
KubeCon
CloudNativeCon
OPEN SOURCE SUMMIT
China 2023


KubeCon | CloudNativeCon

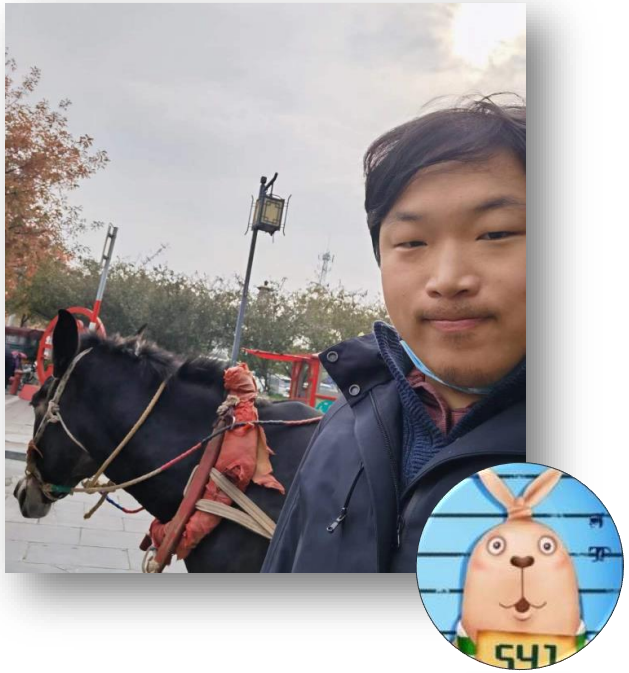
OPEN SOURCE SUMMIT

China 2023

SIG Cluster Lifecycle: What's new in Kubespray

Kay Yan

About me



Kay Yan

Github ID: yankay

Approver of Kubespray

Principal Engineer of DaoCloud

* Deploy Kubernetes is my Job, >500 various environment have been delivered in 7 years.

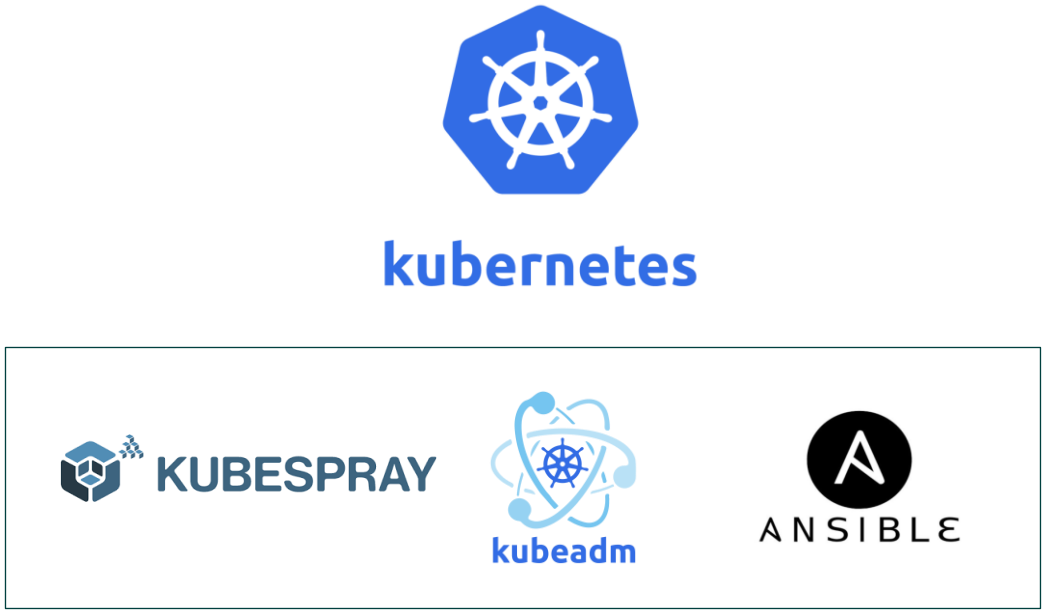
Agenda

1. What is Kubespray
2. Deep dive
3. Highlight new feature
4. Community

What is Kubespray

Kubespray is a sig-cluster-lifecyle's project to create, configure and manage kubernetes clusters.

Deploy a **Production Ready Kubernetes Cluster** with **Ansible**.



