DEVCONF.us

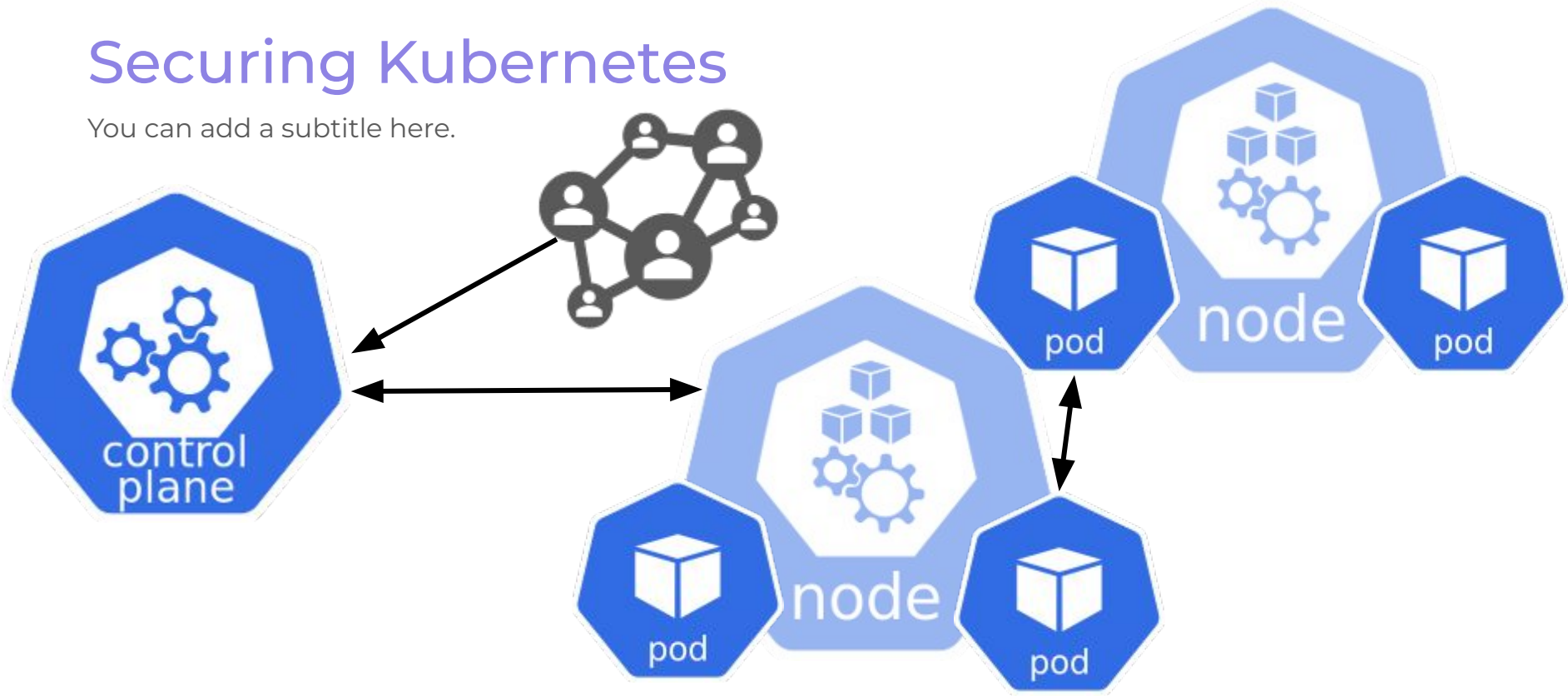
Stop Kubernetes' Revolving Door: A Hands-On Workshop to Secure a Kubernetes Cluster

