating to Aqua Enforcer group)

A screenshot of a computer

Description automatically generated

**Aqua Enforcer group setting of the AKS cluster:**

A screenshot of a computer

Description automatically generated

**The ‘Enforcement mode’ setting must be “Enforce” if not already.**

Figure 3: The AKS cluster Kube Enforcer group setting

A screenshot of a computer

Description automatically generated

# 4.0 Runtime Policy with Block Non-compliant Images control

Below steps needs to be performed to configure Runtime policy with Block Non-compliant Images control.

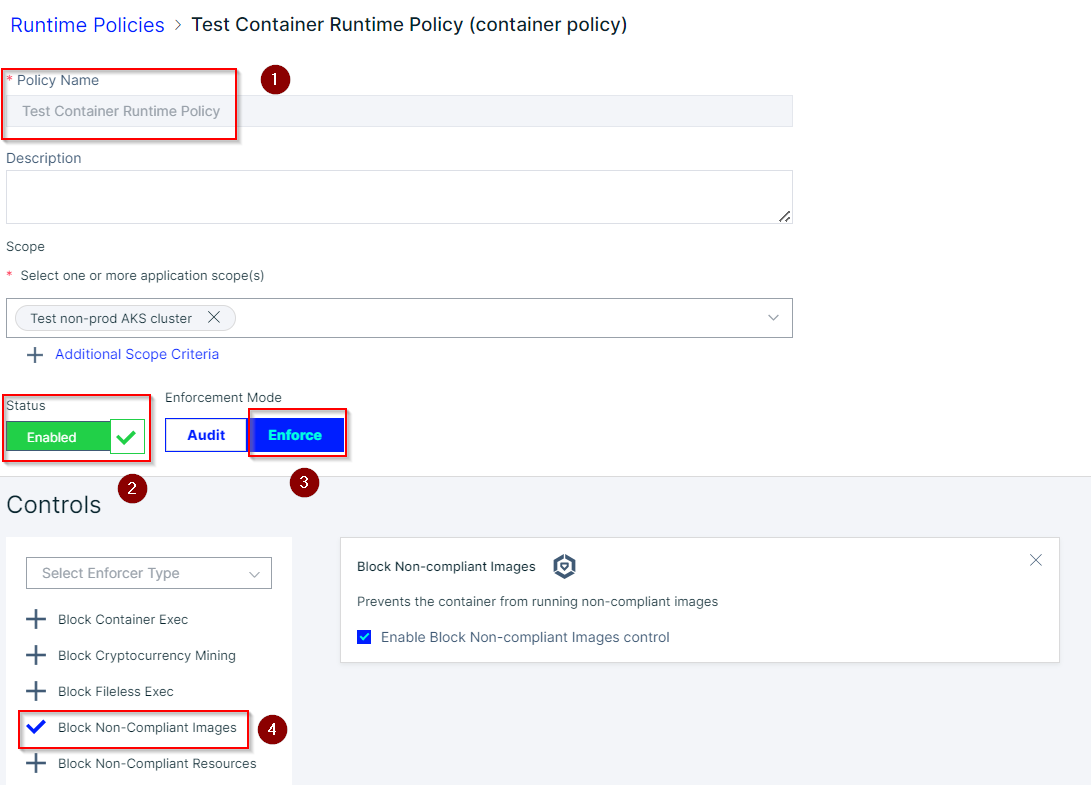
**Controls:**

Block Non-compliant Images: Prevents the container from running non-compliant images

Figure 4: Runtime policy (Navigating to create policy)

A screenshot of a computer

Description automatically generated



# 5.0 Testing of the control ‘Block Non-compliant Images’

Testing the policy 'Runtime Policy’ with ‘Block Non-compliant Images’ control on ‘AKS-AM-EastUS-NP-SREDO’ AKS cluster.

Below image tried to deploy for testing ‘Block Non-compliant Images’ control. But due to ‘Block Non-compliant Images’ control with ‘Enforce’ mode, the action is not allowed to deploy the image.

Image: acreastussredo.azurecr.io/elc/baseimage/php:v20210903-185452

**Trying to deploy the image:**

Deploying image, but action is denied as the image is marked as non-compliant image in Aqua SaaS.



