**ELC - Runtime Policy with Drift Prevention 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](#_Toc162618513)

[1.0 Purpose and Scope 3](#_Toc162618514)

[2.0 AquaSec Enforcers Architecture 4](#_Toc162618515)

[2.1 AquaSec Runtime Policy 4](#_Toc162618516)

[3.0 The AKS cluster Aqua Enforcer group Setting. 5](#_Toc162618517)

[4.0 Runtime Policy with Drift Prevention control 6](#_Toc162618518)

[5.0 Testing of the control ‘Drift Prevention’ 7](#_Toc162618519)

[5.2 Scenario 1: 9](#_Toc162618520)

[6.0 Reference links 11](#_Toc162618521)

[7.0 Appendix 11](#_Toc162618522)

[8.1 Abbreviations 11](#_Toc162618523)

# Objective of the Document

This document is regarding Runtime policy with drift prevention control, which is help us to prevent executables that are not in the original image of containers which are running on Azure AKS cluster environment.

# 1.0 Purpose and Scope

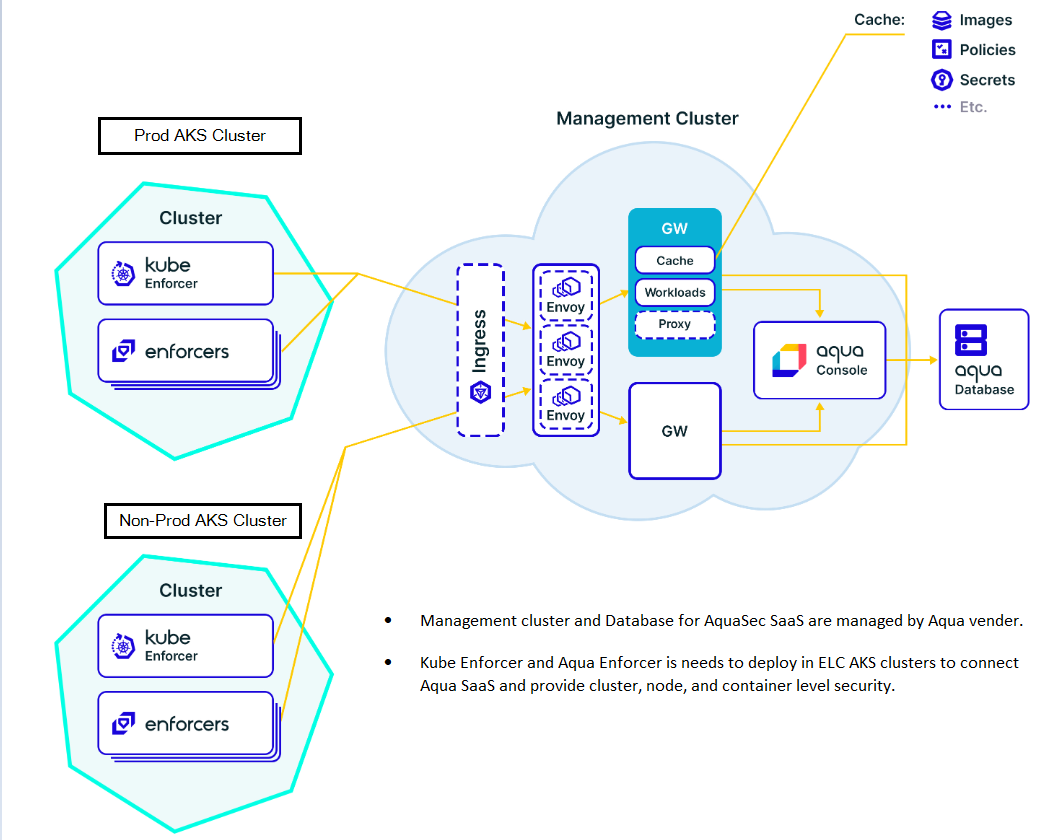
The purpose of Runtime policy is to strength and security in the Azure AKS clusters environment by setting up drift prevention control.

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 Aqua Enforcer group Setting.

The Aqua Enforcer can be deployed in [Docker](https://www.docker.com/products/container-runtime), [container](https://containerd.io/#:~:text=containerd%20is%20available%20as%20a,to%20network%20attachments%20and%20beyond.), [CRI-O](https://docs.openshift.com/container-platform/3.11/crio/crio_runtime.html), [Garden](https://www.cloudfoundry.org/blog/garden-and-runc/), and [Podman](http://docs.podman.io/en/latest/Introduction.html" \t "_blank" \o "Podman) container runtime environments. The Aqua Enforcer provides complete and identical runtime enforcement in all environments.

