KubeCon | CloudNativeCon

China 2018

Hardening Multi-Cloud Kubernetes Clusters as a Service

Who We Are

Alban Crequy

CTO Kinvolk

Love Kubernetes,
Containers, Linux

Dirk Marwinski

Development Architect SAP
Gardener Team

Agenda

Project Gardener

Warm-up: Traditional Pen-Testing

The race: A Second Opinion

Cool-down: Security Add-on

Summary & Conclusion

KubeCon | CloudNativeCon

China 2018

Project “Gardener”

WHAT IS GARDENER?

@ANTHEAJUNG

100% KUBERNETES

OPEN SOURCE

CNCF officially certified!

KUBERNETES IN KUBERNETES IN KUBERNETES!

hybrid cloud

HOMOGENEOUS INFRASTRUCTURE

ARCHITECTURE IN THREE COMPONENTS

RUNS THE GARDENER

a kubernetes controller responsible for managing custom resources

CONTAINS SHOOT CLUSTER'S [CONTROL PLANE] AS WORKLOAD

CONTAINS ONLY WORKER NODES

AN EXTENDED API SERVER &

A BUNDLE OF KUBERNETES CONTROLLERS

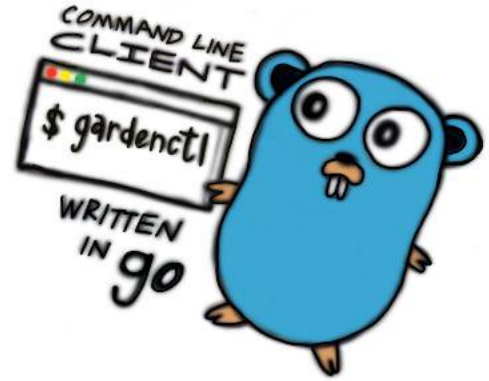
THAT DEFINES AND MANAGES NEW API OBJECTS USED FOR MANAGEMENT OF KUBERNETES CLUSTER

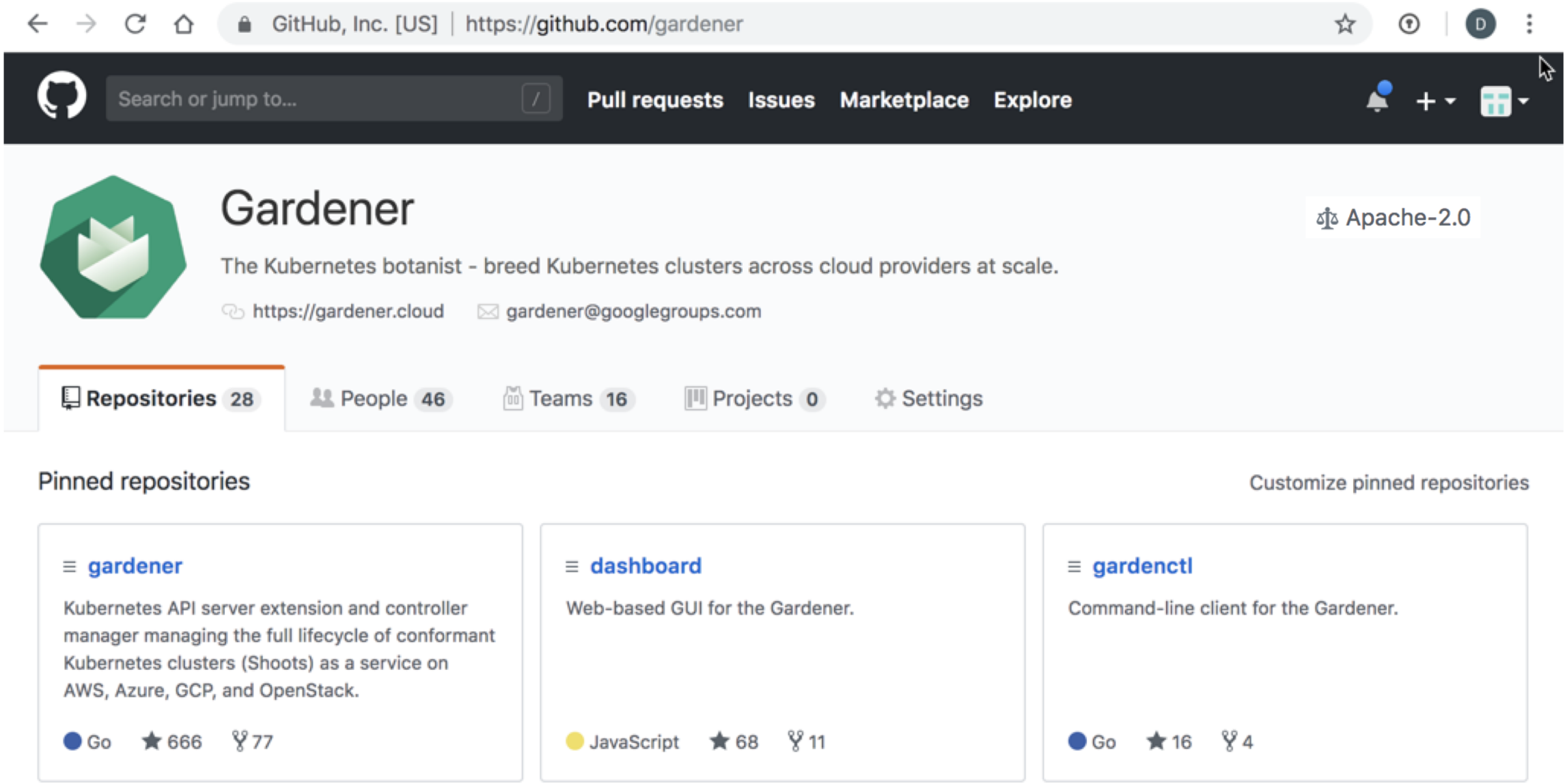
A SERVICE TO MANAGE LARGE-SCALE KUBERNETES CLUSTER

