
KubeCon
CloudNativeCon
Europe 2021
Virtual
Forward Together »

Cloud Provider AWS Update and Roadmap

Nick Turner, Ayberk Yilmaz, Yang Yang, Amazon & Nicole Han, VMWare

Agenda

- Legacy Cloud Provider Extraction/Migration
- AWS Cloud Provider V2
- Credential Provider
- AWS Load Balancer Controller

Background - Cloud Provider

- The cloud provider interface and implementations were built into Kubernetes.
- The community realized this was going to cause significant bloat and maintenance effort unless it could be extracted into separate repositories, binaries, and build systems.
- Thus began a multiyear effort to extract all cloud-specific code from Kubernetes.

Background - Cloud Provider

Extraction efforts by component

Component	Extraction Effort
Kube controller manager (node, node lifecycle, service, route)	Cloud controller loops are being extracted into the cloud controller manager.
Kube controller manager (volume controller loops)	Volume controller loops are being replaced by CSI drivers.
Kubelet (Docker Image Credential Provider)	Built-in credential provider will be replaced by the external credential provider node binary.

Background - Cloud Provider

Extraction efforts by component

Component	Extraction Effort
Kubelet (fetching node addresses)	Cloud controller manager will manage node addresses.
Kube API Server (ssh tunnel)	Network proxy
Kube API Server (persistent volume labels [1] [2])	Persistent Volume Controller (cloud code removed)

Timeline

Extraction timeline by component (estimates!)

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		
In tree code removal					Earliest Possible	

Cloud Controller Manager

- Upstream features are no longer being accepted (pull requests are limited to bug fixes).
- The code has been duplicated in the cloud-provider-aws repository.
- Installation by helm chart and kops are currently supported.

Cloud Controller Manager

Responsibilities

What are the cloud-controller-manager's responsibilities?

- For AWS, run the node, nodelifecycle, route and service controllers.

Controller	Responsibility
Node	Update node status, node addresses.
Node Lifecycle	Act on node events, like deletions.
Service	Manage cloud loadbalancers for loadbalanced services.
Route	Manage a cloud route table if nodes have CIDRs.

Cloud Provider AWS v2

- **v2 new implementation:** continue to support the existing AWS provider in “out-of-tree” mode

- **v1 legacy implementation:** many known issues and gaps in current provider implementation, for example
    - Allow for hostnames other than private dns as a node name
    - Allow load balancer names to be provided via service annotation

- The v2 implementation is only supported for new clusters

Cloud Provider AWS v2

Implement Interfaces:

- **Instances:** initial implementation of **InstancesV2** interface
  - InstancesV2 ≈ Instances → significantly reduce API calls to the cloud provider
  - use the node name or provider ID field to find the node in the cloud provider
  - TODO: support node naming policy other than private DNS names
- **Zones:** this is **deprecated** in favor of retrieving zone/region information from InstancesV2
  - After Kubernetes v1.20, zone/region information should be added in the InstanceMetadata type we're using as part of the new InstancesV2 interface
- **LoadBalancer:** initial pass of implementation is working in progress
  - Some key issues we need to address: friendly LB names, more expressive APIs for load balancer configuration options, etc.

Credential Provider

- Kubelet fetches credentials to fetch images
- Three “in-tree” implementations: ACR, ECR, GCR
- As part of the extraction, cloud specific code should be removed
- A new plugin architecture to fetch credentials
  - “Plugin” is a separate binary
  - Kubelet asks the plugins to fetch credentials
  - Communication via stdio using JSON
  - For details see KEP-2133

Credential Provider

- Cluster operators need to pass two new flags to Kubelet:
  - --image-credential-provider-bin-dir
  - --image-credential-provider-config
- Implementation for ECR is ready
- Cloud Provider will ship with the ECR plugin
- More info can be found on our docs (even an example config)

AWS Load Balancer Controller

A controller to help manage Elastic Load Balancers for a Kubernetes cluster.

- Satisfies Kubernetes Ingress resources by provisioning Application Load Balancers.
- Satisfies Kubernetes Service resources by provisioning Network Load Balancers.

formerly known as "AWS ALB Ingress Controller", we rebranded it to be "AWS Load Balancer Controller".

AWS Load Balancer Controller

What's supported?

- Ingress resources with Application Load Balancers
  - Instance mode & IP mode
  - Ingress Groups
- Service resources with Network Load Balancers
  - Compatible API with in-tree Service/NLB support
  - IP mode only
- TargetGroupBinding CRD
  - expose applications with an existing TargetGroup(ALB/NLB)

AWS Load Balancer Controller

What's coming?

- NLB instance mode support
- NLB Static private IP support
- NodeSelector support for instance mode (Ingress/Service/TargetGroupBinding)
- IngressClassParams support
- Ingress Path type support
- Ingress Simplified SSL redirection configuration

Thank You!

- https://cloud-provider-aws.sigs.k8s.io/
- https://github.com/kubernetes/cloud-provider-aws
- https://github.com/kubernetes-sigs/aws-load-balancer-controller

Find us on k8s slack:

- @nckturner, @Nicole Han, @ayberk, @m00nf1sh