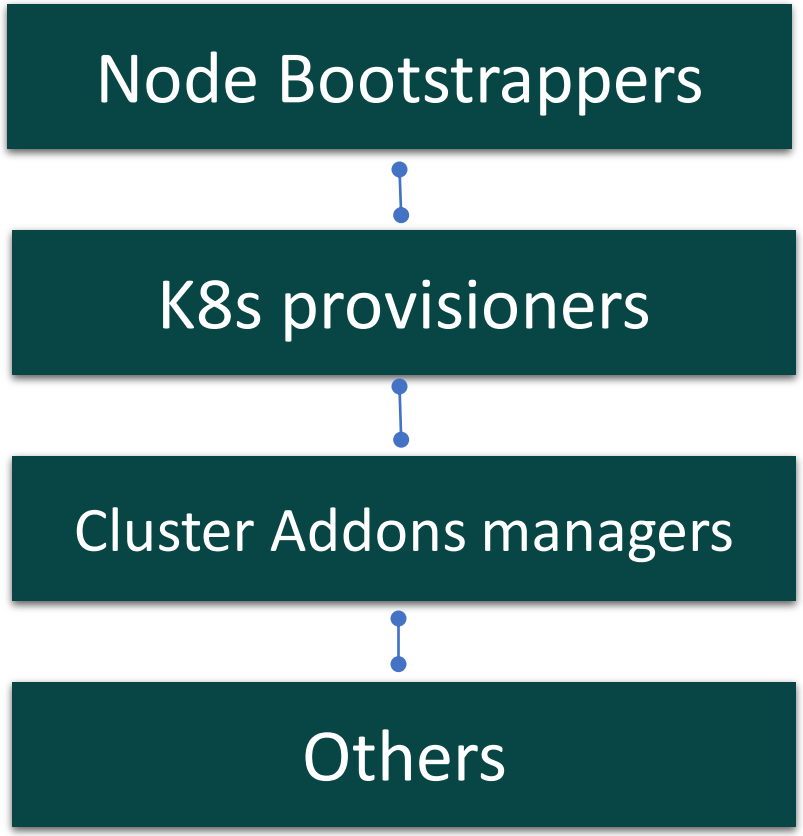
The Stack of SIG Cluster Lifecycle

kubeadm

kops, kubespray

cluster-addons

minikube, etcdadm



cluster-api
cluster-api-providers*
cluster-api-operator

image-builder

(*) currently there are 12 cluster API providers hosted by the SIG: AWS, Azure, Cloudstack, DigitalOcean, GCP, IBM Cloud, kubemark, kubevirt, nested, OpenStack, Packet, VSphere

From: SIG Cluster Lifecycle Intro - Fabrizio Pandini, VMware & Cecile Robert-Michon, Microsoft – Kubecon 2022

Features at Glance

- Can be deployed **Cloud or Baremetal** Infrastructure
- **Highly available** cluster
- **Composable** (Choice of the network plugin for instance)
- Supports most popular **Linux distributions**
- **Continuous integration tests**

Kubespray is like a mother taking care of the clusters everywhere, and do **a lot of work** for it.

Options can choose

Cloud	Supported Linux	CRI	CNI	CSI	Others
AWS	Flatcar Container Linux	Containerd	Calico	cephfs-provisioner	Coredns
Google Cloud	Ubuntu 20.04, 22.04	Docker *	Cilium	rbd-provisioner	Metallb
Equinix	CentOS/RHEL/Oracle 7, 8, 9 Alma/Rocky Linux 8, 9	CRI-O	cni-plugins (MacVlan…)	aws-ebs-csi-plugin	Ingress-nginx
HuaweiCloud	Fedora 37, 38; CoreOS	Crun	Multus	azure-csi-plugin	Kube-vip
Upcloud	Debian 10,11,12	Gvisor	Flannel	cinder-csi-plugin	Cert-manager
Vsphere	Kylin V10	Kata	Cannel	gcp-pd-csi-plugin	Argocd
Openstack	OpenSUSE Leap 15.x/Tumbleweed	Youki	Weave	local-path-provisioner	Registry
Hetzner	Amazon Linux 2		Kube-OVN	local-volume- provisioner	Helm
Nifcloud	UOS Linux ; openEuler		Customize		

The Voltron moment

There are many projects in Kubespray.
Users can choose their own mix and also plug-in custom components if they want.