THE KUBERNETES BOTANIST

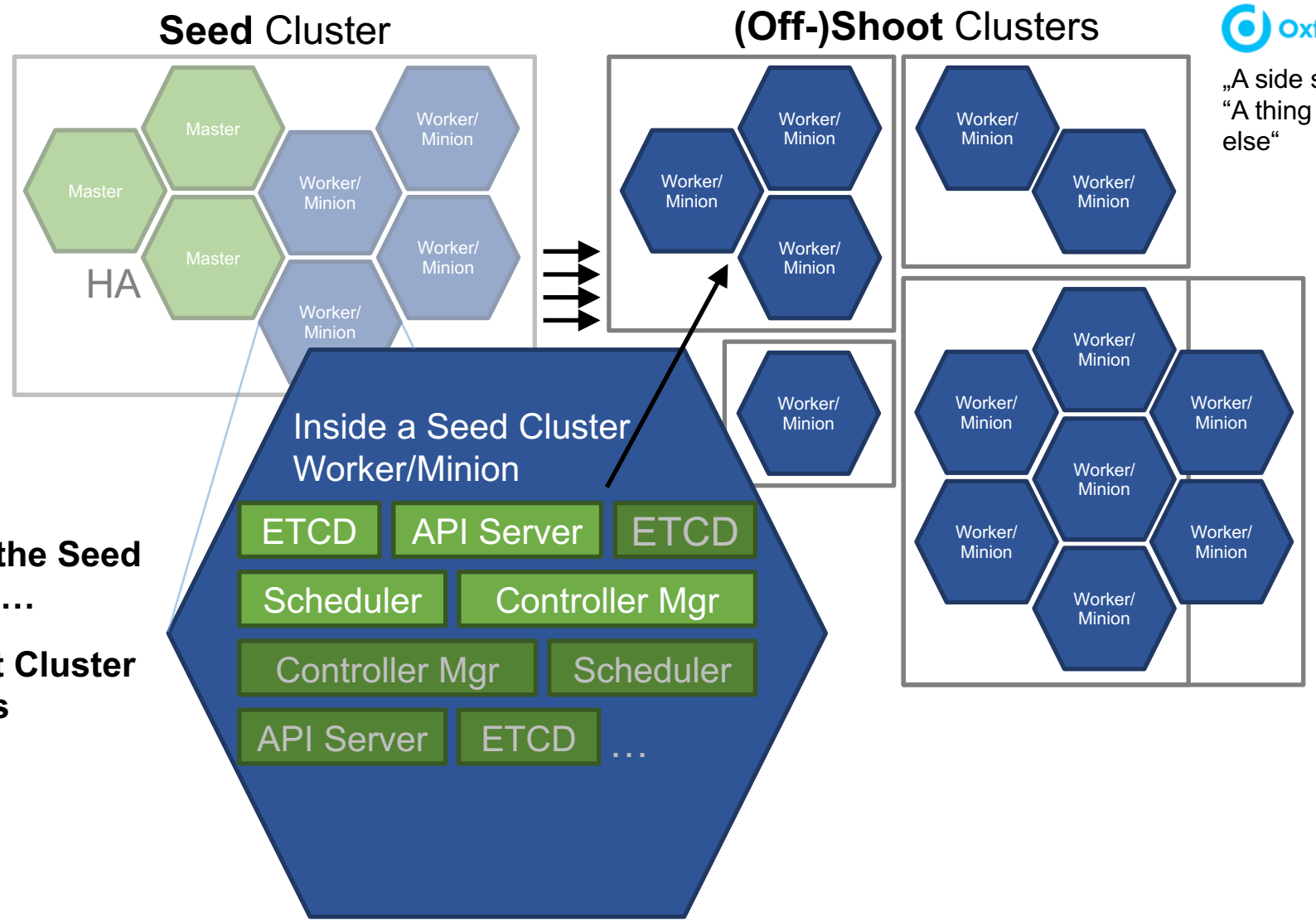
INTERACT WITH CENTRAL UI

"gardener DASHBOARD"




GitHub, Inc. [US] | https://github.com/gardener
Search or jump to...
Pull requests
Issues
Marketplace
Explore
Gardener
Apache-2.0
The Kubernetes botanist - breed Kubernetes clusters across cloud providers at scale.
https://gardener.cloud
gardener@googlegroups.com
Repositories 28
People 46
Teams 16
Projects 0
Settings
Pinned repositories
Customize pinned repositories
gardener
Kubernetes API server extension and controller manager managing the full lifecycle of conformant Kubernetes clusters (Shoots) as a service on AWS, Azure, GCP, and OpenStack.
Go 666 77
dashboard
Web-based GUI for the Gardener.
JavaScript 68 11
gardenctl
Command-line client for the Gardener.
Go 16 4

Gardener Cluster Setup



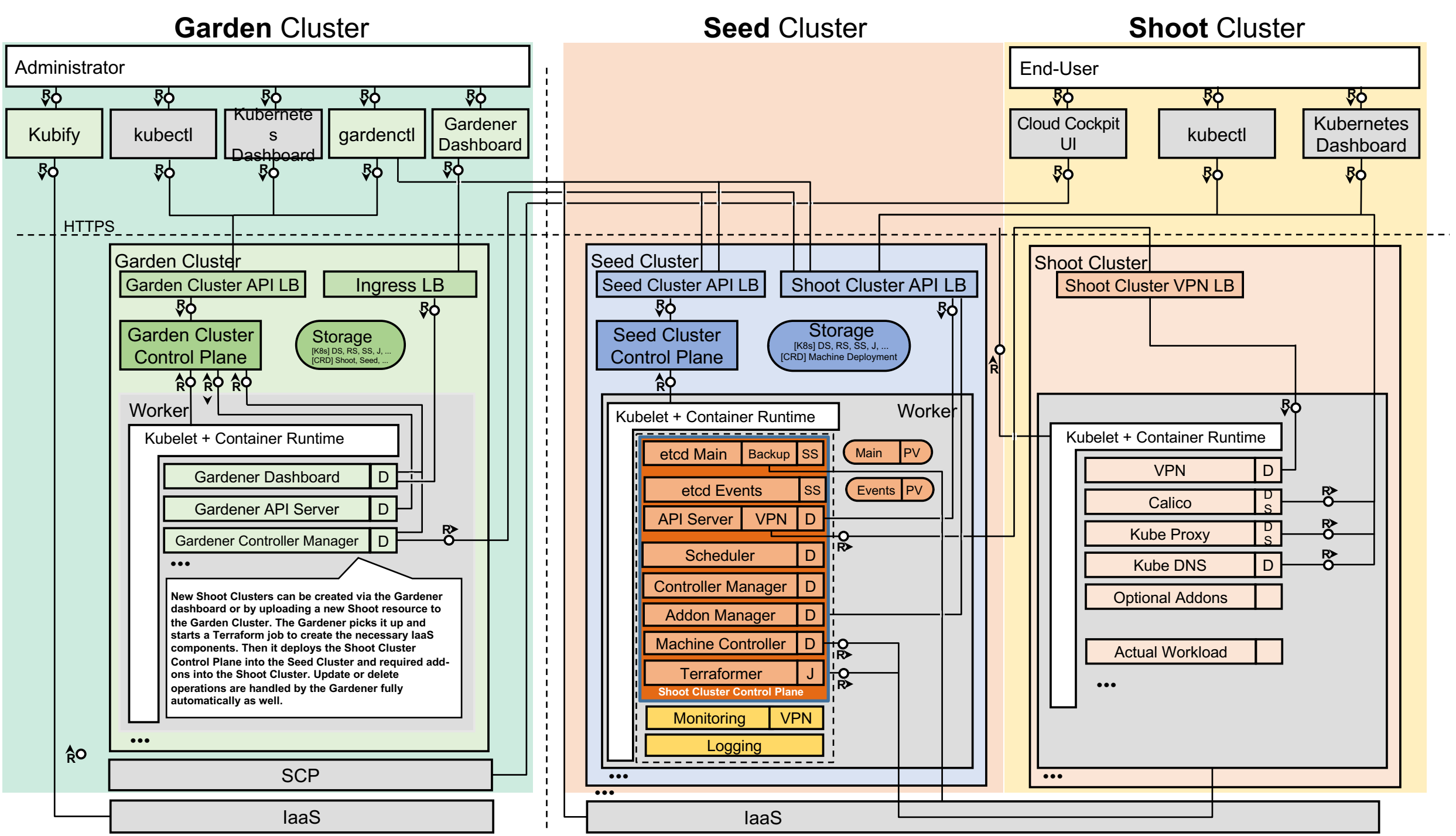
Oxford Dictionaries

„A side shoot or branch on a plant“ or “A thing that develops from something else“

Zooming into the Seed Cluste reveals…

Multiple Shoot Cluster Control Planes

Machine De-/Provisioning, Self-Healing, Auto-Update and Auto-Scaling via our own Machine Controller Manager


Garden Cluster
Seed Cluster
Shoot Cluster
Administrator
Kubify
kubectl
Kubernetes Dashboard
gardenctl
Gardener Dashboard
End-User
Cloud Cockpit UI
kubectl
Kubernetes Dashboard
HTTPS
Garden Cluster
Garden Cluster API LB
Ingress LB
Garden Cluster Control Plane
Storage
[K8s] DS, RS, SS, J, ...
[CRD] Shoot, Seed, ...
Worker
Kubelet + Container Runtime
Gardener Dashboard D
Gardener API Server D
Gardener Controller Manager D
New Shoot Clusters can be created via the Gardener dashboard or by uploading a new Shoot resource to the Garden Cluster. The Gardener picks it up and starts a Terraform job to create the necessary IaaS components. Then it deploys the Shoot Cluster Control Plane into the Seed Cluster and required add-ons into the Shoot Cluster. Update or delete operations are handled by the Gardener fully automatically as well.
SCP
IaaS
Seed Cluster
Seed Cluster API LB
Shoot Cluster API LB
Seed Cluster Control Plane
Storage
[K8s] DS, RS, SS, J, ...
[CRD] Machine Deployment
Worker
Kubelet + Container Runtime
etcd Main Backup SS
Main PV
etcd Events SS
Events PV
API Server VPN D
Scheduler D
Controller Manager D
Addon Manager D
Machine Controller D
Terraformer J
Shoot Cluster Control Plane
Monitoring VPN
Logging
IaaS
Shoot Cluster
Shoot Cluster VPN LB
Kubelet + Container Runtime
VPN D
Calico DS
Kube Proxy DS
Kube DNS D
Optional Addons
Actual Workload

An Analogy …

The shoot cluster is like your apartment, you get full access to it and can do what you want.

