1 CheatSheet: Kubernetes Security

CLOUD

Updated: January 12, 2019

- PDF Link: cheatsheet-k8s-security-A4.pdf, Category: Cloud
- Blog URL: https://cheatsheet.dennyzhang.com/cheatsheet-k8s-security-A4
- \bullet 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 updates.
Pod security context	
Admission Controls	Intercepts requests to the Kubernetes API server prior to persistence of the object
Network security policy	a specification of how groups of pods are allowed to communicate with each other.
Linux capabilities	Allow you to break apart the power of root into smaller groups of privileges
SElinux	
$Kubel et\ authentication/authorization$	
AppArmor	a Linux kernel security module: reduce application attack surface
Sandboxed Pods & gVisor	

1.2 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 later
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 cheatsheet

1.3 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 example
networksecurity/networksecurity-port.yaml	Allow TCP 443 from one namespace
networksecurity/networksecurity-deny-othernamespaces.yaml	Deny all ingress traffic from other namespaces
networksecurity/networksecurity-denyegress-exceptdns.yaml	Deny all egress traffic except DNS
Reference	Link: Kubernetes Yaml Templates, Link: kubectl cheatsheet

1.4 Admission Controllers

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

 $https://raw.githubusercontent.com/dennyzhang/cheatsheet.dennyzhang.com/master/cheatsheet-k8s-security-A4/admission_{controlled}. The security of the controlled con$

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

1.5 More Resources

License: Code is licensed under MIT License.

Updated: January 12, 2019