



KubeCon



CloudNativeCon

North America 2021

RESILIENCE

REALIZED

Cloud Provider Extraction

What We've Done
Where We Are,
What's Left!

Walter Fender
Software Engineer
Google

Steven Wong
Software Engineer
VMware

Nicholas Turner
Software Engineer
Amazon

Abstract

Hidden during presentation – for benefit of post event downloaders and search engine indexers

Cloud Provider code allows Kubernetes to run on top of different platforms.

Originally, support for all variations was built directly into a K8s release. This brought bloat - a running cluster used only a subset of the code within the release. Also, any cloud specific bug fix or enhancement demanded a new full K8s release as a carrier.

This will be a status report on removing the cloud provider code from the main Kubernetes repository. Significant early milestones were recently achieved:

- the API Server no longer needs the cloud provider library;
- SSH Tunnels have been deleted.

For each in-tree cloud provider, we will report on efforts, accomplishments, and roadmap for getting "out-of-tree".

We'll also discuss the plans to handle the speed bumps that are left - including interesting topics like multi-repo e2e testing and removing the cluster directory.

Agenda

Cloud Provider – background

What is it? Motivation of the move out-of-tree

General Status Report

“Lightning Talks” from platform specific contributors

- efforts, accomplishments, roadmap

AWS, GCP, vSphere

Cloud Provider futures and interesting topics

How to join and track Cloud Provider SIG activity

Kubernetes Cloud Provider

What is it?

An abstraction layer for platforms that run Kubernetes

Mission:

Ensure that the Kubernetes ecosystem is evolving in a way that is *neutral to all* public and private cloud providers.

Responsible for establishing standards and requirements that must be met by all providers to ensure optimal integration with Kubernetes.

Simplify, develop, and maintain cloud provider integrations as extensions, or add-ons, to Kubernetes clusters

What is abstracted and managed? These are examples, varies by specific cloud platform

Compute: Node management, availability zones

Storage: Volumes

Network: Routes, IP address, load balancing

Why move out of tree?

monolithic in-tree issues

- Legacy cloud providers and storage plugins were built directly into the Kubernetes binaries
- Could not be patched or enhanced independent of a full Kubernetes release
- Resulted in undesirable bloat of Kubernetes itself – any particular deployment needs only a subset, yet irrelevant code is part of the release
- Runs as a privileged component of Kubernetes itself – security and stability risk
- Kubernetes should be an orchestration kernel, with drivers maintained independently by domain experts
- Inclusion can imply endorsement or support for a select set of providers

Cloud Provider Migration

General Status report

Cloud Provider Migration

General Status Update

Kube Controller Manager

- The node-lifecycle, service, and route controllers are disabled when `--cloud-provider=external`.
- Volume controllers (like attach/detach) no longer have access to cloud provider plugins when `--cloud-provider=external`.
 - If CSI is not enabled, then the cloud provider must be enabled for volume plugins only using `--external-cloud-volume-plugin=<cloud-provider-name>`

Cloud Controller Manager

- Vendor specific binary which runs cloud loops like: `cloud-node`, `cloud-node-lifecycle`, `cloud-node-ipam`, `cloud-route`, `cloud-service`.
- See the [KEP](#)

Cloud Provider Migration

General Status Update

API Server

- SSH Tunnels have been replaced by [the network proxy](#).
- Cloud provider code remains in the persistent volume labeling admission plugin.
 - [A KEP was merged in v1.23](#) that will enable webhooks to be built as replacements.

Cloud Provider Migration

General Status Update

Kubelet

- Node addresses were once expected to only be set by kubelet calling the cloud provider -- since 1.7 cloud providers can, like in the cloud-node-controller ([pull request](#)).
- The built-in kubelet image credential provider plugins will be replaced by external image credential providers.
 - In v1.23 the DisableKubeletCloudCredentialProviders feature gate was added ([pull request](#)).
 - See the [KEP](#).
- Kubelet in-tree volume plugins are being replaced by CSI.
 - When the CSI driver to replace a given in-tree plugin is installed, CSI migration can be enabled so that all new and existing volumes will be managed by the CSI driver.
 - See the [Docs](#) and [KEP](#).

Cloud Provider Migration

General Status Update

Leader Migration

- For HA clusters that cannot tolerate downtime, a leader migration feature was merged to facilitate migration to an external cloud controller manager.
- Beta in v1.22.
- See the [docs](#) and the [KEP](#).



