

Support

Documentation

Console

Developers

Start a trial

All Red Hat

Red Hat

Red Hat Blog

Protecting Kubernetes Against MITRE ATT&CK: Persistence

July 14, 2024

Hybrid cloudKubernetesSecurity

Agree and proceed with standard settings

Proceed with Required Cookies only

View cookie preferences

Privacy Statement

SHARE

f

in

X

✉

SUBSCRIBE

[< Back to all posts](#)

This is part three of a nine-part blog series where we examine each of the nine Kubernetes threat vectors across 40 attack techniques and provide actionable advice to mitigate these threats.

- [Part one - Initial Access](#)
- [Part two - Execution](#)
- [Part four - Privilege Escalation](#)
- [Part five - Defense Evasion](#)
- [Part six - Credential Access](#)
- [Part seven - Discovery](#)
- [Part eight - Lateral Movement](#)
- [Part nine - Impact](#)

The third tactic in the Kubernetes attack matrix is Persistence. This tactic groups together techniques that are aimed at enabling an attacker to maintain a presence within a Kubernetes cluster beyond initial access through actions such as taking advantage of Kubernetes controllers, mounting a file to a container, or running recurring Kubernetes Jobs.

StackRox helps guard against these attack vectors by incorporating customizable policy-driven admission control into its platform to enforce security policies on container deployments, enforcing policies on pod configurations, analyzing container image contents, monitoring RBAC configurations for users and service accounts, and collecting runtime activity of all pods.

Technique 3.1: Backdoor container

Issue

More like this

BLOG POST

[Red Hat Insights collaborated with Vulcan Cyber to provide a seamless integration for effective exposure management](#)

BLOG POST

[Confidential Containers with IBM Secure Execution for Linux](#)

ORIGINAL SHOWS

[A new software supply chain security recipe | Technically Speaking](#)

ORIGINAL SHOWS

[Cloud native sustainability with Kepler | Technically Speaking](#)

Page 1 of 5

Similar to [Technique 2.3](#) (New Container) under the Execution tactic, this technique highlights an attacker’s ability to potentially utilize Kubernetes controllers to ensure a container is always running somewhere in the cluster with the ability to execute malicious code.

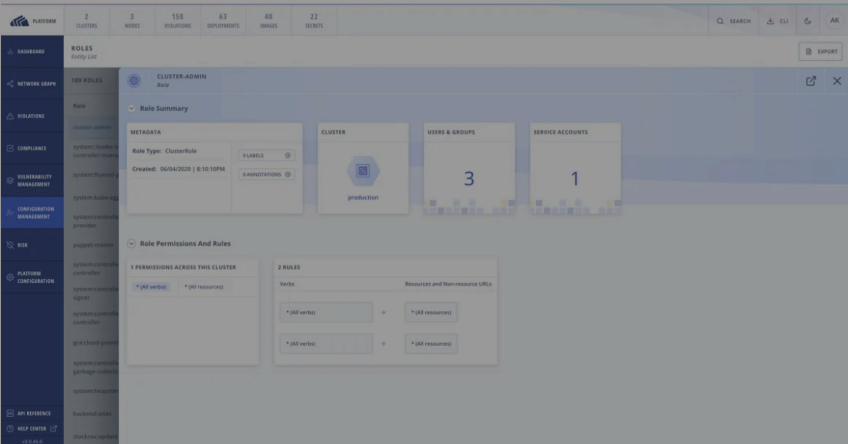
Best Practice for Mitigation

Primary area to configure security controls: Kubernetes

Organizations can implement protections for this technique by controlling and restricting RBAC permissions to create pods and/or abstractions (such as Deployments, DaemonSets, ReplicaSets, and others) that also create pods.

How StackRox Helps

StackRox helps organizations limit Kubernetes RBAC permissions according to the principle of least privilege by monitoring RBAC settings for users and service accounts and identifying ones with overly excessive privileges on clusters. StackRox also analyzes image contents, pod configurations, and runtime activity within pods and gives organizations the ability to optionally block non-compliant container deployments or delete suspicious pods.