Batteries included, but swappable

(*) Timothy St. Clair, Introduction to SIG Cluster Lifecycle, KubeCon 2019, San Diego

Deployment workflow

1. Check ansible version
2. Gather facts
3. Bootstrap OS
4. Preinstall Steps (207 tasks)
5. Install Container Engine(all nodes)
6. Install kubelet and prepare the node(all nodes)
7. Install the control plane (kubeadm init)
8. Join to cluster(worker)
9. Install network plugin
10. Install Kubernetes apps

Lifecycle of cluster operations

- Support full lifecycle of cluster operations
  - New cluster
  - Upgrade cluster
  - Scale a cluster
  - Remove node
  - Reset cluster
- Backup and restore
  - etcd snapshots taken during upgrade

Long-term support in Kubespray

Kubernetes Support matrix

Kubespray	Kube Version (N-2)
master-branch	1.26 ~ **1.28**
2.23	1.25 ~ **1.27**
2.22	1.24 ~ **1.26**
2.21	1.23 ~ **1.25**

Release Cycle: A few weeks releases after the Kubernetes Release

The LCM EcoSystem Of the Kubernetes

BootStrap

Provisioner

Public Cloud

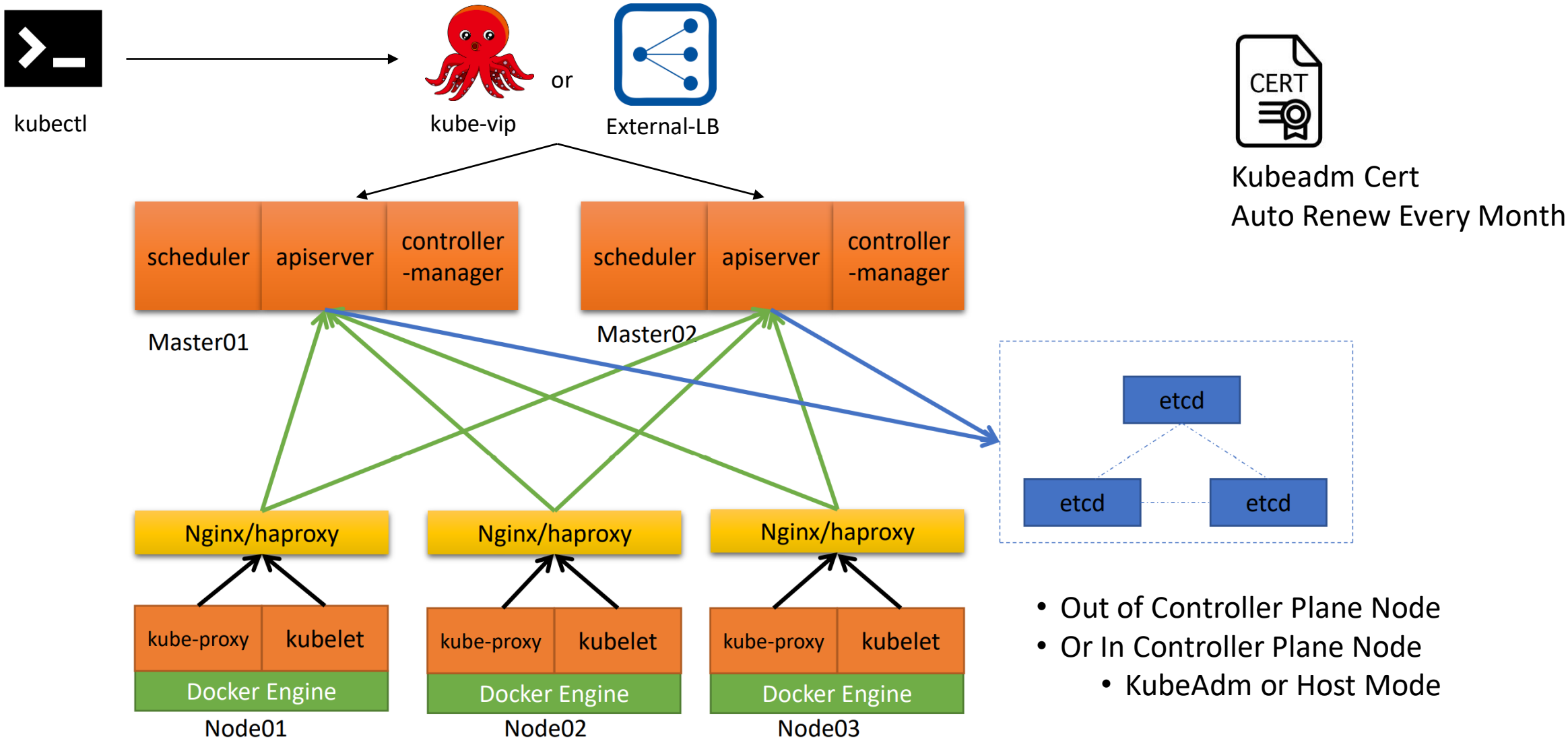
Developer

Commercial

Agenda

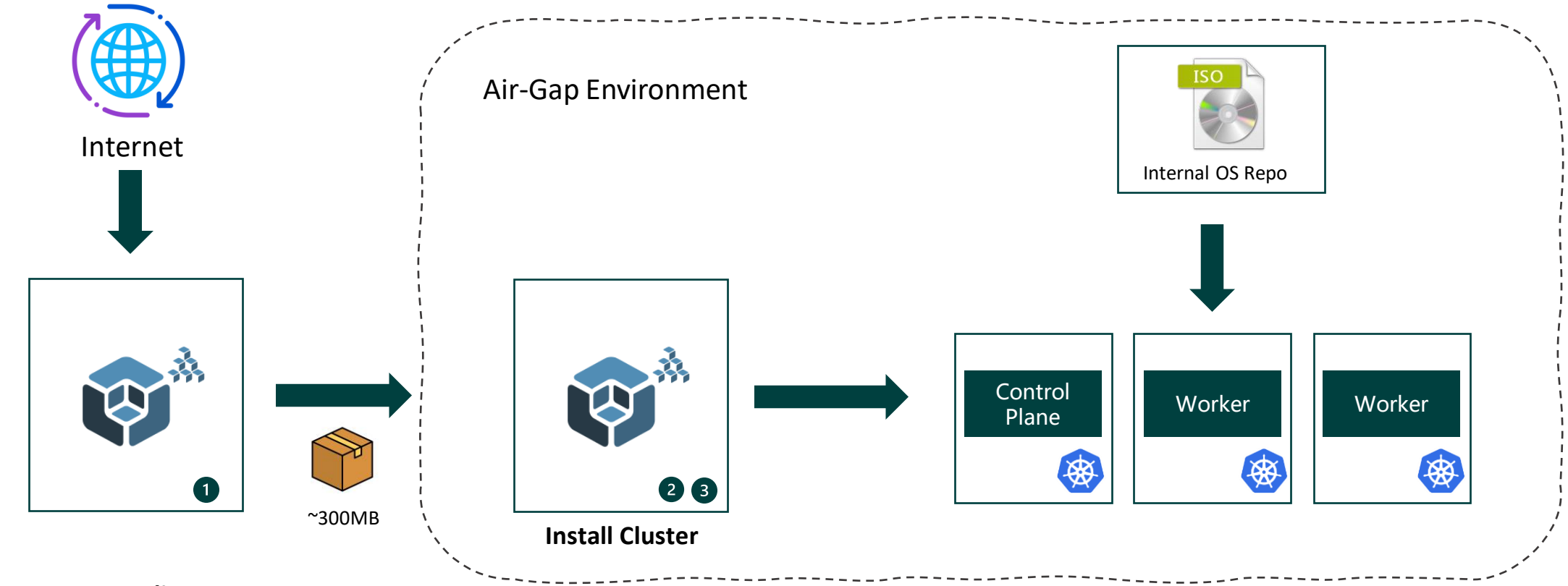
1. What is Kubespray
2. Deep dive
3. Highlight new feature
4. Community

High Availability



- Out of Controller Plane Node
- Or In Controller Plane Node
  - KubeAdm or Host Mode

Air-Gap Environment Deployment



1. **generate_list**
2. **manage-offline-files**
3. **manage-offline-container-images**

Docker-CE is a Special Case!

1. Not Support for Kubernetes in the Future.
2. Cray Dependency on Recent Version

Awesome CI Test

40+ test cases support:

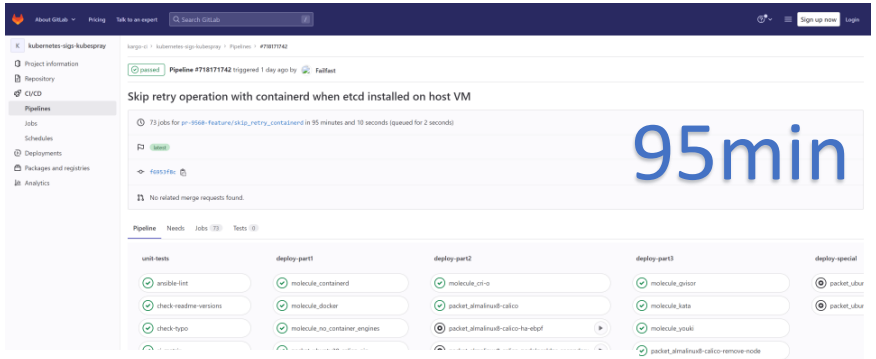
- 13 operating systems
- 8 network plugins
- 30+ environments

CI strategies:

- All-in-one
- Separate roles
- HA
- Upgrade

CI Tips:

- Multi stage test cases
- Only run specific when coding
- Full automated



CI test coverage

To generate this Matrix run `./tests/scripts/md-table/main.py`

containerd

OS / CNI	calico	cilium	custom_cni	flannel	kube-ovn	kube-router	macvlan	weave
almalinux8	✅	❌	❌	❌	✅	❌	❌	❌
amazon	✅	❌	❌	❌	❌	❌	❌	❌
centos7	✅	❌	❌	✅	❌	✅	❌	✅
debian10	✅	✅	❌	❌	❌	❌	✅	❌
debian11	✅	❌	✅	❌	❌	❌	❌	❌
debian12	✅	✅	❌	❌	❌	❌	❌	❌
fedora37	✅	❌	❌	❌	❌	✅	❌	❌
fedora38	❌	❌	❌	❌	✅	❌	❌	❌
opensuse	❌	❌	❌	❌	❌	❌	❌	❌
rockylinux8	✅	❌	❌	❌	❌	❌	❌	❌
rockylinux9	✅	✅	❌	❌	❌	❌	❌	❌
ubuntu20	✅	✅	❌	✅	❌	✅	❌	✅
ubuntu22	✅	❌	❌	❌	❌	❌	❌	❌

KubeVirt in Kubespray CI

1 Create the VM for test

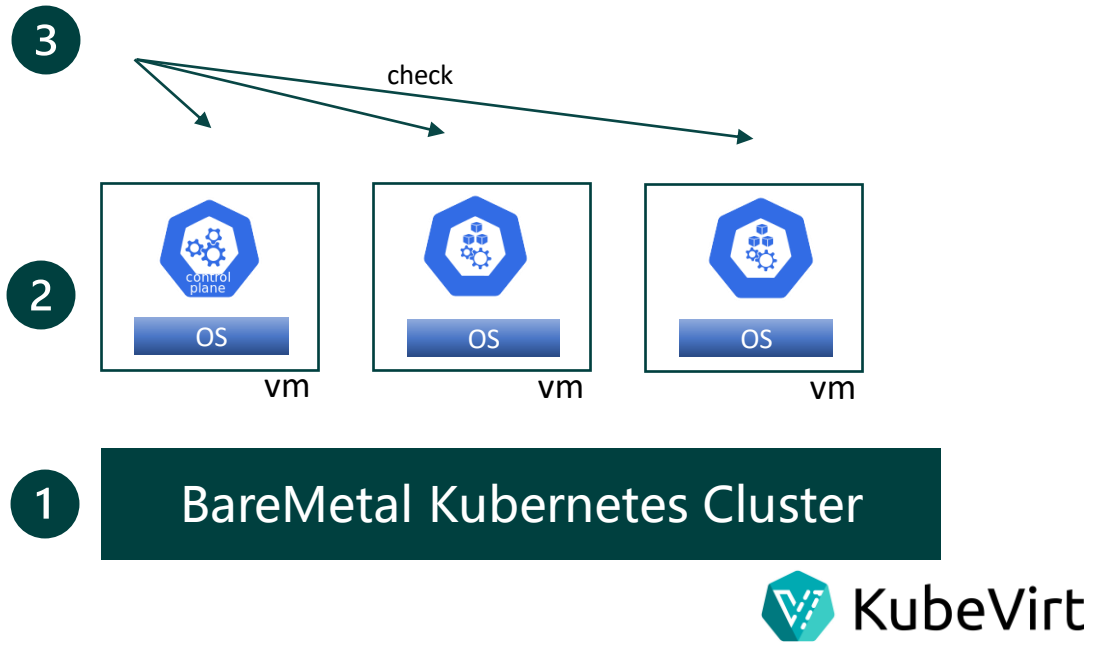
```
kubectl create namespace {{ test_name }}
kubectl apply -n {{ test_name }} vm.yaml
```

2 Deploy Cluster with Kubespray

```
ansible-playbook cluster.yml
```

3 Check Cluster is healthy

```
010_check-apiserver.yml
015_check-nodes-ready.yml
020_check-pods-running.yml
030_check-network.yml
040_check-network-adv.yml
100_check-k8s-conformance.yml
```



50+ VM created Pre PR

Agenda

1. What is Kubespray
2. Deep dive
3. Highlight new feature
4. Community

Options can choose

Cloud	Supported Linux	CRI	CNI	CSI	Others
AWS	Flatcar Container Linux	Containerd	Calico	cephfs-provisioner	Coredns
Google Cloud	Ubuntu 20.04, 22.04	Docker *	Cilium	rbd-provisioner	Metallb
Equinix	CentOS/RHEL/Oracle 7, 8, 9 Alma/Rocky Linux 8, 9	CRI-O	cni-plugins (MacVlan…)	aws-ebs-csi-plugin	Ingress-nginx
HuaweiCloud	Fedora 37, 38; CoreOS	Crun	Multus	azure-csi-plugin	Kube-vip
Upcloud	Debian 10,11,12	Gvisor	Flannel	cinder-csi-plugin	Cert-manager
Vsphere	Kylin V10	Kata	Cannel	gcp-pd-csi-plugin	Argocd
Openstack	OpenSUSE Leap 15.x/Tumbleweed	Youki	Weave	local-path-provisioner	Registry
Hetzner	Amazon Linux 2		Kube-OVN	local-volume-provisioner	Helm
Nifcloud	UOS Linux ; openEuler		Customize		