“Lightning Talks”

Updates from platform specific cloud providers

Alphabetical order



KubeCon



CloudNativeCon

North America 2021

AWS Cloud Provider

Nick Turner



KubeCon



CloudNativeCon

Photo by Yarenci Hdz on Unsplash

AWS Cloud Provider

Status Update

Components

- AWS Cloud Controller Manager
- Kubelet Image Credential Provider for ECR
- CSI Drivers - [EBS](#), [EFS](#), [FSx](#)
- AWS Load Balancer Controller

AWS Cloud Provider

Status Update

What's New?

- AWS Cloud Controller Manager
 - Released [v1.22.0-alpha.0](#)
 - Bug fixes & Cherry picks.
 - New easy to use kops setup example.
- AWS Load Balancer Controller
 - Released [v2.2.0](#)
 - Added support for NLB instance mode.
 - NLB private IP address.
 - Simplified ssl-redirect for Ingress.
 - Ingress PathType.
 - Custom name for ALB/NLB.
 - Ability to filter nodes for instance targets.
- AWS EBS CSI Driver
 - Released v1.3.1
 - Push multi-arch/os image manifest to ECR.

AWS Cloud Provider

Status Update

Coming soon

- AWS Cloud Controller Manager
 - Improved upstream test framework, taking advantage of LKG testing proposal
 - Enabled on EKS
- AWS Load Balancer Controller
 - v2.3.0
 - Optimized security group rules
 - Use constant number of SG rules for allowing ALB traffic, number of ALB will not be dependent on the SG quotas
 - IPv6 target support for ALB (ip targets only)
 - Support EndpointSlices
- CSI
 - CSI migration on EKS
- Kubelet Image Credential Provider
 - First release binaries and documentation

AWS Cloud Provider

Status Update

Feature	1.20	1.21	1.22	1.23	1.24	1.25
HA Migration framework		alpha	beta	GA		
Credential Provider Framework	alpha			beta	GA	
AWS ECR Credential Provider	alpha			beta	GA	
AWS Cloud Controller Manager	alpha		beta	GA		



CLOUD PROVIDER AZURE

updates & highlights from Pengfei & Andy in Shanghai

Recently...

- CSI migration for Azure Disk & File CSI drivers (the first in-tree driver turned on by default with the CSI migration feature in k8s 1.23)
- Out-of-tree cloud-provider-azure GA in k8s 1.21+ (preview in AKS)
- Out-of-tree patch releases have been accelerated compared to k/k in-tree (now with on-demand releases as needed)
- azuredisk/azurefile CSI drivers GA in k8s 1.21+ & AKS



Pengfei Ni
feiskyer

What's next? External ACR credential provider plugin, ARM64 support, prefixed cloud provider managed tags, and more.

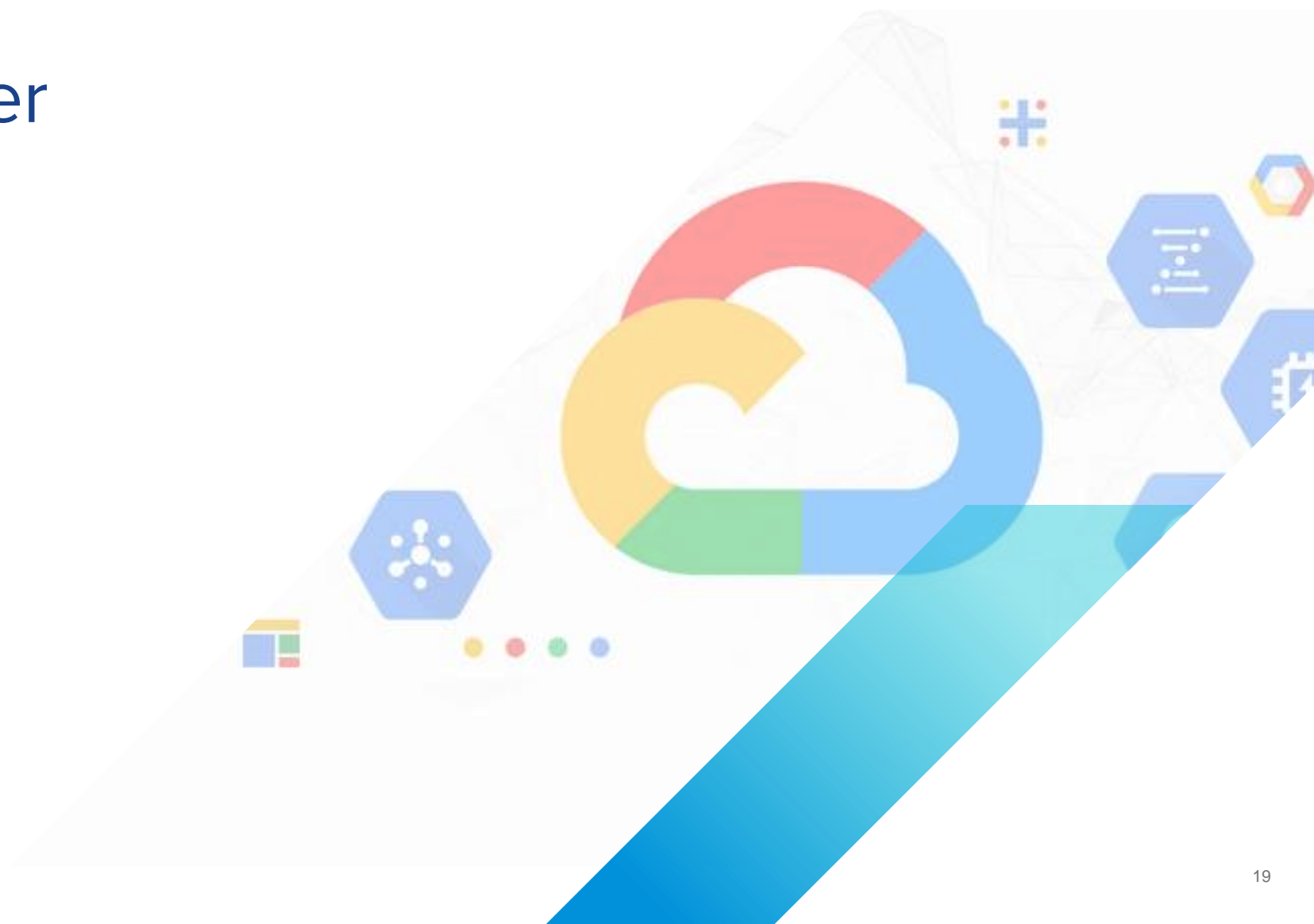
<https://kubernetes-sigs.github.io/cloud-provider-azure/>