The seed cluster is like an apartment building with a master key to all apartments within.

The Garden cluster is the apartment company with full access to all apartment buildings.

Challenges

You are about to invite guests into your apartment but you don’t want them to enter your private bedroom or open your safe.

You need to ensure that your neighbors don’t penetrate or sneak stuff from your apartment.

You don’t want apartment tenants or guests to get control of the apartment building (which would provide them with full access to all apartments).

Somebody who could take over the apartment company can do everything.

KubeCon

CloudNativeCon

China 2018

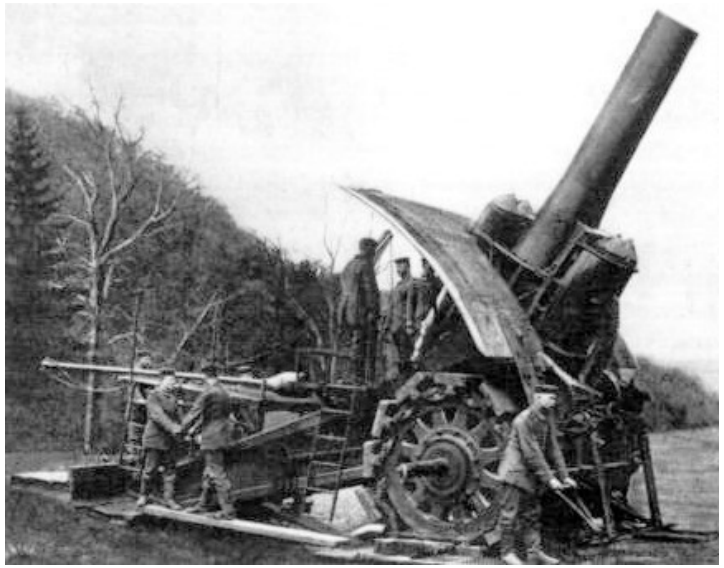
Warm up: The “Traditional” Approach

Warm-up

We have asked our established pen-testers to attack the Gardener setup.

They unpacked the big guns like Rapid7…

… however they openly admitted not to have Kubernetes know-how



(Wikipedia)

Results

This is what they found:

- Shoot cluster can be breached
  - Hey, its your own place, you are perfectly entitled to do that
- Other minor issues

So, are we safe?

KubeCon | CloudNativeCon

China 2018

The Race: A Second Opinion

A Second Opinion …

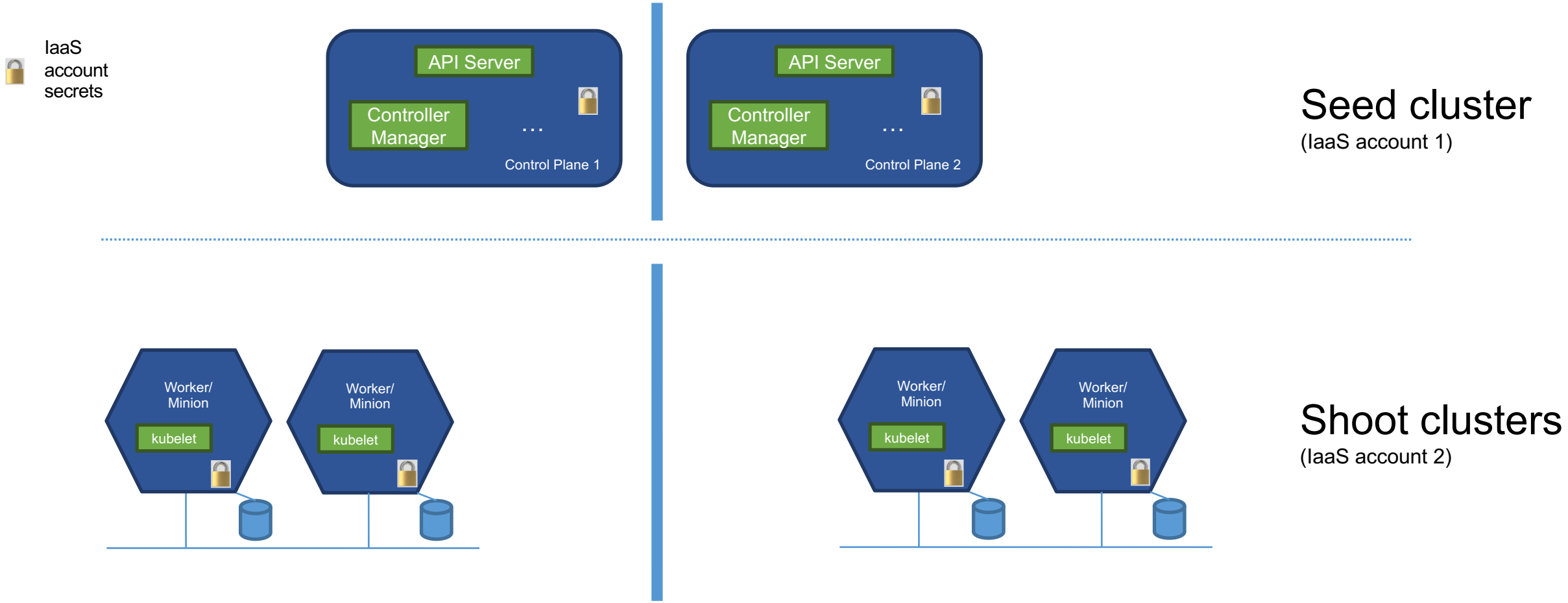
This was too easy. With the Kubernetes expertise from Alban and Michael from Kinvolk, we performed penetration tests.

They came in with filigree tools to try and breach the apartment, apartment building, building company.

Here is what they found …

#1 Shared Account: Full Access to your Neighbour's Appartment

(1) IaaS account secrets on worker nodes

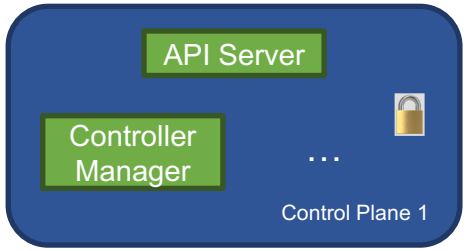


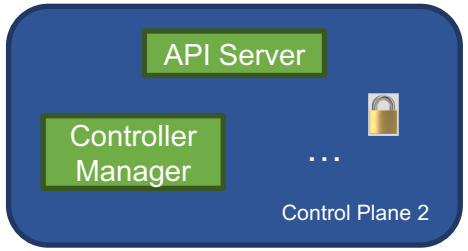
#2 Shared Account: Sneak Stuff out of your Neighbour's Apartment

(2) Tell your controller manager to do things on your behalf

(it has got the account credentials)

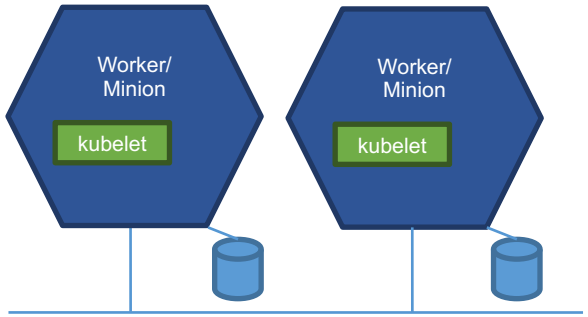
IaaS account secrets

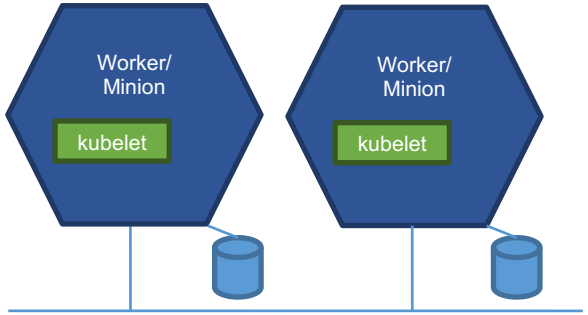




Seed cluster

(IaaS account 1)