New Feature **in 2 years**

Operation System updated

New support:

- RHEL/Oracle/Alma/Rocky Linux 9
- Debian Bookworm
- Ubuntu 22.04
- Fedora 37, 38
- Kylin Linux Advanced Server V10
- UOS
- OpenEuler

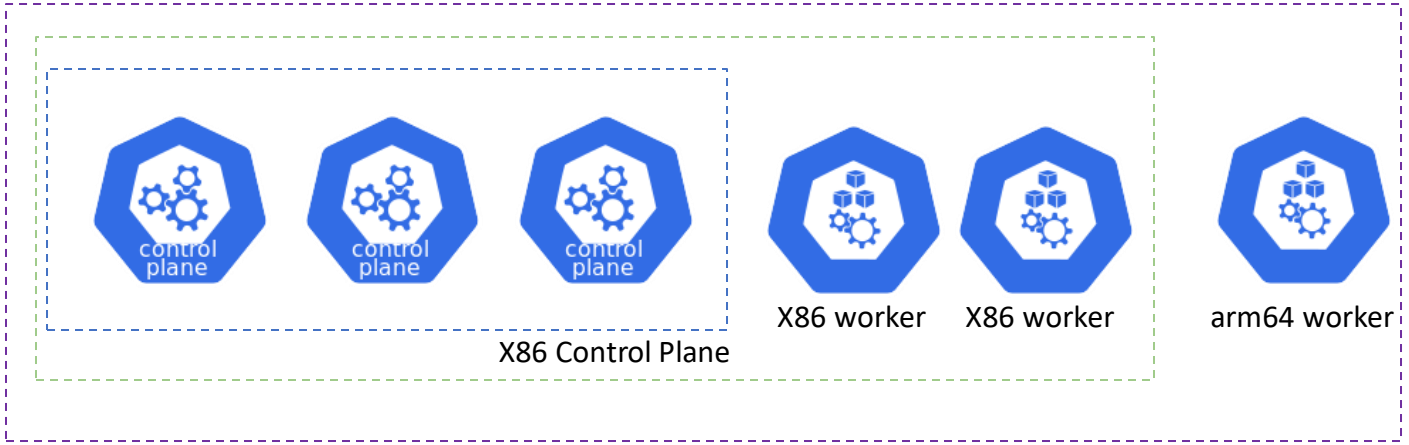
Drop support

- Debian Jessie, Stretch
- Ubuntu 16.04, 18.04
- Fedora 34, 35

Multi-Arch updated

Arch Support:

- x86
- arm64
- arm
- ppc64le （new）



New Features:

- Fully support Multi-Arch Image
- Multi-Arch Cluster(Experimental)

Deploy x86 & arm64 in One Cluster :

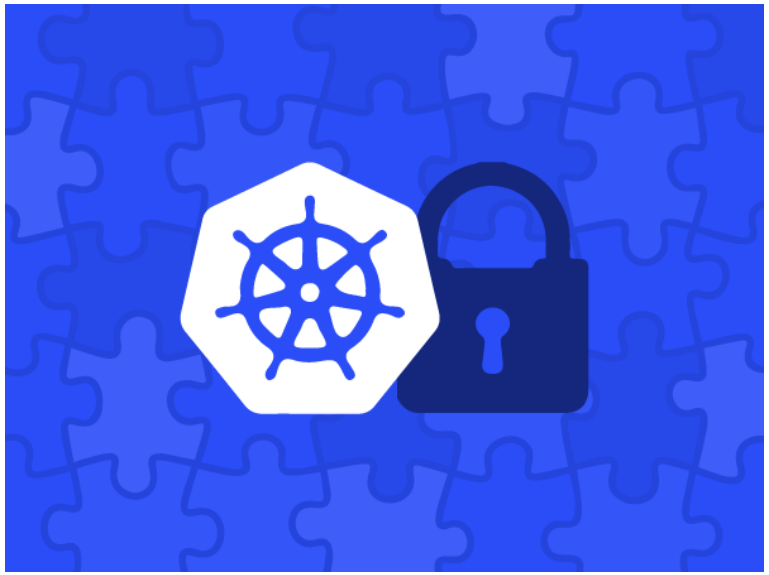
1. Deploy an x86 Cluster
2. Scale the cluster with arm64 nodes

