KubeCon | CloudNativeCon

Europe 2022

WELCOME TO VALENCIA

KubeCon CloudNativeCon Europe 2022

SIG Cloud Provider

Portable K8s Across all Clouds,

Roadmap and Updates

Steven Wong
Software Engineer
VMware

Nicholas Turner
Software Engineer
Amazon

Thursday May 19 11:55am Room 3FG *Feria Valencia* https://sched.co/ytow

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, with an implementation for each.

The agenda will include:

- An overall status report on removing the cloud provider code from the main Kubernetes repository to “out of tree repositories;
- “Lightning talks” for individual cloud providers, reporting efforts, accomplishments, and roadmap for features and getting "out-of-tree".
- We’ll also discuss the plans to handle cloud provider migration - including interesting topics like building and migrating to cloud controller managers, and kubelet image credential providers.

The goal of SIG Cloud Provider is to promote a vendor-neutral ecosystem for our community. We will close with details on how you can get involved with the SIG as either a cloud infrastructure supporter, a K8s distribution author, or a K8s user.

Agenda

Cloud Provider – background
- What is it? Motivation of the move out-of-tree

General Status Report

“Lightning Talks” from platform specific contributor’s efforts
- accomplishments, roadmap for features and getting out-of-tree

Cloud Provider futures and interesting topics
- building and migrating to cloud controller managers, and kubelet image credential providers

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.
- Leader migration is GA in 1.24. This allows an HA cluster to migrate cloud controllers from KCM to CCM. (KEP)

Cloud Controller Manager

- Vendor specific binary which runs cloud loops like: cloud-node, cloud-node-lifecycle, cloud-node-ipam, cloud-route, cloud-service. (KEP)

Cloud Provider Migration

General Status Update

API Server

- SSH tunnels were removed and replaced by the network proxy. (KEP)
- Replacing the persistent volume labelling admission controller is planned for 1.25. (KEP)

Kubelet

- Node addressing functionality is replaced by the cloud-node controller.
- Volume plugin code is replaced by CSI migration.
- Docker image credential plugins are replaced by the kubelet image credential provider, which is now beta. (KEP)

Cloud Provider Migration

General Status Update

Things to know

- In order to migrate without CSI migration enabled, the in-tree cloud provider in the KCM must be enabled for volume plugins only using --external-cloud-volume-plugin=<cloud-provider-name>
- In order to replicate the node-ip feature in the kubelet when the external CCM is enabled, there exists an annotation alpha.kubernetes.io/provided-node-ip.
  - This feature allows the node addresses provided by the cloud provider to be filtered to a specific address specified by the flag/annotation.
- There is currently a bug where the kubelet and cloud-node controller both reconcile node addresses during upgrade, when the ccm is running as leader but nodes have not been upgraded to have --cloud-provider=external. This means they must agree on the set of addresses to avoid flapping during that time.

KubeCon CloudNativeCon Europe 2022

“Lightning Talks”

Updates from platform specific cloud providers

Alphabetical order

Photo by Yarenci Hdz on Unsplash

KubeCon CloudNativeCon Europe 2022

Provider IBM Cloud

Overview and Update for KubeCon Europe 2022

Sahdev Zala, John Kasperski

Provider IBM Cloud overview and update

Cloud Provider SIG sub-project for building, deploying, maintaining, supporting, and using Kubernetes on IBM Public and Private Clouds

- https://github.com/kubernetes/community/blob/master/sig-cloud-provider/README.md#provider-ibmcloud

GitHub repos and recent progress

- Cloud Provider
  - Cloud Controller Manager (CCM) implementation
- Cluster API
  - Implementation of an IBM Cloud Provider for the Kubernetes Cluster API project
  - Updated to K8s Cluster API v1.13, Enhanced e2e testing, Doc and logging improvements
  - Added EventRecorder framework to get resources events, Enabled linters per golangci/golangci-lint
- VPC Block CSI Driver
  - Provides Container Storage Interface to manage the lifecycle of IBM VPC Block Data volumes
  - Handle provision when zone/region not provided, Code refactor, Doc and test improvements
- PowerVS Block CSI Driver
  - Provides CSI interface to manage the lifecycle of Power Virtual System volumes
  - Repo moved under Kubernetes-Sigs GitHub recently
  - Support for volume access modes ReadWriteMany and ReadOnlyMany, GH workflow, Dependencies update