Andy Zhang
andyzhangx

GCP Cloud Provider

Walter Fender - Google



KubeCon



CloudNativeCon

North America 2021

GCP Cloud Provider - What We've Done

One of the first Kubernetes implementations and one of the largest investments.

- Many features are only tested on GCP
 - Node tests
 - Scalability tests
 - Networking tests
 - API Machinery tests
 - Storage tests
- More GCP specific code in K/K than any other cloud provider
 - Code such as SSHTunnel was just for GCP
 - SSHTunnels has finally been removed!!!
 - GCP specific control code, eg NodelpamController
- More to extract to get out
 - CCM
 - APIServer Network Proxy
 - CSI
 - Credential Provider

GCP Cloud Provider - Where We Are

Reference Implementation: <https://github.com/kubernetes/cloud-provider-gcp>

Status: Cloud Controller Manager with NodePamController ☒

Credential Provider ☒ (Not yet default)

Windows Nodes ☒

APIServer Network Proxy ☒

CSI - Coming soon

Automatic conformance testing ☒

Automatic e2e testing ☒

But let's take a look

File Edit View Search Insert Help

ion, see: <https://developers.google.com/compute/docs/disks#performance>.

Created [https://www.googleapis.com/compute/v1/projects/wfender-test/global/instanceTemplates/kubernetes-minion-template].

NAME	MACHINE_TYPE	PREEMPTIBLE	CREATION_TIMESTAMP
kubernetes-minion-template	n1-standard-2		2021-10-05T21:02:58.325-07:00

Using subnet default

Attempt 1 to create kubernetes-windows-node-template

WARNING: You have selected a disk size of under [200GB]. This may result in poor I/O performance. For more information, see: <https://developers.google.com/compute/docs/disks#performance>.

Created [https://www.googleapis.com/compute/v1/projects/wfender-test/global/instanceTemplates/kubernetes-windows-node-template].

NAME	MACHINE_TYPE	PREEMPTIBLE	CREATION_TIMESTAMP
kubernetes-windows-node-template	n1-standard-2		2021-10-05T21:02:54.396-07:00

Created [https://www.googleapis.com/compute/v1/projects/wfender-test/zones/us-central1-b/instanceGroupManagers/kubernetes-minion-group].

NAME	AUTOSCALED	LOCATION	SCOPE	BASE_INSTANCE_NAME	SIZE	TARGET_SIZE	INSTANCE_TEMPLATE
kubernetes-minion-group	no	us-central1-b	zone	kubernetes-minion-group	0	3	kubernetes-minion-template

Waiting for group to become stable, current operations: creating: 3

Waiting for group to become stable, current operations: creating: 3

Group is stable

INSTANCE_GROUPS=kubernetes-minion-group

NODE_NAMES=kubernetes-minion-group-54xc kubernetes-minion-group-bbkh kubernetes-minion-group-vmxr

Trying to find master named 'kubernetes-master'

Looking for address 'kubernetes-master-ip'

Using master: kubernetes-master [external IP: 34.123.148.55; internal IP: (not set)]

Waiting up to 300 seconds for cluster initialization.