Shoot clusters

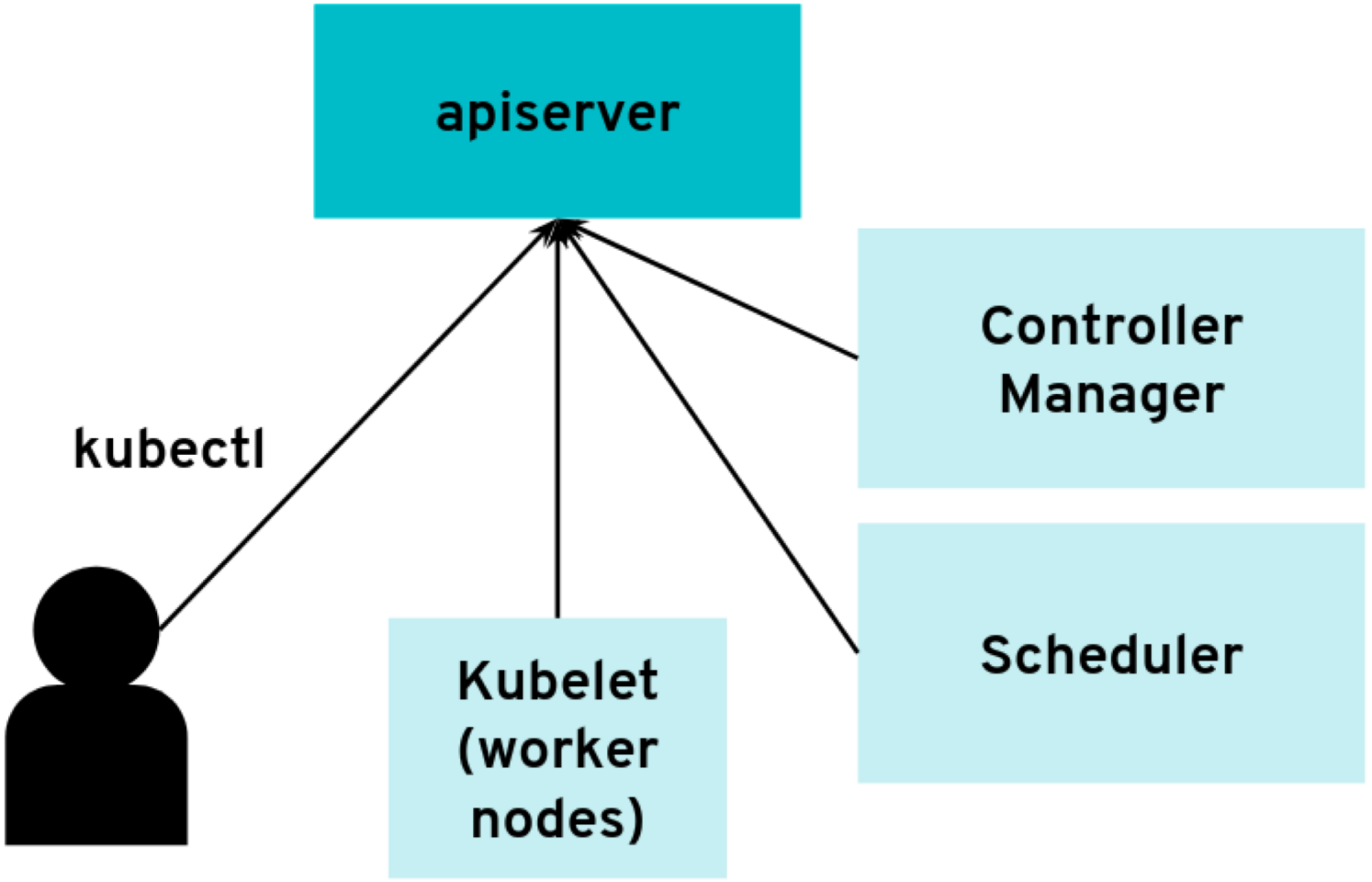
(IaaS account 2)

#1 + #2 General recommendations

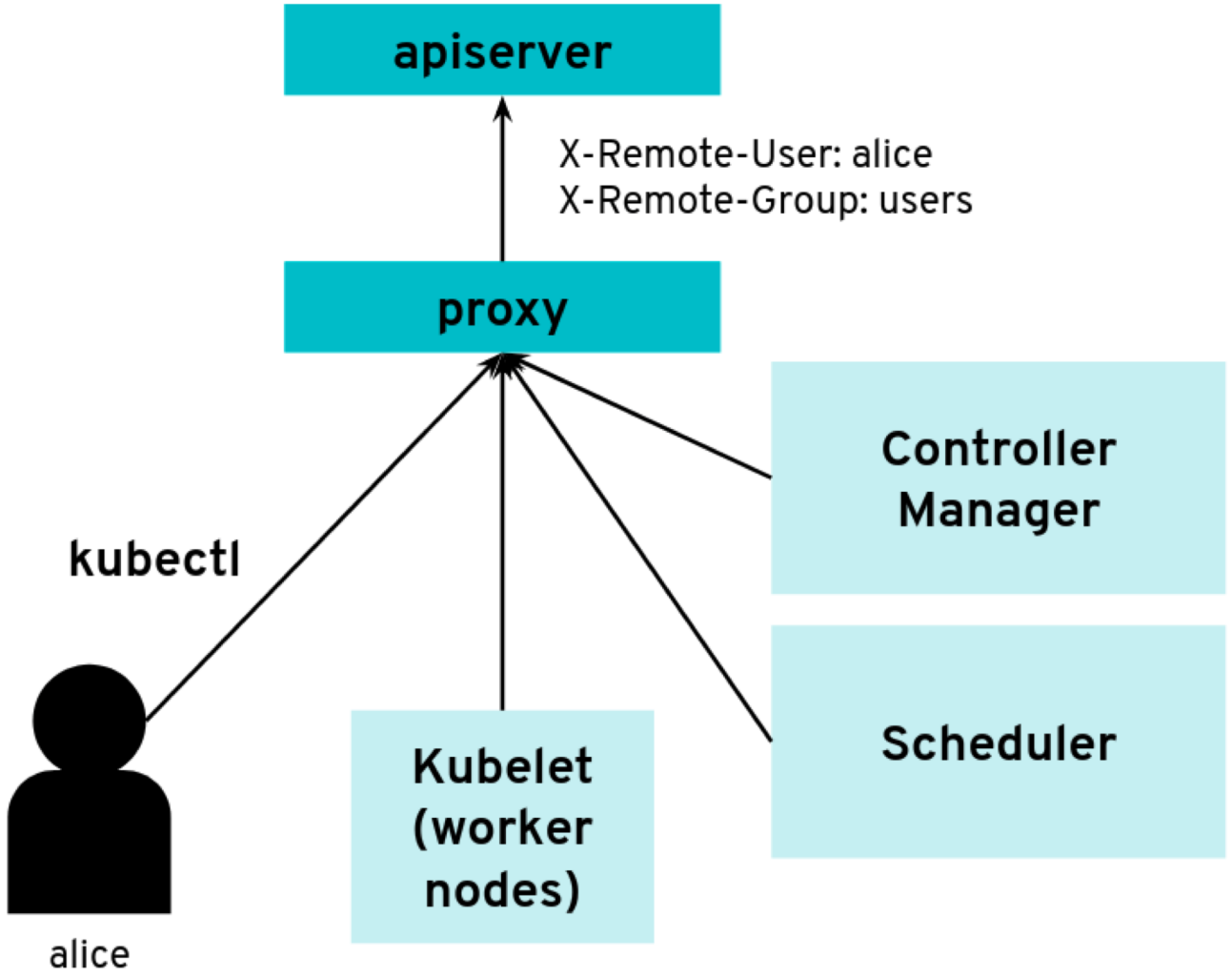
(1) Do not store account credentials on the worker nodes.
(2) You can add an Admission Webhook to protect apartments from each other.

