1 CheatSheet: Kubernetes Security CLOUD

- PDF Link: cheatsheet-k8s-security-A4.pdf, Category: Cloud
- Blog URL: `https://cheatsheet.dennyzhang.com/cheatsheet-k8s-security-A4`
- Related posts: Kubectl CheatSheet, Kubernetes Yaml Templates, #denny-cheatsheets

File me Issues or star this repo.

1.1 Summary

Name	Summary
Kubernetes RBAC	Kubernetes API Security
Pod Security Policy	enable fine-grained authorization of pod creation and update
Pod security context	
Admission Controls	Intercepts requests to the Kubernetes API server prior to per
Network security policy	a specification of how groups of pods are allowed to communi
Linux capabilities	Allow you to break apart the power of root into smaller grou
SElinux	
Kubelet authentication/authorization	
AppArmor	a Linux kernel security module: reduce application attack su
Sandboxed Pods & gVisor	

1.2 Regulations

Name	Summary
GDPR	EU General Data Protection Regulation
PCI DSS	Payment Card Industry Data Security Standard

1.3 Basic Concepts

Name	Summary
IdM	Identity Management
AuthN vs AuthZ	Authentication vs Authorization
OAuth vs OpenID	OAuth: Open Authorization; OpenID: an authentication mechanism
OAuth vs OAuth2	
SAML	
Malware	short for "malicious software"
virus	Infects other programs, caryying out malicious missions
worm	It doens't need to infect another program. It performs and replicates by i
trojan horse	A program that contains malware like a virus or worm
ransomware	A link of attachment executes a malware to encrypt your system and den
vishing	A common type of social engineering that is done over the phone
phishing	A common type of social engineering that fools you to respond to a malic
Data classifications levels	Restricted, Private/Protected, Confidential, Public
PII	Personally identifiable information

1.4 Security - PodSecurityPolicy

- A PodSecurityPolicy is a cluster-level resource that controls security sensitive aspects of the pod specification.

Yaml	Summary
podsecurity/securitycontext-user.yaml	Configure userid, at both pod and container levels
podsecurity/podsecurity-privileged.yaml	Create pod security with privileged access
podsecurity/podsecurity-restricted.yaml	Create pod security with restricted access, then apply it la
podsecurity/podsecurity-enforce.yaml	Enforce policy security by defining role and cluster role
podsecurity/podsecurity-advanced.yaml	A more complicated definition of pod security policy
podsecurity/podsecurity-example.yaml	A full example with everything included
Reference	Link: Kubernetes Yaml Templates, Link: kubectl cheatshe

1.5 Security - NetworkPolicy

Yaml	Summary
networksecurity/networksecurity-denyall-ingress.yaml	Allow all ingress
networksecurity/networksecurity-allowall-ingress.yaml	Deny all ingress
networksecurity/networksecurity-denyall.yaml	Deny all ingress and egress
networksecurity/networksecurity-pod.yaml	Whitelist traffic control
networksecurity/networksecurity-complicated.yaml	A comprehensive network policy exam
networksecurity/networksecurity-port.yaml	Allow TCP 443 from one namespace
networksecurity/networksecurity-deny-othernamespaces.yaml	Deny all ingress traffic from other nam
networksecurity/networksecurity-denyegress-exceptdns.yaml	Deny all egress traffic except DNS
Reference	Link: Kubernetes Yaml Templates, Li

1.6 Admission Controllers

- An admission controller is a piece of code that intercepts requests to the Kubernetes API server prior to persistence of the object

https://raw.githubusercontent.com/dennyzhang/cheatsheet.dennyzhang.com/master/cheatsheet-k8s-security-A4/admission$_{\text{controller.png}}$

Name	Summary
Example: admission webhook	GitHub: denyenv-validating-admission-webl
Example: Admission controller for guarding namespace	GitHub: k8s-namespace-guard

1.7 More Resources