‘Deployment’ .yaml files:

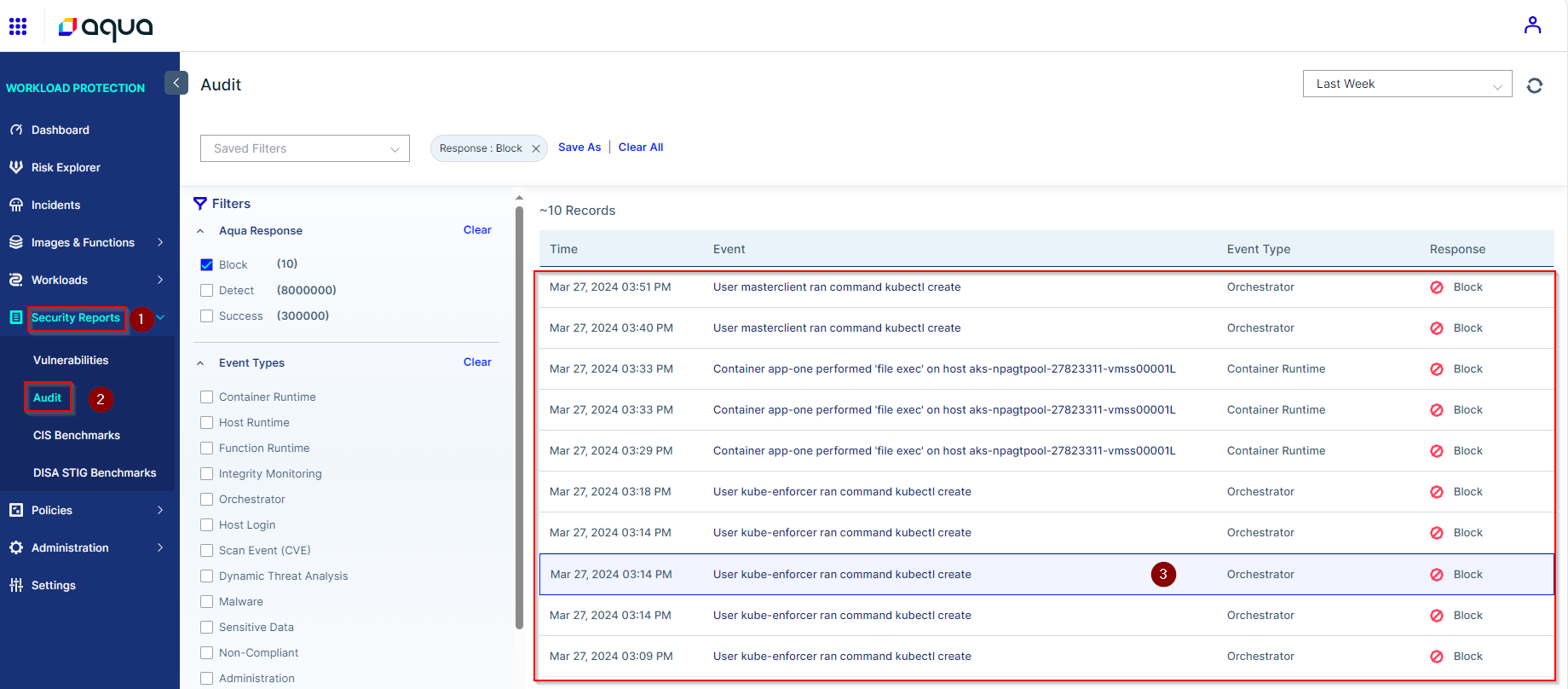
Below Deployment files need to deploy in AKS cluster to test the controls.



SharePoint link of ‘app-two - Block Non-compliant Images’ files:

Tested the controls on AKS cluster ‘AKS-AM-EastUS-NP-SREDO’. Event audit alert has been checked of the cluster on Aqua SaaS console.

Figure 5: Audit event (Navigating to Audit logs)



## 5.2 Scenario 1:

**We are getting below event details in the ‘Security Control and details’ of the event alert:**

**Security Control**

**Block Non-compliant Images - Prevent running containers based on an image that was found to be non-compliant after it was scanned**

**Details**

**Unauthorized image. Image is marked as non-compliant**

Figure 6: Audit event log

A screenshot of a computer

Description automatically generated

The Event alert give us details along with AKS cluster name, Namespace, Aqua policy name, Security Controls and Finding with violated parameters.

# 6.0 Reference links

* [Container Runtime Policies – Aqua Docs (aquasec.com)](https://docs.aquasec.com/saas/workload-protection/runtime-policies/classic-runtime-policies/container-runtime-policies/)
* [Enforcers Overview – Aqua Docs (aquasec.com)](https://docs.aquasec.com/saas/workload-protection/enforcers/enforcers-overview/)
* [Aqua Enforcer – Aqua Docs (aquasec.com)](https://docs.aquasec.com/saas/workload-protection/enforcers/aqua-enforcer/)

# 7.0 Appendix

Figure 1: High-level architecture diagram on page number 4

Figure 2: The AKS cluster Aqua Enforcer group on page number 5

Figure 3: The AKS cluster Aqua Enforcer group setting on page number 5

Figure 4: Runtime policy on page number 6

Figure 5: Audit event on page number 7

Figure 6: Audit event log on page number 8

# 8.1 Abbreviations

|  |  |
| --- | --- |
| **Abbreviations** | **Descriptions** |
| AKS | Azure Kubernetes Service |
|  |  |
|  |  |