SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 — 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Enabling Integrity Protection for GitOps based Application Deployment

Kugamoorthy Gajananan * Yuji Watanabe * Hirokuni Kitahara * Ruriko Kudo *

Keywords: GitOps, Signature, Integrity

Abstract

For building and deploying applications for modern cloud environment, developers utilize a container orchestration platform (Kubernetes). In this context, GitOps operates by using Git as a single source of truth for declarative infrastructure and applications configurations.

Deploying and managing application in Kubernetes requires to ensure integrity of workloads' resource configurations. Integrity Shield [1] protects integrity of resource configurations of application by requiring that resource manifests of an application are digitally signed before deployed to cluster. However, to use such integrity protection in the context of GitOps, there exist two problems.

First challenge is that ArgoCD transforms the configuration in the Git repository before deploying to the cluster. In cluster, it is not possible to know how the deployed configuration was created using what source information, what resources should exist in the cluster at a given time – not traceable.

Even if the configuration in the Git repository has a signature, the deployed manifest from transformation by ArgoCD does not have a signature. Therefore it is not possible to verify signature of deployed configuration in cluster – not verifiable.

Therefore, we propose an approach that verifies signature of source materials, if the verification passed, auto generates new signature to the generated application manifest - so that admission of the resource manifest can be verified in a cluster and publish manifest build information as verifiable transparent records.

References

[1] Integrity Shield: http://github.com/open-cluster-management/integrity-shield

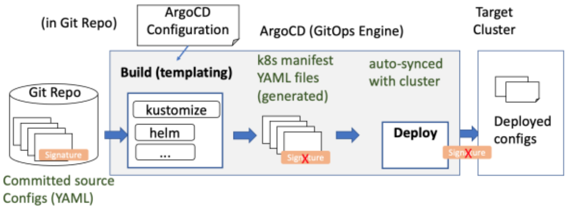

Figure 1. ArgoCD manifest build

* IBM Research, 19-21, Nihonbashi Hakozaki-cho, Chuo-ku, Tokyo 103-8510 Japan