However, be warned that depending on the IaaS provider there are most likely more attack vectors!

#3 Privilege Escalation



#3 Authenticating Proxy

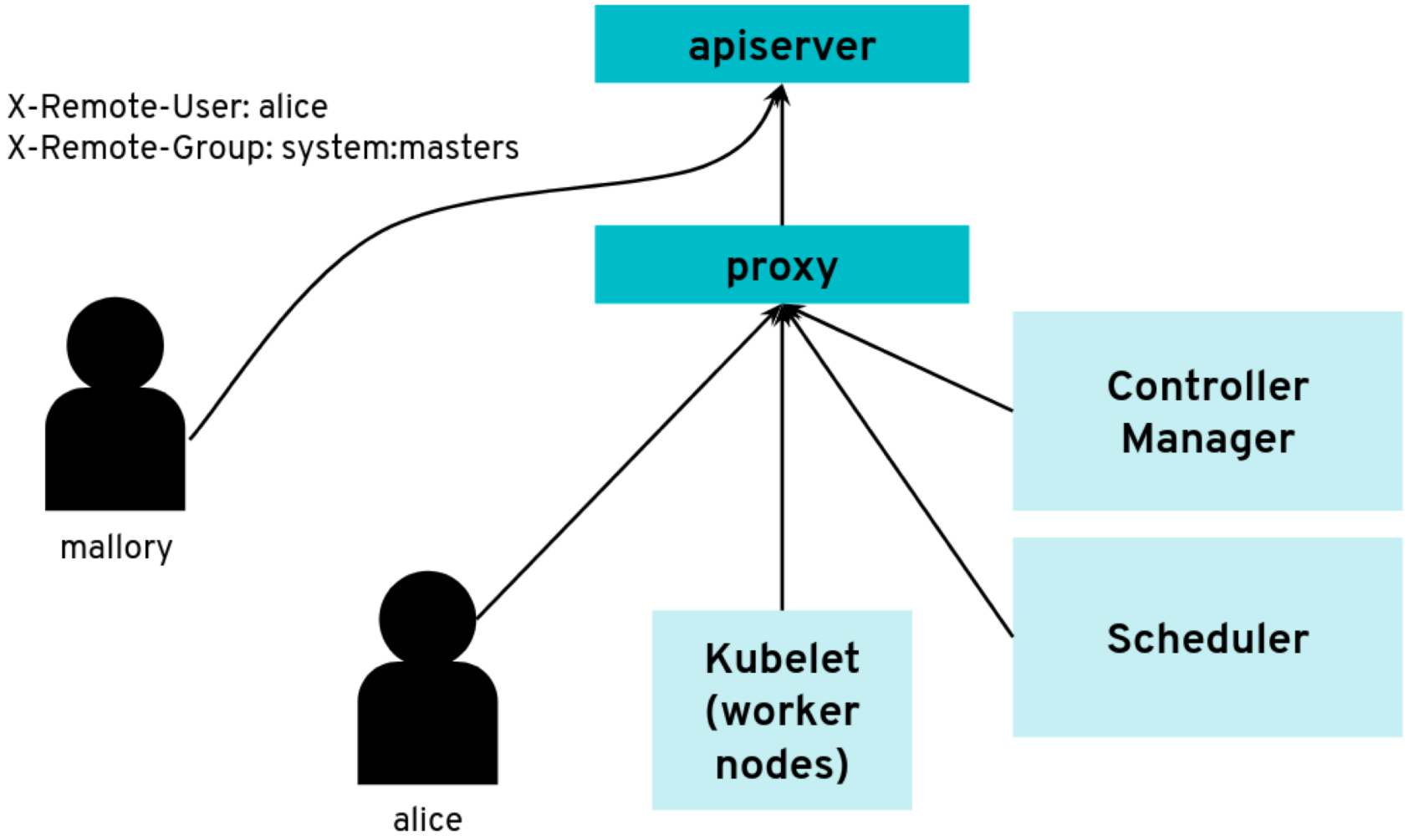


#3 Bad Proxy Configuration

Configuring the apiserver to accept requests from proxy:

--requestheader-client-ca-file=/srv/kubernetes/ca/ca.crt
--requestheader-username-headers=X-Remote-User
--requestheader-group-headers=X-Remote-Group

#3 Proxy CA Certificate



#3 The Exploit

By setting the HTTP headers, it is possible to impersonate another user and gain their privileges

#3 The Fixes

Using different CA in the apiserver configuration:

--client-ca-file=/srv/kubernetes/ca/ca.crt

--requestheader-client-ca-file=/srv/kubernetes/ca-front-proxy/ca.crt

Kubernetes already had a warning in the documentation, which we improved:
https://github.com/kubernetes/website/pull/10093

Metadata Service

Cloud providers provide a metadata service on all instances
- AWS, GCP, Azure: 169.254.169.154
- AliCloud: 100.100.100.200

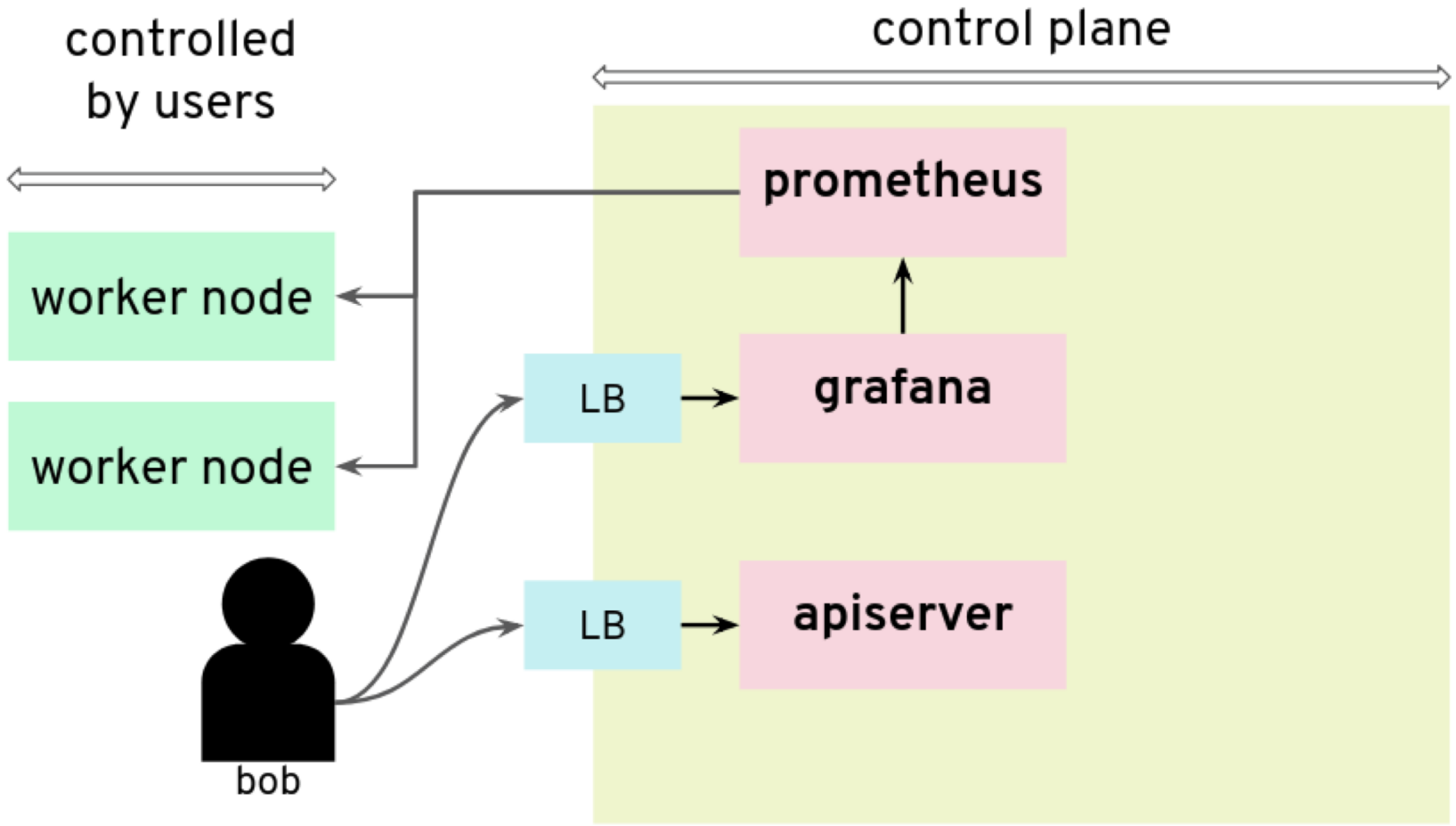
It contains bootstrap information, including a kubeconfig.
It can contain credentials to talk the the cloud provider API.

