EKS Security Hardening Checklist

BhanuReddy.cloud | Cloud Security Consulting

Namespace and Pod Security Standards

[ ] Namespaces not labeled to enforce the pod security standards.

[ ] Deployment Pod is running in default namespace.

Root User and Non-Root Enforcement

[ ] StatefulSet containers are running with UID as zero (root user).

[ ] DaemonSet running with UID as zero (root user).

[ ] Deployment containers has runAsNonRoot not set to true.

[ ] StatefulSet has runAsNonRoot not set to true.

[ ] DaemonSet has runAsNonRoot not set to true.

[ ] Deployment containers are running with low user UID.

[ ] Deployment containers are running with low group UID.

[ ] StatefulSet containers are running with low user UID.

[ ] StatefulSet containers are running with low group UID.

[ ] DaemonSet are running with low user UID.

[ ] DaemonSet containers are running with low group UID.

EKS Security Hardening Checklist

Privileges, Capabilities and Host Access

[ ] Deployment containers are running with default capabilities.
[ ] StatefulSet with containers are running with default capabilities.
[ ] DaemonSet running with default capabilities.
[ ] StatefulSet containers are running with privileged flag set to true.
[ ] DaemonSet running with SYS_ADMIN privileges.
[ ] Deployment containers running with NET_BIND_SERVICE capability.
[ ] DaemonSet containers are not set with drop NET_RAW capability.
[ ] DaemonSet containers are running with the hostPID flag set to true.
[ ] DaemonSet containers are running with hostNetwork flag set to true.
[ ] DaemonSet has hostPort not set to 0.
[ ] DaemonSet pod is mounting a host-sensitive os directory.
[ ] DaemonSet has socket mounted inside the containers for pod.
[ ] DaemonSet containers are set with hostPath volumes mounted.

Service Account Tokens and RBAC

[ ] Deployment pods automountServiceAccountToken not set to false.
[ ] StatefulSet pod automountServiceAccountToken not set to false.
[ ] DaemonSet has pods automountServiceAccountToken not set to false.
[ ] Default service account token automountServiceAccountToken not set to false.
[ ] Cluster Roles have excessive permissions to networking resources.
[ ] Overly permissive verb assigned to configmaps resources in cluster roles.

Read-Only Filesystems and Seccomp

[ ] Deployment container root filesystem is not mounted as read only.
[ ] StatefulSet containers root filesystem is not mounted as read only.
[ ] DaemonSet running with containers where root filesystem is not mounted as read only.
[ ] Deployment containers are not set with Default Seccomp profile.
[ ] StatefulSet containers are not set with default seccomp profile.
[ ] DaemonSet containers are not set with default seccomp profile.

EKS Security Hardening Checklist

Resource Requests and Limits

[ ] StatefulSet with containers are not specified with CPU requests usage.
[ ] StatefulSet with containers are not configured with CPU limit usage.
[ ] StatefulSet with containers are not specified with memory requests usage.
[ ] StatefulSet with containers are not configured with memory limit usage.
[ ] Deployment containers are not specified with CPU requests usage.
[ ] Deployment containers are not configured with CPU limit usage.
[ ] Deployment containers are not specified with memory requests usage.
[ ] Deployment containers are not configured with memory limit usage.
[ ] DaemonSet containers are not specified with CPU requests usage.
[ ] DaemonSet containers are not configured with CPU limit usage.
[ ] DaemonSet containers are not specified with memory requests usage.
[ ] DaemonSet containers are not configured with memory limit usage.

Image Hygiene

[ ] Deployment container images with tag ':latest' used.