Cluster Hardening

- Full support with config
- Cluster hardening Guide

```
## kube-apiserver
authorization_modes: ['Node', 'RBAC']
kube_apiserver_request_timeout: 120s
kube_apiserver_service_account_lookup: true

# enable kubernetes audit
kubernetes_audit: true
audit_log_path: "/var/log/kube-apiserver-
log.json"
audit_log_maxage: 30
audit_log_maxbackups: 10
audit_log_maxsize: 100
……
```



Best Practice: NTP & Sysctl

NTP

Time synchronization is very important for the Etcd and kubernetes.

```
ntp_enabled: true
ntp_timezone: Asia/Shanghai
ntp_manage_config: true
ntp_force_sync_immediately: true
```

Sysctl

- Required **kernel variables** has been configured by default.
- Support customize the additional variables for tunning

```
additional_sysctl:
 - { name: kernel.pid_max, value: 4194304 }
 - { name: net.netfilter.nf_conntrack_max, value: 1048576 }
 - { name: fs.inotify.max_user_watches, value: 65536 }
 - { name: fs.inotify.max_user_instances, value: 8192 }
```

Public Mirror to speed up deploy

KubeCon CloudNativeCon OPEN SOURCE SUMMIT China 2023

Challenge:

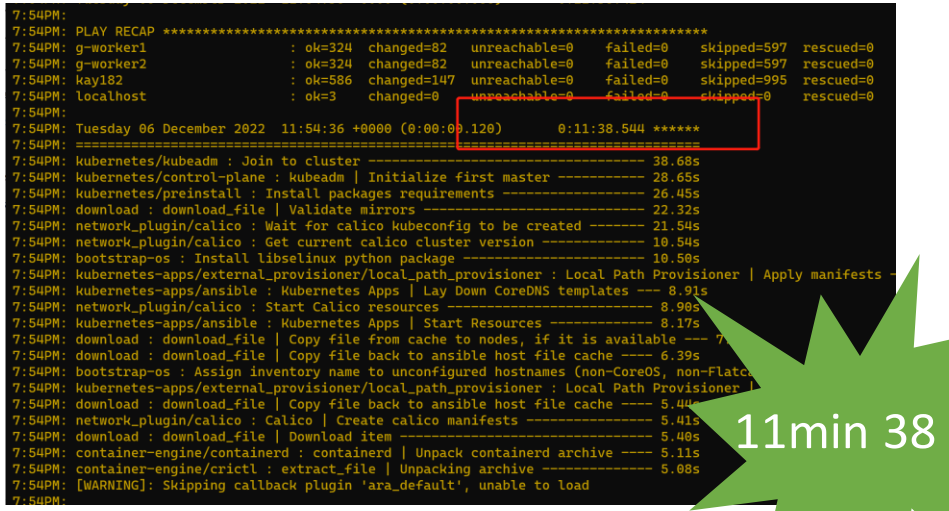
There needs **hours** to download **image and file**,
it makes kubespray not easy to use in some area.

Solution:

If you want to download quickly in China,
the configuration can be like:

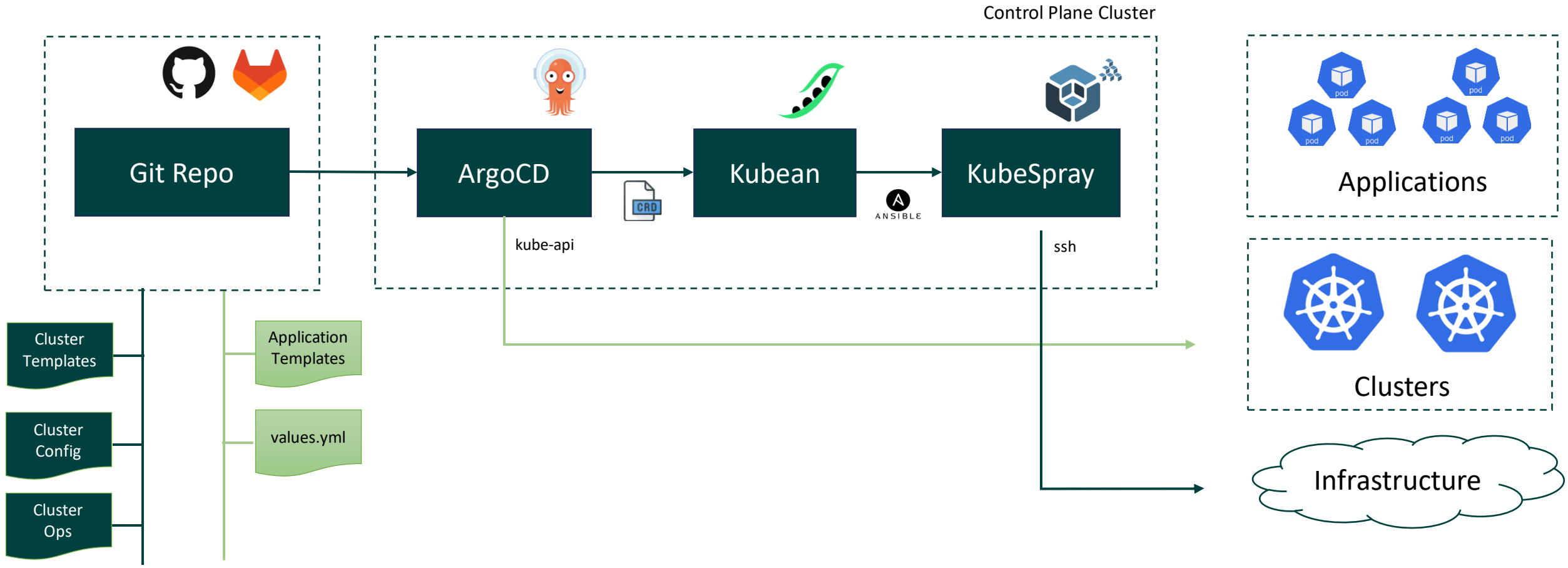
```
gcr_image_repo: "gcr.m.daocloud.io"
kube_image_repo: "k8s.m.daocloud.io"
docker_image_repo: "docker.m.daocloud.io"
quay_image_repo: "quay.m.daocloud.io"
github_image_repo: "ghcr.m.daocloud.io"
files_repo: "https://files.m.daocloud.io"
```

Use mirror sites only if you trust the provider. The Kubespray team
cannot verify their reliability or security.
You can replace the `m.daocloud.io` with any site you want.



The opensource project to provide mirror:
https://github.com/DaoCloud/public-image-mirror

Integrate with GitOps Solution



gitops ❤ KUBESPRAY

Agenda

1. What is Kubespray
2. Deep dive
3. Highlight new feature
4. Community

Thanks to Contributors

a Pure Bazaar Global Community

World Wide Popular !

1338 Developers
>50 in a release

7306 Commits

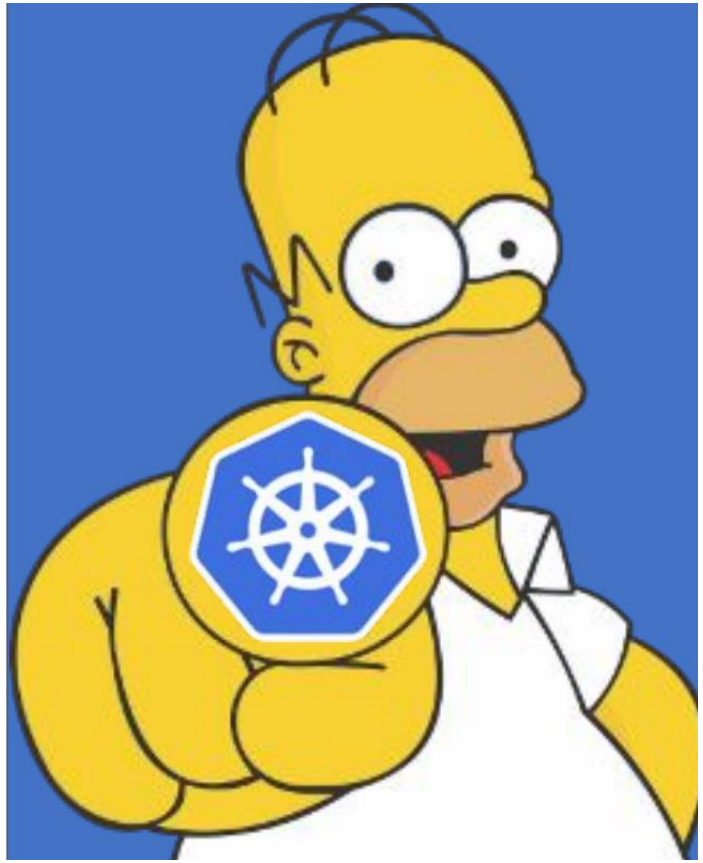
> 14k
Stars

> 3k
Issues

> 6k
PRs

> 6k
Forks

We need your help!



There is still a lot of work to do in order to get the full puzzle in place!

It can be changed the code easily because it's just shells!

slack #kubespray
#kubespray-dev

GitHub kubernetes-sigs/kubespray

WeChat QR code in Next Page.

Demo

If we have time.

Questions and Answers