#4 Attack via Grafana

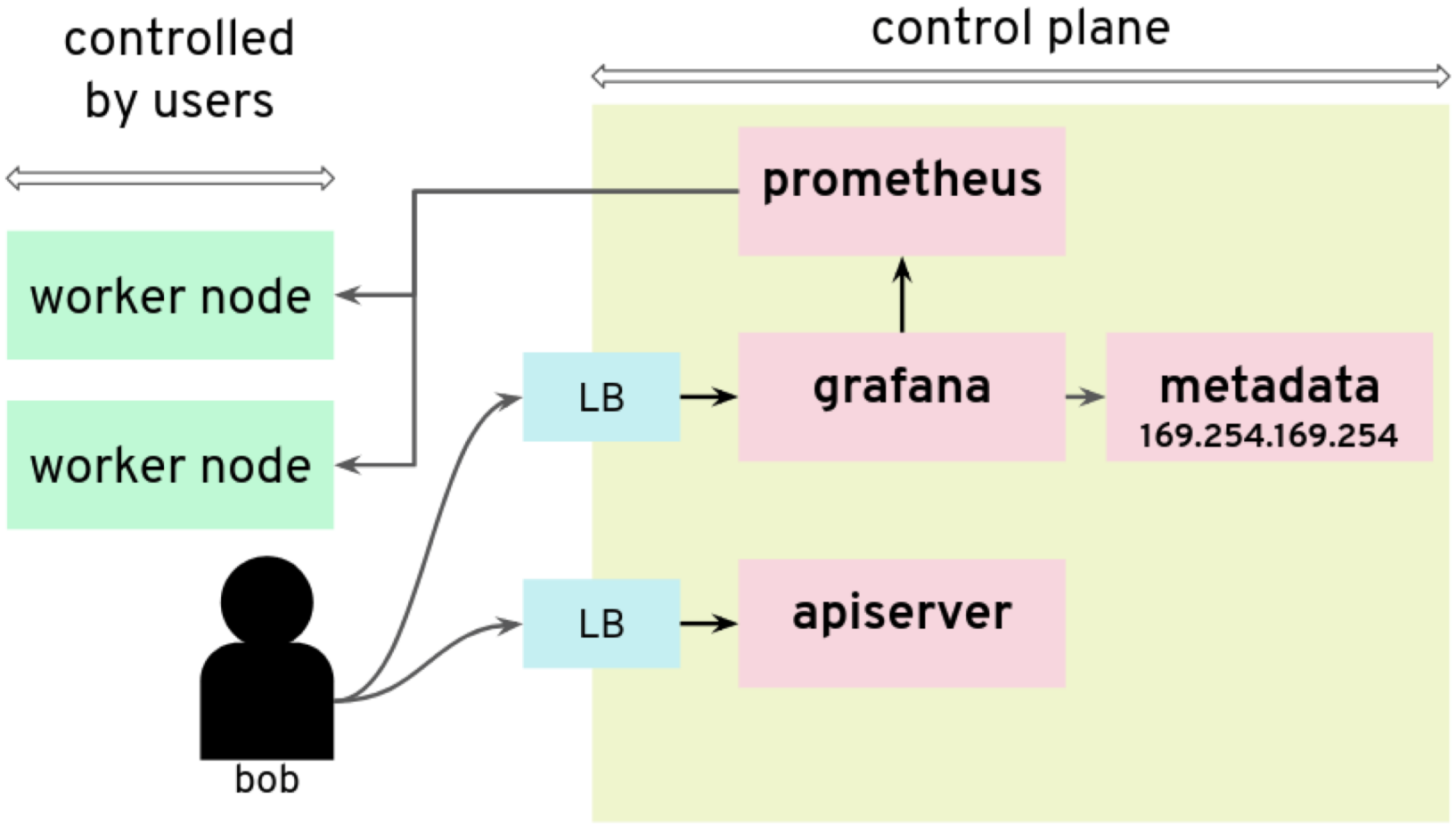
Grafana

- Grafana was offered as a service to users of the shoot cluster
- It lives in the control plane: another possible attack surface to explore

