Configuring and Managing Kubernetes Security

KUBERNETES SECURITY FUNDAMENTALS

Anthony E. Nocentino
ENTERPRISE ARCHITECT @ CENTINO SYSTEMS

@nocentino www.centinosystems.com

Course Overview

Kubernetes Security Fundamentals

Managing Certificates and kubeconfig Files

Managing Role Based Access Controls

Summary

Authenticating to the API Server

Authentication Plugins

Users

ServiceAccount

Authorization

Securing the API Server

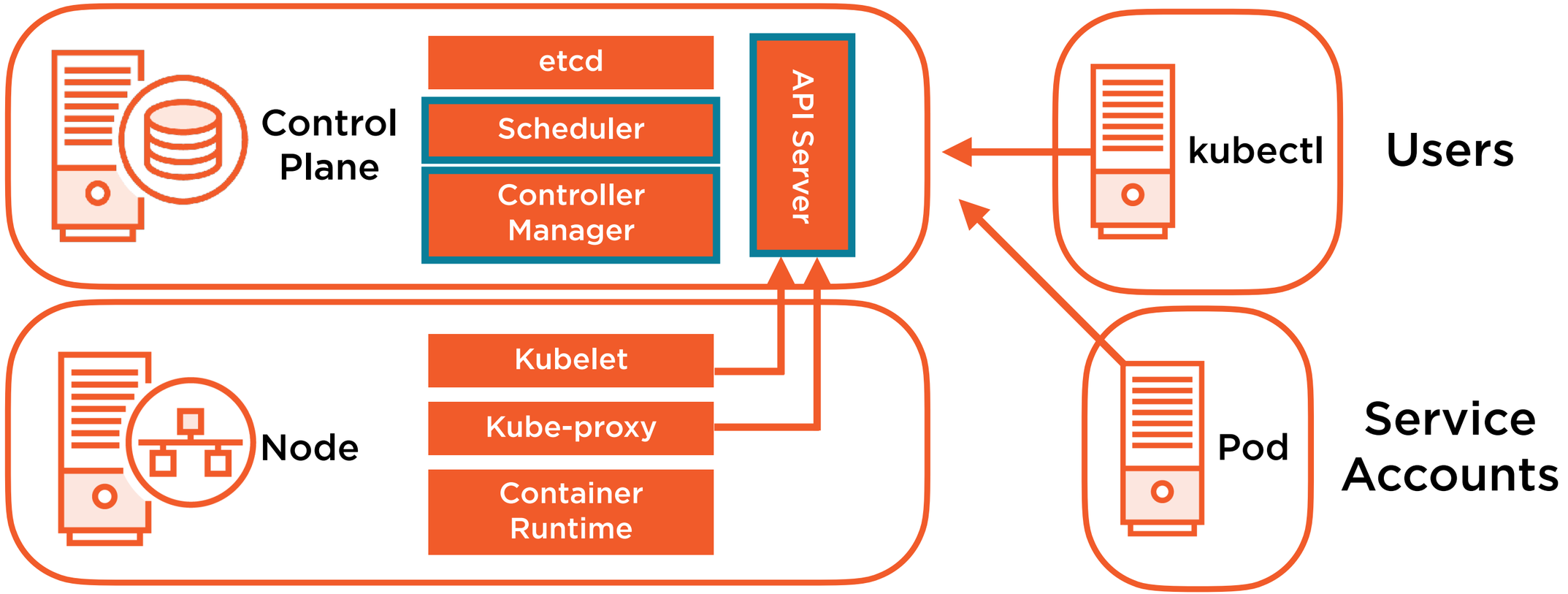
Authentication

Authorization

Admission Control

Managing the Kubernetes API Server and Pods

API Server - Authentication



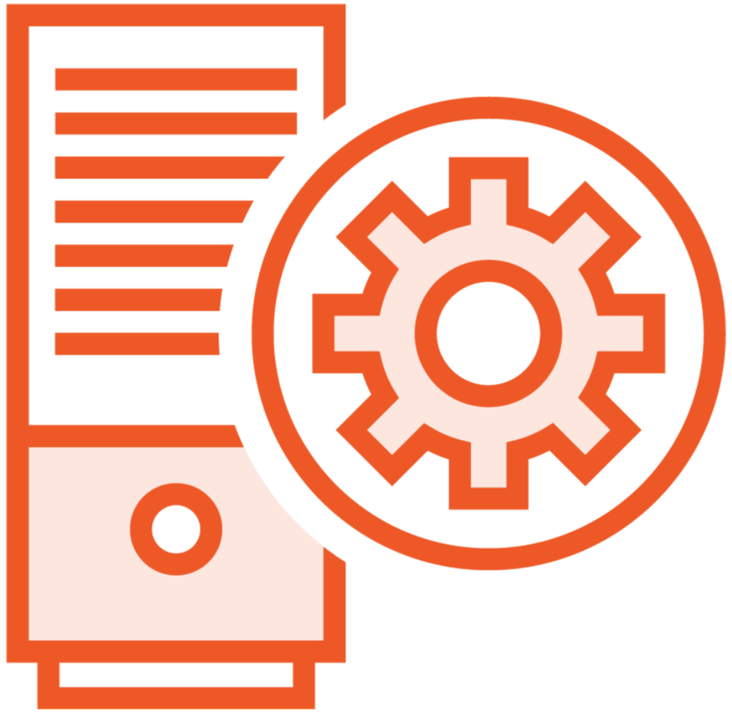
Authentication Plugins

Client Certificates	Authentication Tokens	Basic HTTP
Most commonly used	HTTP Authorization Header in the client request	Static password file
Default when using kubeadm	Service Accounts	Only read during API Server startup
Common Name (CN) is the username	Bootstrap Tokens and Static File	Simple to set up and use (Dev)