Technique 3.2: Writable hostPath mount

Issue

With this technique, the hostPath volume mounts a file or directory to the container, which would allow an attacker to persist on the container host.

Best Practice for Mitigation

Primary areas to configure security controls: Kubernetes and Cloud Provider

Kubernetes

In Kubernetes, users can apply Pod Security Policies to limit the file paths that can be mounted using a host mount or disallow host mounts completely (note that [Persistent Volume Claims bypass this policy](#)). They can also mark any required host paths as read-only whenever possible.

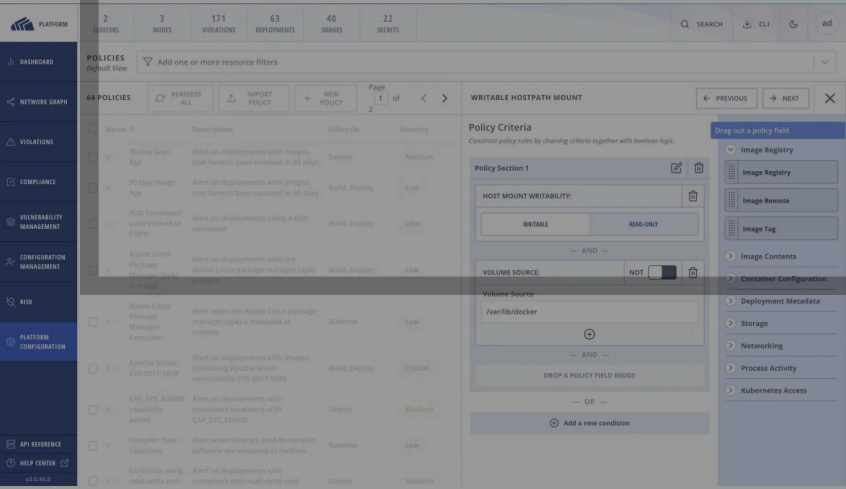
Cloud Provider

When configuring cloud provider environments, teams can limit node lifetimes by ensuring reverse uptime of 24 hours

or less and automatically provision new nodes to replace them.

How StackRox Helps

The StackRox platform helps mitigate this threat by delivering dynamic policy-driven admission control as part of its platform that enables organizations to automatically enforce security policies, including limitations on host mounts and their writability, before containers are ever deployed into Kubernetes clusters.



Technique 3.3: Kubernetes CronJob

Issue

A Kubernetes Job creates one or more pods to accomplish a specific task, and a CronJob creates Jobs on a recurring schedule. An attacker can take advantage of this Kubernetes object to schedule Jobs to run containers that execute malicious code within a cluster.

Best Practice for Mitigation

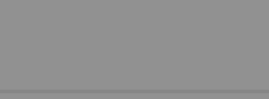
Primary area to configure security controls: Kubernetes

Organizations can take steps to control RBAC permissions to create Jobs and pods and/or the abstractions (such as Deployments, DaemonSets, ReplicaSets, and others) that also create pods.

How StackRox Helps

StackRox helps mitigate against the threat of an attacker leveraging Kubernetes CronJobs for malicious activities by monitor pods running within a cluster, including all runtime activity, as well as monitoring native Kubernetes objects including CronJobs, even if containers are not currently running.

ABOUT THE AUTHOR



Wei Lien Dang

Senior Director, Product and Marketing

in

Wei Lien Dang is Senior Director of Product and Marketing for

Red Hat Advanced Cluster Security for Kubernetes. He was a co-founder at StackBox, which

[Read full bio →](#)

Browse by channel

[Explore all channels →](#)



Automation

The latest on IT automation for tech, teams, and environments



Artificial intelligence

Updates on the platforms that free customers to run AI workloads anywhere



Open hybrid cloud

Explore how we build a more flexible future with hybrid cloud



Security

The latest on how we reduce risks across environments and technologies



Edge computing

Updates on the platforms that simplify operations at the edge



Infrastructure

The latest on the world's leading enterprise Linux platform



Applications

Inside our solutions to the toughest application challenges



Original shows

Entertaining stories from the makers and leaders in enterprise tech