#4 Architecture with Grafana

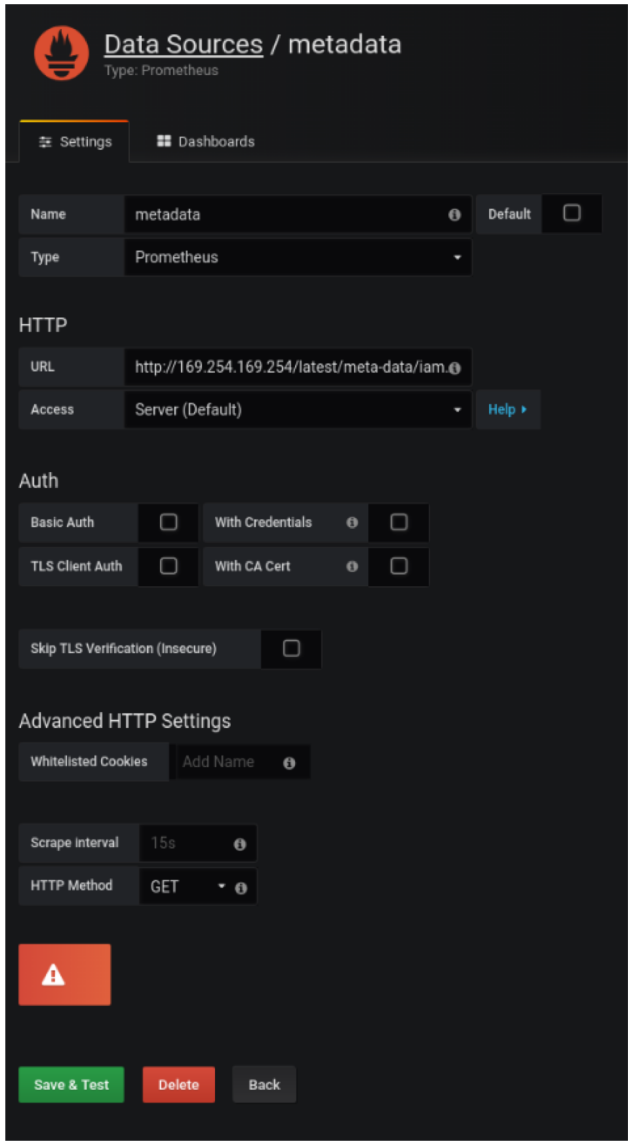


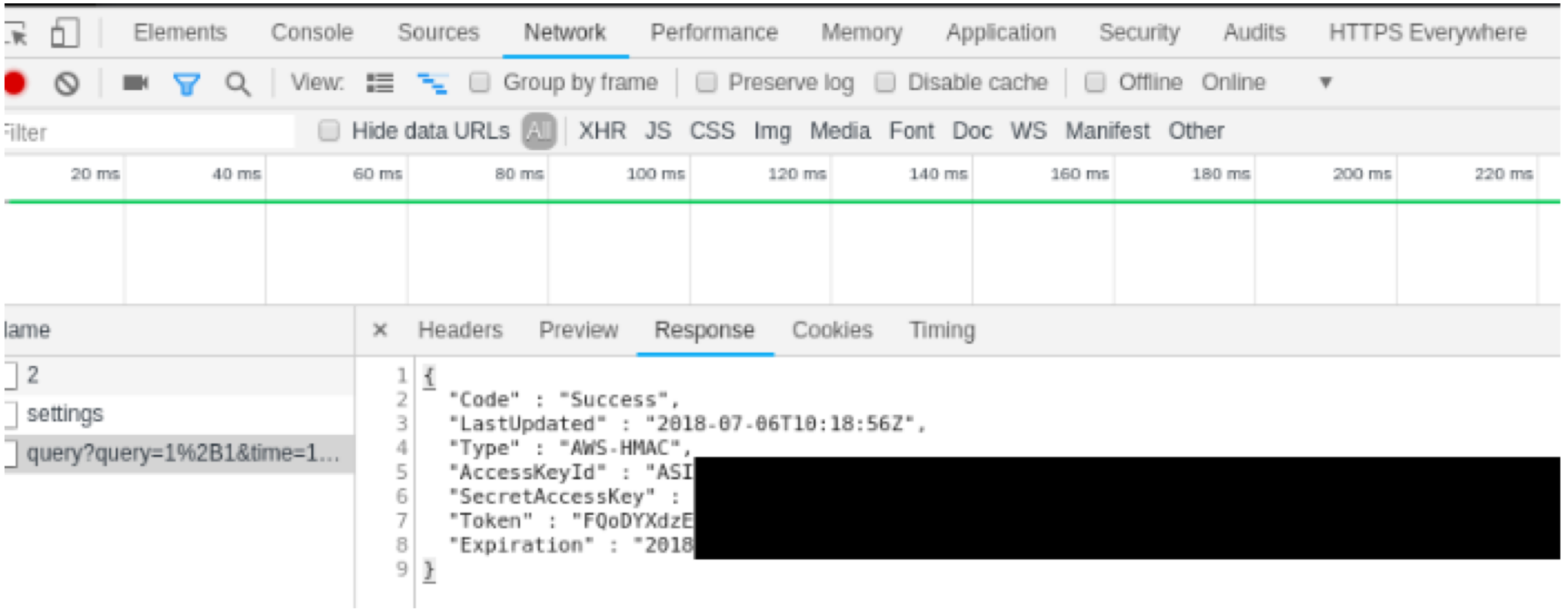
#4 Use Grafana for Metadata Access



#4 Use Grafana for Metadata Access

KubeCon | CloudNativeCon China 2018



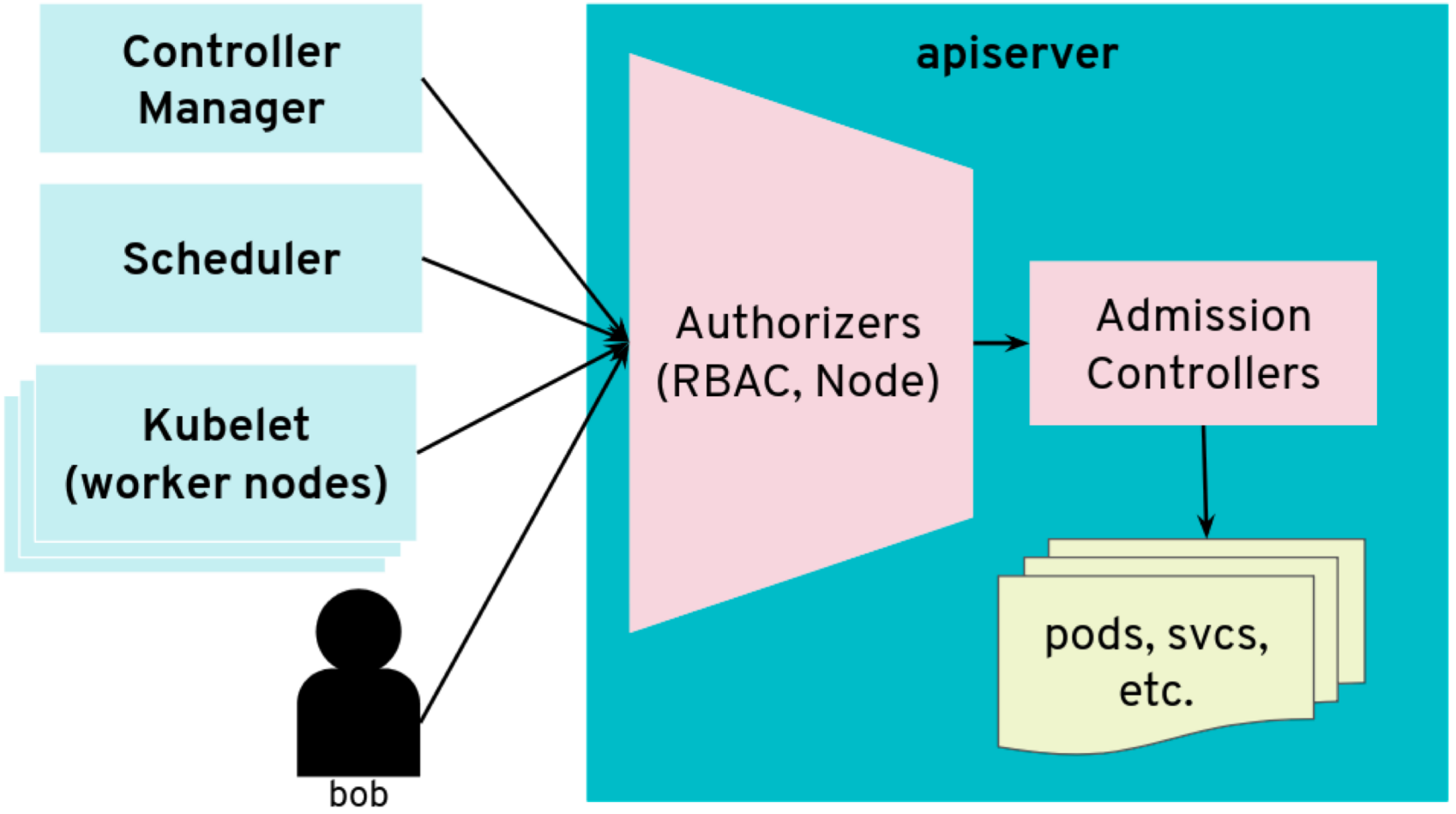


#4 General recommendation

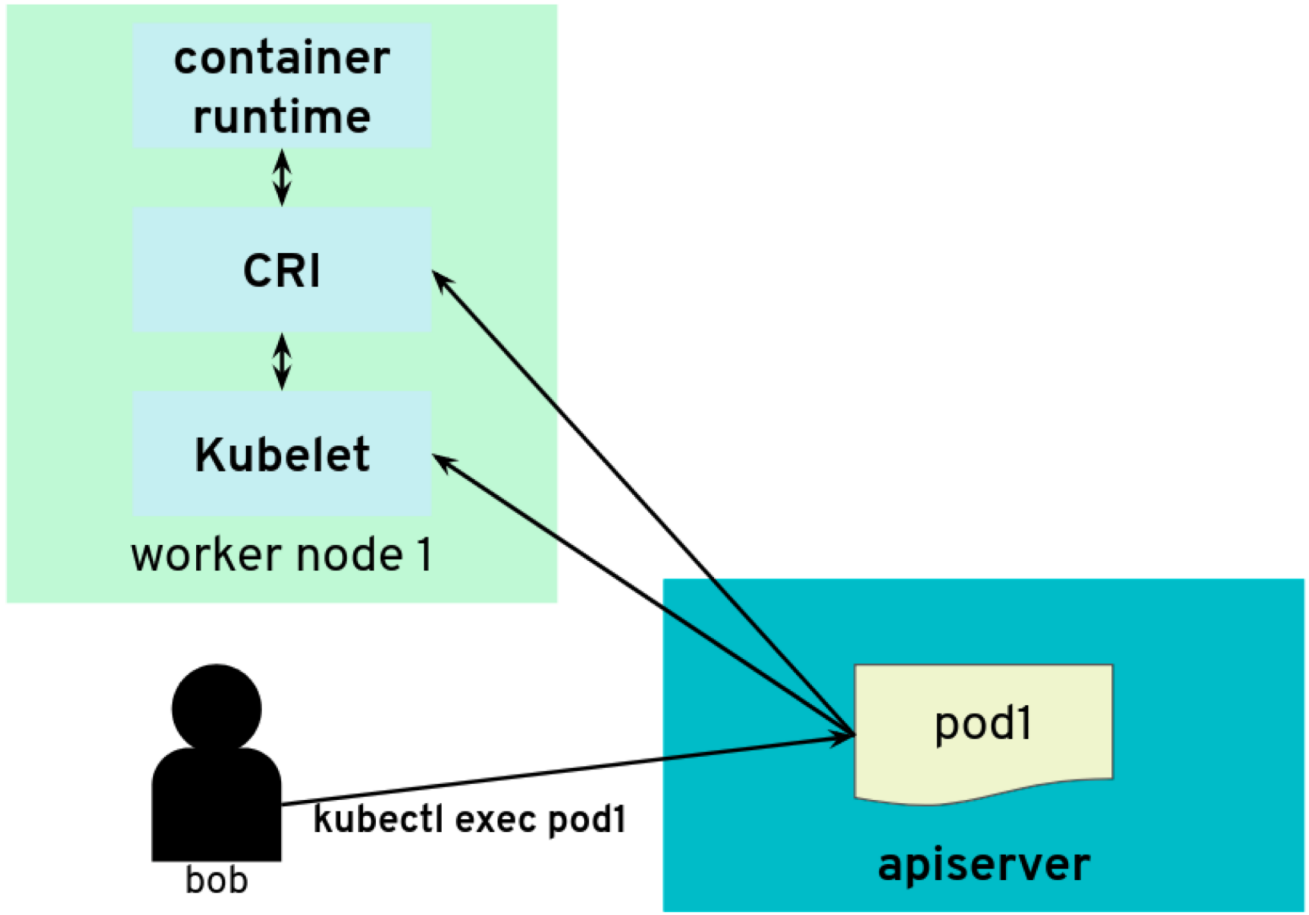
Mind which endpoints Grafana has access to