Users in Kubernetes

- Users are managed by external systems
- No User API Object
- Authentication plugin implements authentication
- Authentication is pluggable
- Usernames used for access control and logging
- Users can be aggregated into groups

Service Accounts



Authenticate Pods to the API Server

Apply permissions for authorization

Namespaced API Object

Default `ServiceAccount` per Namespace

All Pods must have a `ServiceAccount` defined

Create `ServiceAccounts` Object

Service Accounts Credentials

Credential stored as a `Secret`

- CA Certificate
- Token
- Namespace

Interact with the API server

Image pull secret

Mounted inside a Pod as files using a `Volume`

`/var/run/secrets/kubernetes.io/serviceaccount`

Creating a ServiceAccount

```
apiVersion: v1
kind: ServiceAccount
metadata:
 name: mysvcaccount1
```

```
kubectl create serviceaccount mysvcaccount1
```

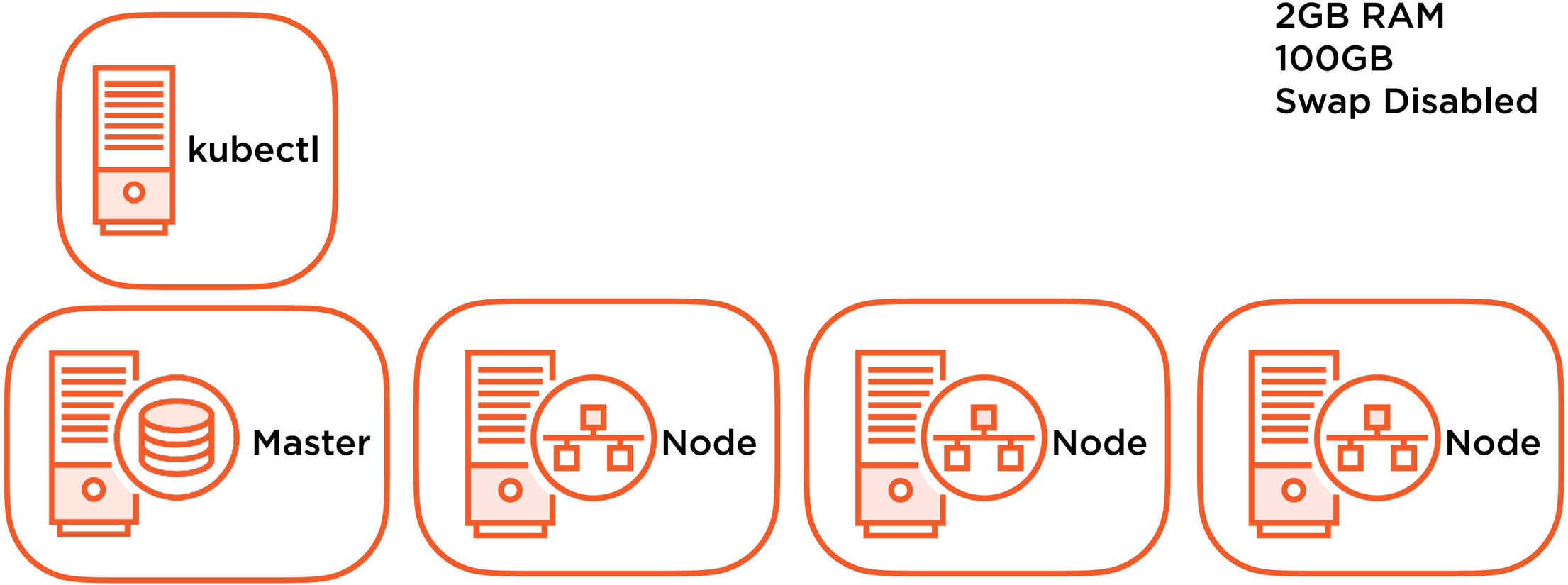
Configuring a Service Account in a Pod Spec

```
spec:
   serviceAccount: mysvcaccount1
   containers:
   - image: nginx
     name: nginx
```

Hostnames set
Host file on each

Lab Environment

Ubuntu 16.0.4
VMware Fusion VMs
2vCPU
2GB RAM
100GB
Swap Disabled



c1-master1	c1-node1	c1-node2	c1-node3
172.16.94.10	172.16.94.11	172.16.94.12	172.16.94.13

Demo

Investigating Certificate based authentication

Working with Service Accounts

Accessing the API Server inside a Pod

Authorization Plugins

Role-based Access Control (RBAC)

Node

Attribute-based Access Control (ABAC)

Demo

Managing authorization for a ServiceAccount

Review

Authenticating to the API Server

Authentication Plugins

Users

ServiceAccount

Authorization

Up Next:
Managing Certificates and kubeconfig Files