Savitha Raghunathan
Senior Software Engineer, Red Hat

Rey Lejano
Solutions Architect, Red Hat

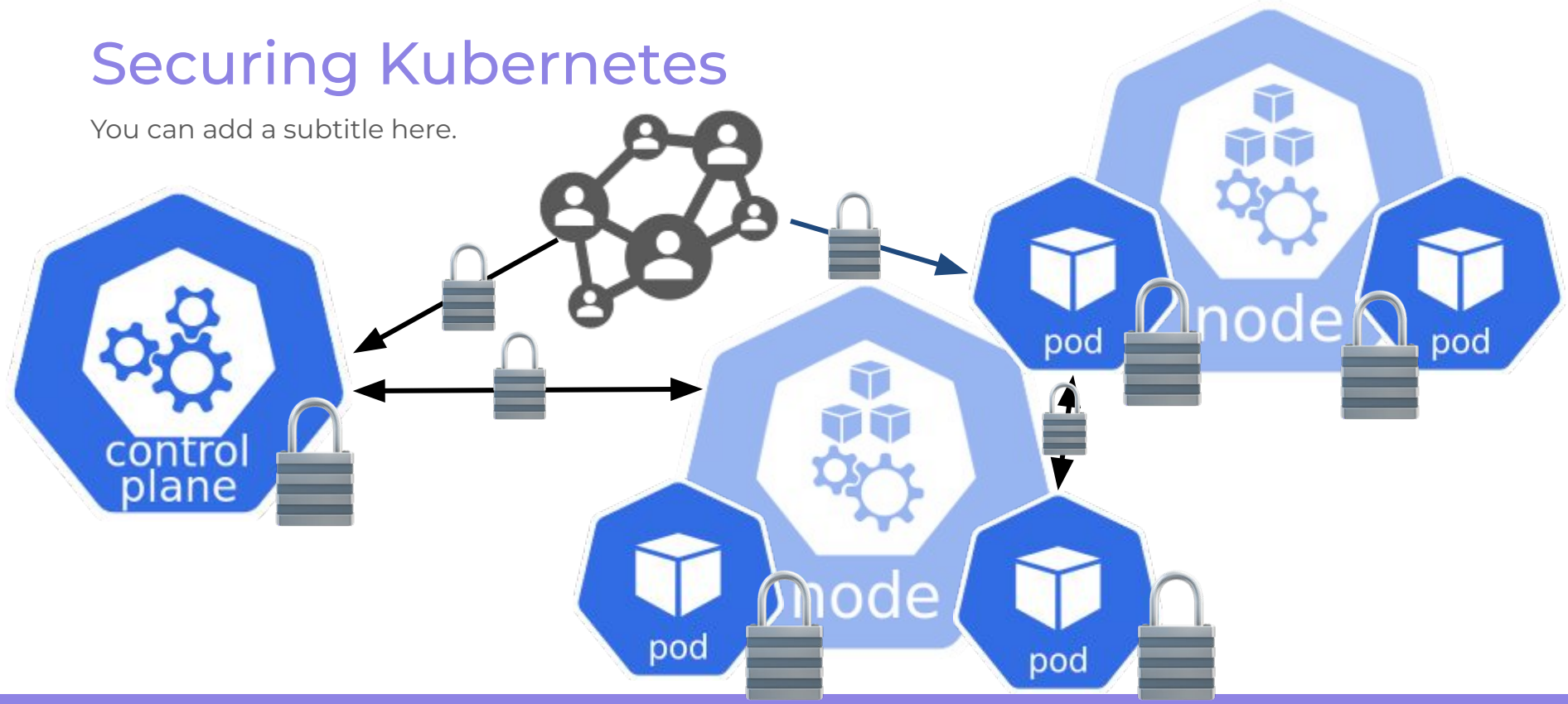
Securing Kubernetes

You can add a subtitle here.



Securing Kubernetes

You can add a subtitle here.



Kubernetes Security Checklist

https://kubernetes.io/docs/concepts/security/security-checklist/

Basic security guidance to improve the security posture of Kubernetes but is not sufficient

Security checklist topics:

Authentication & Authorization

Network Security

Pod Security

Admission Controllers

Logs and Auditing

Pod Placement

Secrets

Images

Workshop

Workshop Environment

RHEL

Red Hat Enterprise Linux

RHEL releases are based on Fedora

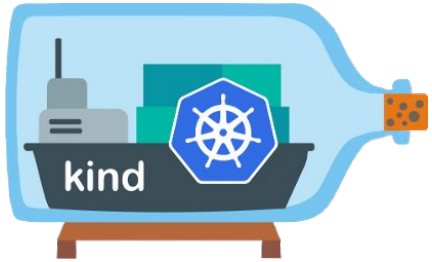
Fedora is the community distribution

- 2 year life cycle support
- community support

RHEL is the enterprise distribution

- 10 year life cycle support
- enterprise-level support available

kind



Kubernetes in Docker

Run local Kubernetes clusters using Docker container “nodes” on MacOS, Windows, or Linux.

Used by the Kubernetes project to test and run integration tests.

Pre-reqs:

- Docker
- kubectl

https://kind.sigs.k8s.io/docs/user/quick-start

Access the Workshop

GitHub:

https://github.com/cloudnativeessentials/101-kubernetes-security

Workshop:

https://demo.redhat.com/workshop/y5mmdf

Password:

pqw5zenr

Accessing VM via SSH

Requirements:

- Ability to SSH (native in Linux and MacOS)
- Windows: WSL or Putty

Login command in the format `ssh <user>@<machine fqdn or IP>`

e.g. `ssh lab-user@rhel9.77.sandbox77.opentlc.com`

Enter the password when promoted

```
$ ssh lab-user@rhel9.77.sandbox77.opentlc.com
The authenticity of host 'rhel9.77.sandbox777.opentlc.com (35.222.22.100)' can't be established.
ED25519 key fingerprint is SHA256:vAA5XSjyDd2pkPBOuz9XLSYvxYrQq9M58DEmlmmoo/M.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added 'rhel9.77.sandbox77.opentlc.com' (ED25519) to the list of known hosts.
lab-user@rhel9.77.sandbox77.opentlc.com's password:

[lab-user@rhel9 ~]$
```

Kubernetes Security Workshop

Topics covered

Authentication & Authorization

- system:masters group is not used for user or component authentication after bootstrapping
- the Role Based Access Control Good Practices are followed for guidance related to authentication and authorization.

Kubernetes Security Workshop

Topics covered

Network Security

- CNI plugins in-use supports network policies.
- Ingress and egress network policies are applied to all workloads in the cluster.
- Default network policies within each namespace, selecting all pods, denying everything, are in place.

Kubernetes Security Workshop

Topics covered

Pod Security

- RBAC rights to create, update, patch, delete workloads is only granted if necessary.
- Appropriate Pod Security Standards policy is applied for all namespaces and enforced.
- For nodes that support it, Seccomp is enabled with appropriate syscalls profile for programs.

Kubernetes Security Workshop

Topics covered

Admission Controllers:

- A pod security standard policy is enforced by the Pod Security Admission or/and a webhook admission controller.