Use network policies in the control plane to block unnecessary access

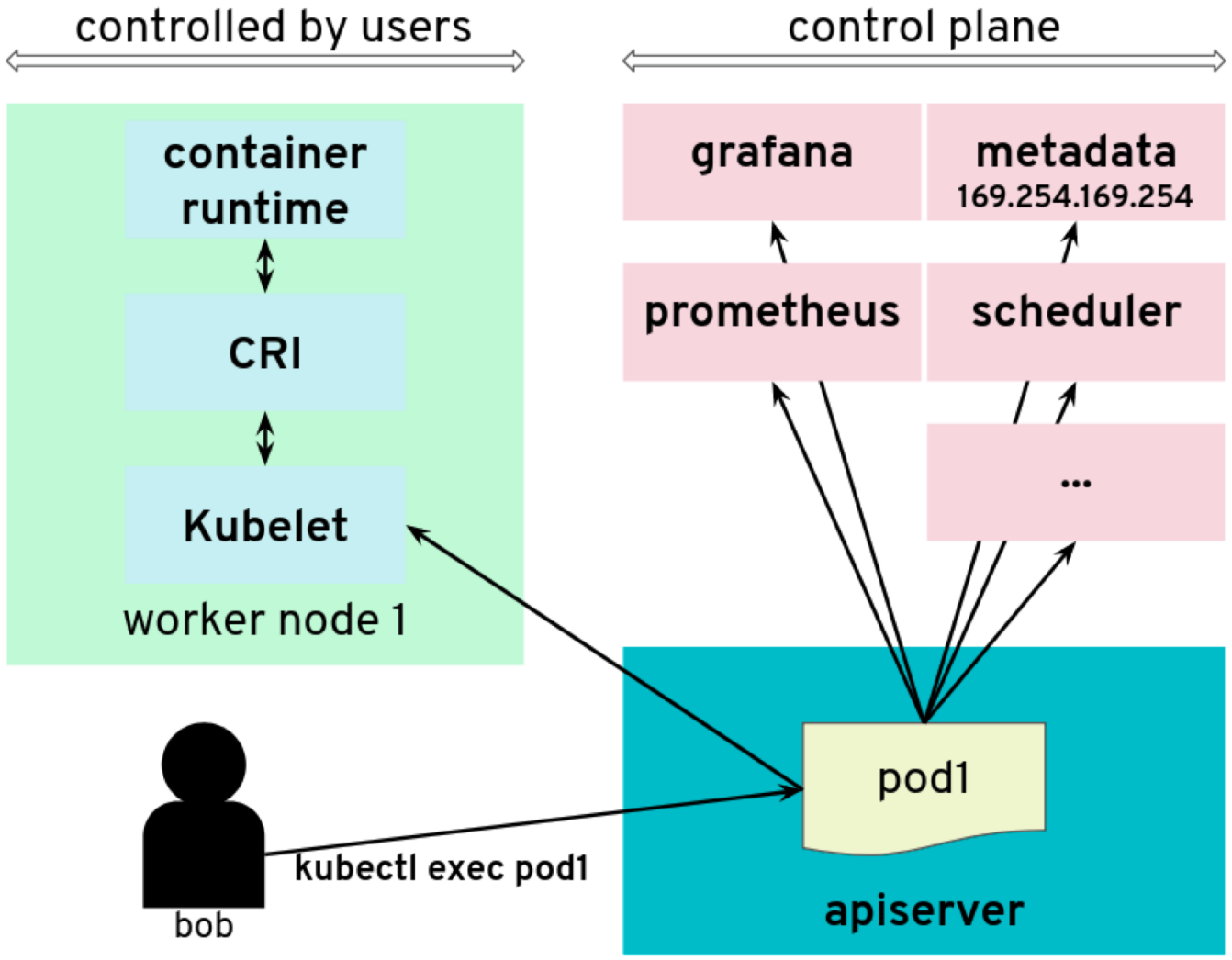
#5 Malicious HTTP Redirects



#5 Malicious HTTP Redirects



#5 Malicious HTTP Redirects



#5 Malicious HTTP Redirects

Kubernetes fix:
- add feature gate “ValidateProxyRedirects”
- https://github.com/kubernetes/kubernetes/pull/66516

Gardener fix: CVE-2018-2475
- Additional network policies were introduced in the latest version
- Please update

KubeCon | CloudNativeCon

China 2018

Cool Down:
Security Add-On Project

Motivation & Goals

- Our apartment owners (cluster owners) have a hard time to secure their own places.
- In general there are free and commercial tools that help secure clusters.
- We can however protect against some common configuration mistakes and enforce best practices.
- We will enforce certain restrictions for apartments owners but will also allow them to loosen them in case they are too tight (“keep some doors unlocked”).
- Keep it simple.
- Part of Gardener but will work with conformant Kubernetes clusters.

Planned Features

- Block access to the metadata service for all pods.
- Disallow root containers and privileged containers, and privilege escalation.
- Deny hostPath, hostNetwork, hostPID, hostIPC, hostPorts
- Enable seccomp and AppArmor profiles by default
- Disable service account tokens in pods
- Restrict repositories from where images can be pulled (ImagePolicyWebhook admission controller)

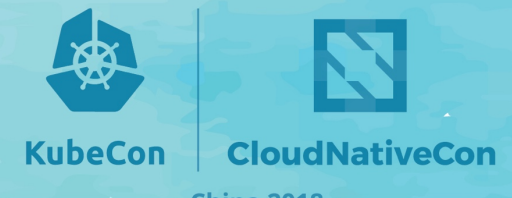
…

KubeCon | CloudNativeCon

China 2018

Conclusion & Outlook

Summary and Recommendations



Securing a Kubernetes Cluster Setup is hard.

The “**shared account**” model is quite **dangerous** and difficult to secure if you provide your customers with cluster-admin access.

Cluster owners are application developers who in many cases **lack the in-depth knowledge** on how to secure a Kubernetes cluster.

Make sure your pen-testers are specialized in Kubernetes to validate your cluster and application setup.

Thank You

References

Project Gardener: https://gardener.cloud/

GitHub: https://github.com/gardener

Gardener Blog: https://kubernetes.io/blog/2018/05/17/gardener/

Gardener CNCF Presentation:
https://www.youtube.com/watch?v=DpFTcTnBxbM

Kinvolk: https://kinvolk.io

KubeCon | CloudNativeCon

China 2018