Provider IBM Cloud overview and update

Cloud Provider Interfaces

- Load Balancer
  - Configures external VPC ALB
- Instances V1/V2 (i.e. Nodes) and Zones
  - Metatdata service calls VPC to gather node information
- Clusters and Router
  - Not implemented, Calico provides routing

Recent Work and Roadmap

- OpenShift 4.10: Initial open source release
  - Two open source repos (ccm, vpc controller), complicated build process
- OpenShift 4.11: Single open source repo
  - Simplified usage and build process, improved performance
- Working on making repo ready for the community development
  - Code refactoring and doc improvements

KubeCon CloudNativeCon Europe 2022

Cloud Provider vSphere

Overview and Update for KubeCon Europe 2022

Lubron Zhan, Fang Han, Xudong Liu

Cloud Provider vSphere overview and update

Releases

- 1.22.6
  - Support k8s 1.22
  - Dual stack support - IPV4 and IPV6 (Alpha)
  - Ability to exclude subnets for internal/external node ip selection
- 1.23.0
  - Support k8s 1.23
  - Support selecting external/internal node ip from list of cidr

Roadmap

- E2E test pipeline
- 1.24 release
- GA Dual stack support

KubeCon CloudNativeCon Europe 2022

Cloud Azure

Overview and Update for KubeCon Europe 2022

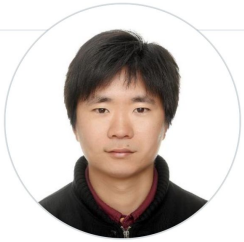
Penfei Ni, Andy Zhang, Qi Ni

CLOUD PROVIDER AZURE

updates & highlights from Pengfei & Andy & Qi in Shanghai

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

Pengfei Ni
feiskyer



Andy Zhang
andyzhangx

Qi Ni
nilo19

Recent Achievements

- GA of Azure disk in-tree driver to CSI migration in v1.24
- Refactoring test infra & migrating e2e tests from AKS Engine to Cluster API Provider Azure (CAPZ)
- acr-credential-provider has been added as part of cloud-provider-azure repo
- cloud provider new features: custom config for LB probe rules with service annotations, private link support with service annotations, ARM64, node IP based SLB backend pool, and more
- New CSI driver features: Windows Server 2022, AzureDisk online resize, cross subscription on Azure File and Blob

What's Next

- VMSS Flex
- Dual-stack IPv4/IPv6 networking
- Operation tracing
- CSR auto approver
- Azure Lustre CSI Driver
- Azure Disk CSI Driver v2 GA
- Turn off FloatingIP on SLB
- blobfuse2 support on Blob CSI driver
- GA of Azure File in-tree driver to CSI migration in v1.25

KubeCon CloudNativeCon Europe 2022

Cloud AWS

Overview and Update for KubeCon Europe 2022

Nick Turner

Cloud Provider AWS

General Status Update

Releases

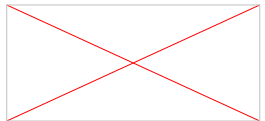
- Stable releases of the Cloud Controller Manager: v1.24.0, v1.23.1, v1.22.1, v1.21.0, v1.20.0
- AWS Load Balancer Controller: v2.4.1

Update and Roadmap

- CCM usage by distributions:
  - EKS has migrated to the AWS CCM (service and node-lifecycle controllers) in 1.22+.
  - Kops has migrated to the AWS CCM in 1.22+.
- CSI migration:
  - Kops and EKS support the EBS CSI driver installation through managed addons.

GCP Cloud Provider

Walter Fender - Google



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 NodeIpamController
- 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 NodeIpamController

- 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

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

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 9AM Pacific Time, next on tbd
- See Kubernetes contributor calendar for details. Agenda+Notes link

Cloud Provider Extraction meeting series

- *usually* Biweekly Thursday 9:30AM Pacific, Next tbd
- See K8s community calendar for details. Agenda+Notes link

Link to join Slack

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

Video Recordings

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

Q&A

Thank You