This will continually check to see if the API for kubernetes is reachable.

This may time out if there was some uncaught error during start up.

GCP Cloud Provider - What's Left!

Cloud Provider LKG Testing :

<https://docs.google.com/document/d/1U1YRLsAAZsVs6VyrXj8hkfA6aJp9nDZsG5NsfZ1POPE/edit?resourcekey=0-iVuzWZn3mxL2Qil-4peFFQ#heading=h.fxpk50cps4zs>

Integrate with Prow for Post Submit testing on both K/K and cloud-provider-gcp submits

Fix K/K extraction so cloud provider and credential provider feature gates can be enabled

Look at easier installation than kube-up

Look at providing a sample HA implementation

vSphere Cloud Provider

Nicole Han, Software Engineer III, VMware

vSphere Cloud Provider

Recent updates since v1.18

- Add new zone/region topology labels **topology.Kubernetes.io/zone** and **topology.Kubernetes.io/region**
- Add new instance type labels **node.kubernetes.io/instance-type**.
 - example: **node.Kubernetes.io/instance-type=m3.medium**
- Initial support for NST-T routable pods
- Introduce initial support for vSphere paravirtual cloud provider
 - Two modes: vsphere / vsphere-paravirtual
- Add initial support for NSX-T routable pods in vSphere paravirtual cloud provider
 - add IPPool and RouteSet APIs
 - introduce node and ippool controllers to do node ipam
 - implement Route interface in vSphere paravirtual cloud provider
- Helm chart migration: installation by Helm chart is currently supported

vSphere Cloud Provider

Migration to out of tree

Kubernetes is moving away from maintaining cloud providers in-tree and everyone will need to use out-of-tree cloud providers

Install out-of-tree vSphere cloud provider

- [vSphere](#) 6.7U3 (or later) is a prerequisite from using CPI
- The Kubernetes version must be 1.18 or higher
- Install CPI: refer to [examples, tutorials and docs](#) / use [official vSphere CPI helm chart](#)
- Check more details here: https://cloud-provider-vsphere.sigs.k8s.io/concepts/in_tree_vs_out_of_tree.html



KubeCon



CloudNativeCon

28

North America 2021

vSphere Cloud Provider

Roadmap

- CPI migration: merge vSphere cloud provider and vSphere paravirtual cloud provider
- Add IPv4/IPv6 dual-stack support
- Support k8s 1.22 in the next release (1.22)

Ask questions: [#provider-vsphere](#) [#sig-cloud-provider](#)



File issues: <https://github.com/kubernetes/cloud-provider-vsphere/issues>



Cloud Provider

Futures and interesting topics

Cloud Provider SIG

futures and interesting topics

[DisableCloudProviders](#) and [DisableKubeletCloudCredentialProviders](#) feature gates need to be brought to Beta. We know this will break a considerable number of K/K tests. These tests either depend on cloud provider functionality, test features which depend on cloud provider functionality or are dependent on e2e systems which depend on cloud provider functionality. We need to identify these cases. Then we need to either fix them or move them out of tree.

Need a plan on how to handle multi-repo dependencies and multi-repo testing. Leading candidate right now is the [Last Known Good](#) proposal. Please take a look and comment.

As part of the clean up of legacy cloud provider artifacts, we would really like to remove the “cluster” directory. However this needs to be coordinated with other SIGs (cluster lifecycle, testing, scalability)

Making the various cloud-provider-<X> work better. Standardizing on branching, how to bring them, docs for them etc.

Kubernetes Cloud Provider SIG

How to get involved and learn more





github.com/kubernetes/cloud-provider



Link to join the group  

- <https://groups.google.com/forum/#!forum/kubernetes-sig-cloud-provider>

Regular SIG meeting:

- Biweekly Wednesday 1PM Pacific Time, next on Oct 27 
- See [Kubernetes contributor calendar](#) for details. Agenda+Notes [link](#) 

Cloud Provider Extraction meeting series

- *usually* Biweekly Thursday 1:30PM Pacific, Next Oct 21
- See [K8s community calendar](#) for details. Agenda+Notes [link](#)

Link to join Slack 

- <https://kubernetes.slack.com/archives/C718BPBQ8>

Video Recordings  YouTube 

- <https://youtube.com/playlist?list=PL69nYSiGNLP3dXLcYbRKCbpPCN-8CDFAB>

Q&A

Thank You

This deck is available here: <https://sched.co/IV7E>