CLOUD NATIVE ECOSYSTEM

Upstream Open Source

Photo: Bridget Kromhout

Cloud Native Ecosystem
Upstream Open Source

We contribute upstream to Kubernetes and related open source projects to meet cloud native user needs on Azure.

We participate in the Cloud Native Computing Foundation (CNCF) and other open governance initiatives.

We connect our Azure product counterparts with what's happening in the broader ecosystem.

github.com/Azure/container-compute-upstream

Kubernetes & CNCF governance

Kubernetes Special Interest Groups (SIGs) & Working Groups:

WG-LTS, WG Gateway API, sig-release (Kubernetes release management), SRC (Security Response Committee), sig-apimachinery, sig-apps, sig-auth, sig-autoscaling, sig-cli, sig-cloud-provider, sig-cluster-lifecycle, sig-contribex, sig-network, sig-node, sig-scheduling, sig-storage, sig-testing, sig-windows

CNCF Technical Advisory Groups (TAGs):

tag-runtime, code of conduct, containerd, moby, Istio, OCI, OPA Gatekeeper

Kubernetes Enhancement Proposals (KEPs)

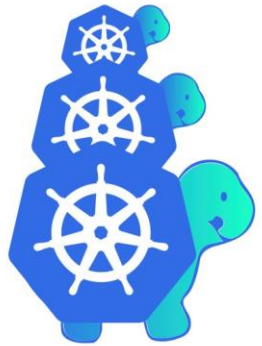
Recent KEPs we're leading to move feature enhancements from idea to alpha, beta, and graduated:

- 3299 KMS v2 encryption at rest (beta v1.27, targeting stable v1.29)
- 3221 Structured Authorization Configuration (implementing, targeting alpha v1.29)
- 3331 Structured OIDC Configuration (implementing, targeting alpha v1.29)
- 1981 Windows Privileged Containers and Host Networking Mode (stable v1.26)

Product tie-in: Azure Kubernetes Service (AKS):

- KMSv2 and Windows Privileged containers are already available on AKS
- We build, scan, and patch CNCF container artifacts for the rest of Microsoft

Kubernetes SIG Cluster Lifecycle: Cluster API



Cluster API (CAPI) brings declarative, Kubernetes-style APIs to cluster creation, configuration, and management. The API is shared across multiple cloud providers.

CAPZ (Cluster API Provider Azure) can be used to manage AKS clusters.

cluster-api.sigs.k8s.io/

capz.sigs.k8s.io/

Service Mesh

Azure team members contribute upstream to the CNCF graduated project Istio, built on industry-standard Envoy

Previous project: Open Service Mesh (OSM)

Product tie-in in public preview: AKS Istio Add-on

istio.io

Azure Active Directory Workload Identity

Using Kubernetes primitives, you can configure identities and bindings to match pods. Without any code modifications, containerized applications can securely access resources using AAD as the identity provider.

Previous project: AAD Pod Identity

Product tie-in generally available: AKS Workload Identity

azure.github.io/azure-workload-identity

OPA Gatekeeper

Gatekeeper is a policy controller for Kubernetes.

- uses the Open Policy Agent constraint framework to describe and enforce policy for Kubernetes resources
- applies at-scale enforcements and safeguards on your clusters in a centralized, consistent manner

Product tie-in: Azure Policy (a supported implementation of Gatekeeper for AKS and Arc)

github.com/open-policy-agent/gatekeeper

Supply Chain Security: Eraser

Given a list of images, Eraser can remove them from all Kubernetes nodes, while differentiating between running vs non-running images. Eraser has support for CRI runtimes (dockershim, containerd, CRI-O).

Eraser was recently accepted as a CNCF Sandbox project.

Product tie-in: Image Cleaner (https://learn.microsoft.com/azure/aks/image-cleaner)

github.com/Azure/eraser

OPEN SOURCE NEEDS YOU!

brendandburns @brendandburns · Dec 7
Phippy's visit to Seattle kicks off with the iconic Seattle Space Needle

Join the Adventure!

brendandburns @brendandburns · 19h
Phippy wonders if this one could run PHP or containers...