Figure 2: The AKS cluster Aqua 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 Aqua Enforcer group setting

A screenshot of a computer

Description automatically generated

# 4.0 Runtime Policy with Drift Prevention control

Below steps needs to be performed to configure Runtime policy with Drift Prevention.

**Controls:**

Drift Prevention: Prevent executables that are not in the original image from running.

Figure 4: Runtime policy (Navigating to create policy)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

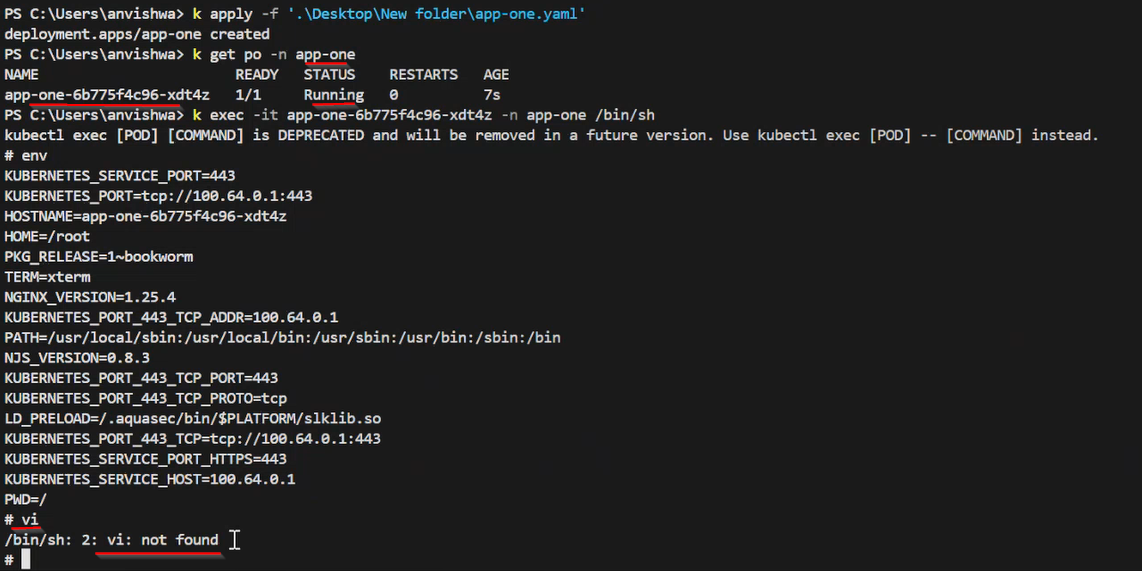
# 5.0 Testing of the control ‘Drift Prevention’

Testing the policy 'Runtime Policy’ with ‘Drift Prevention’ control on ‘AKS-AM-EastUS-NP-SREDO’ AKS cluster.

Below modification are tried to perform in original image for testing ‘Drift Prevention’ control. But due to ‘Drift Prevention’ control with ‘Enforce’ mode, the action is not allowed to change the original image.

**Trying to modify in original image:**

Installing ‘vi editor’ which is not part of the original image.



A screenshot of a computer screen

Description automatically generated

‘Deployment’ .yaml files:

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



SharePoint link of ‘app-one - Drift Prevention.yaml’ 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)

A screenshot of a computer

Description automatically generated

## 5.2 Scenario 1:

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

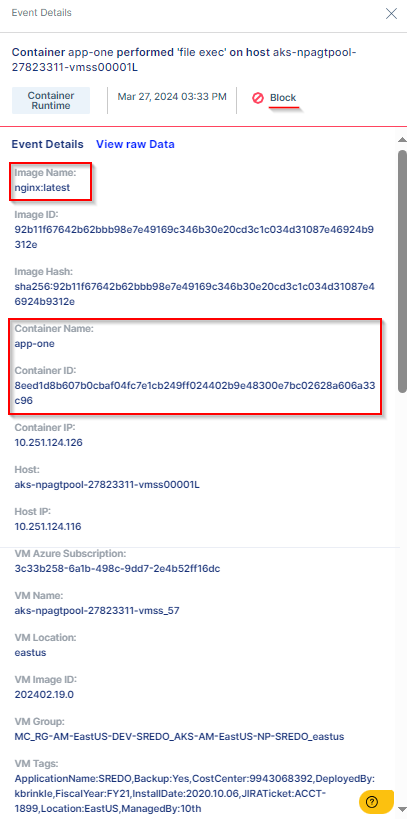
**Resource:**

**/var/lib/dpkg/tmp.ci/postrm**

**Details**

**Unauthorized file lockdown by runtime policy**

Figure 6: Audit event log



A screenshot of a computer

Description automatically generated

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 6

Figure 4: Runtime policy on page number 6

Figure 5: Audit event on page number 8

Figure 6: Audit event log on page number 9

# 8.1 Abbreviations

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