Kubernetes guild

Network & Security

(basic)

LMJ

Agenda

Meet Paul

- Ingress
- Security Context
- Networking
- Network Policies / Calico
- Secrets
- AppArmor
- Vulnerability Advisor

Wrap-up

Paul

IBM Software Engineer

Very experienced developer, with a vast experience in backend applications. He learns fast and uses his networking to connect to the right people, when necessary.

Goals

- Leverage Cloud engineering skills.
- Implement Microservices on his current project.
- Make sure he is compliant to IBM best practices.

Pain Points

- Hard to follow tech trends and pick the right one.
- Introduce a new technology to the team is tough.
- Feel insecure when asked to contribute with network and security insights.

Motivations:

Deliver the project in-time and with low maintenance cost. A good design prunes a good product.

Paul wants to expose his services to be consumed by the rest of the team.

. Inbound connections routing

What else?
. Load balancer
. Terminate SSL
. Name based virtual hosting

Ingress
. https://console.bluemix.net/docs/containers/cs_apps.html#cs_apps_public_ingress
. https://kubernetes.io/docs/concepts/services-networking/ingress/

Paul wants to avoid someone to change the time in your pod

. Linux capabilities

What else?
. user and groups assignments

SecurityContext
. https://kubernetes.io/docs/tasks/configure-pod-container/security-context/
. http://man7.org/linux/man-pages/man7/capabilities.7.html

Paul wants to access a service from other department

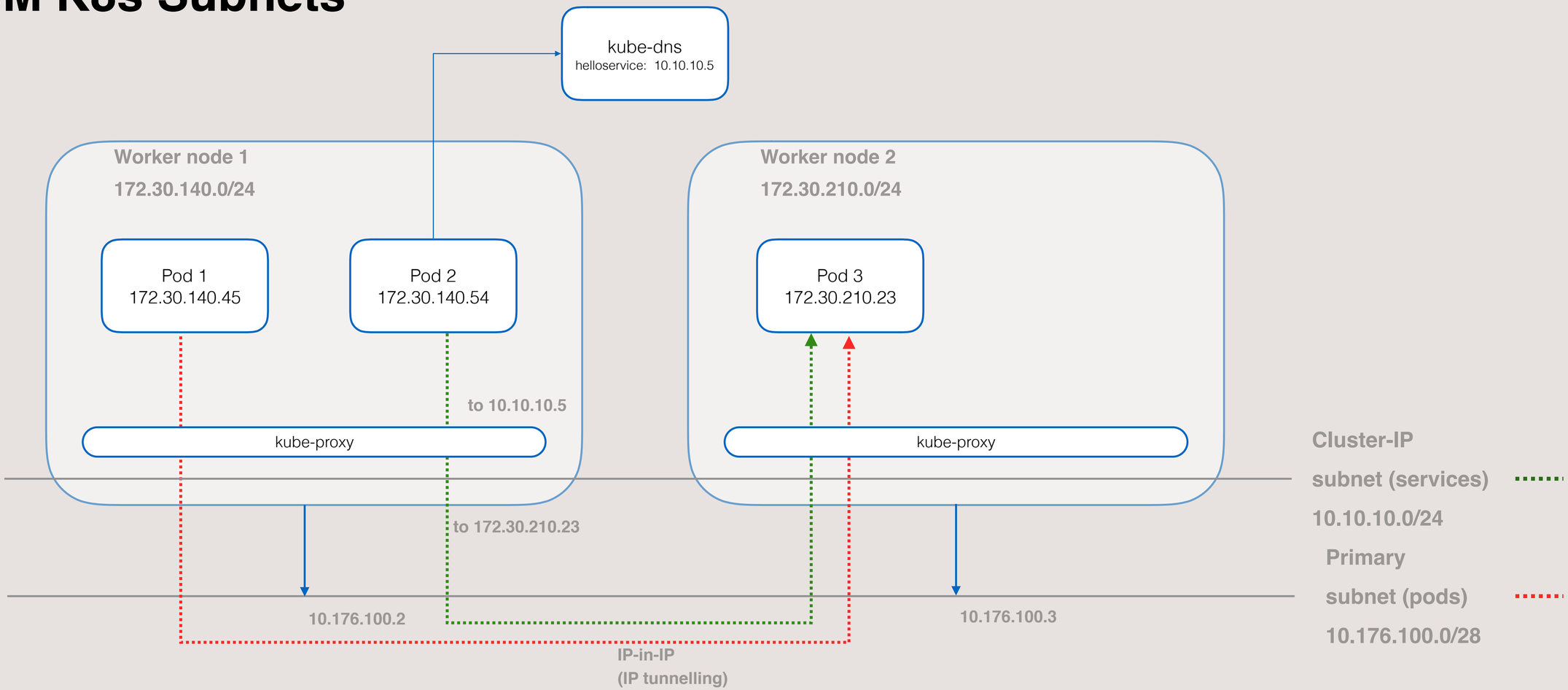
. 2 subnets - for Pods and for Services

<service_name>.*<namespace>*.svc.cluster.local
<pod_IP>.*<namespace>*.svc.cluster.local

Networking

. https://kubernetes.io/docs/concepts/services-networking/dns-pod-service/

IBM K8s Subnets



What if Paul needs to use an external service from his applications?

. still networking/DNS…

. Simplifies and abstracts external services endpoints.

. It can point to a different cluster (Intranet) or to a public service.

. and how about the physical network?

Paul wants to protect his pods from unwanted internal access

. Cluster-wide network policies (or think about mini-firewalls, distributed)

NetworkPolicy

. https://kubernetes.io/docs/concepts/services-networking/network-policies/

Calico

. https://www.projectcalico.org/
. https://console.bluemix.net/docs/containers/cs_security.html#cs_security
. https://www.ibm.com/blogs/bluemix/2017/07/kubernetes-and-bluemix-container-based-workloads-part5/

. IP-Table based policies doesn’t mean you need to throw your firewall away!

Paul wants to protect credentials/keys in production

. Environment variables
. Mounted volumes

. Secrets and Pod lifetime (applicable to mounted volumes)

Secrets

. https://kubernetes.io/docs/concepts/configuration/secret/

. Ensure who can access Secrets
. Base64 encoding at least

Paul is using not reviewed open-source libraries in his Beta test

. Control what an application can use from the host machine (worker node)

. Enforcing or Complain modes
. Armors are (going to be) bundled (high/medium/low)
. Armors can be created/customized

App Armor

. https://kubernetes.io/docs/tutorials/clusters/apparmor/
. https://github.ibm.com/alchemy-containers/armada-docker-security

Paul is using public images from the Internet to speed up his work

. Images are available everywhere, and even coming from a "trusted" source don’t ensure its quality.

Vulnerability advisor

. https://console.bluemix.net/docs/containers/va/va_index.html#va_index
. http://w3.blueprint.sby.ibm.com/b_dir/blueprint.nsf/url/AB649851?OpenDocument

Paul

IBM Cloud Engineer

What he learned (among other things):

. Microservices architecture is nice but hard.

. Entire team must be involved on the design.

. Quality plan for non-functional requirements - Network/Sec.

. Kubernetes is a part of something bigger.

What is next?

. Guidelines

. Design patterns

. Automation

Who is up to help? #kubernetes_guild

Questions

Thank you