The definitive CNI Landscape Chart

Presented by Calico, the most adopted Container Networking and Security Technology

Environment	Default CNI (Officially supported by Kubernetes Platform/Service Provider)			Bring your own CNI (Third-party integrations)
Microsoft AKS	**Azure CNI** (Native VNet networking, overlay networking preview) Azure CNI is the default plugin from Microsoft that allows Kubernetes pods to be connected directly to Azure Virtual Networks (VNet). With Azure CNI Overlay, the cluster nodes are deployed into an Azure Virtual Network (VNet) subnet, whereas pods are assigned IP addresses from a private CIDR.	**Kubenet** (Route based networking) Kubenet is a simple networking plugin that is included by default in Kubernetes. It uses a virtual network built on top of the Azure Network fabric to enable communication between pods.	**Azure-CNI powered by Cilium** (eBPF dataplane, preview) Azure CNI Powered by Cilium combines the robust control plane of Azure CNI with the dataplane of Cilium to provide high-performance networking and security. **Note:** Cilium configuration is managed by AKS and can't be modified. Also CiliumNetworkPolicy custom resources and Hubble aren't supported.	**BYOCNI** (Overlay networking) Bringing your own container networking interface (CNI) for more control over network topology, routing policies, and security configurations. Third-party CNIs may offer additional functionality beyond default options and work across providers. Example: Using Calico as a BYOCNI. **Pros:** • Traffic encryption • Pluggable dataplane • eBPF dataplane supports XDP, DSR, and source IP preservation • Expanded security controls • Observability into networking flow logs • FIPS 140-2 US compliant **Cons:** • Learning curve
	Pros: • Pods acquire IP from Azure Network (VNet) • Conserves IP address space (Overlay) • Best integration with Azure products • Windows support • Best performance **Cons:** • IP exhaustion (VNet) • Limited control over, network topology, routing policies & security configurations	**Pros:** • Easy-to-use • Conserves IP space • Ideal for small to medium-sized clusters • Choice of policy engine **Cons:** • Limited to 400 Nodes per cluster (Hard limit) • No windows support • Limited control over, network topology, routing policies & security configurations	**Pros:** • Functionality equivalent to existing Azure CNI and Azure CNI Overlay plugins **Cons:** • Available only for new clusters. Linux only • K8s `internalTrafficPolicy=Local` services not supported. • Services can't use the same host port with different protocols (TCP or UDP) • Limited control over, network topology, routing policies & security configurations	
	CNI Chaining: Microsoft AKS supports third-party CNIs. Use Azure web portal or Azure CLI to deploy your AKS with Calico (eBPF & IPtables dataplane).	**CNI Chaining:** Microsoft AKS supports third-party CNIs. Use Azure web portal or Azure CLI to deploy your AKS with Calico (eBPF & IPtables dataplane).	**CNI Chaining:** Not supported.	
Amazon EKS	**AWS-CNI** (Native VPC networking) Kubernetes pods are connected directly to the Amazon VPC.	**Pros:** • Best performance • Native VPC routing • Integration with all other AWS products	**Cons:** • Limited control over, network topology, routing policies & security configurations	
	CNI Chaining: Amazon EKS runs upstream Kubernetes, so you can install alternate compatible CNI plugins to Amazon EC2 nodes in your cluster.			

Red Hat OpenShift

OVN-Kubernetes

OVN-Kubernetes provides networking capabilities for OpenShift clusters.

Pros:
- Fully supports and implements Kubernetes network policy resources
- Supports IPsec encryption
- Supports IPv6

Cons:
- No support for setting the external traffic policy or internal traffic policy for a Kubernetes service to local
- Difficult for users to migrate from OpenShift SDN to OVN
- Can be difficult to run a dual-stack cluster

Openshift SDN

OpenShift SDN (Software Defined Networking) is another Container Network Interface (CNI) plugin OpenShift clusters.

Pros:
- Easy to setup, and configure
- Well established and battle tested
- Excellent integration with all openshift features

Cons:
- Limited scalability
- Doesn't support IPv6
- Partial support for Kubernetes network policy resources

OpenShift supports third-party CNIs that are deployed and managed through an operator. Each OpenShift partner that has a third-party CNI will be granted a certification that allows them to release an OpenShift version which can be installed using the official OpenShift GUI or by the OC command line utility.

GKE

GKE v1

GKE v1 is a good option for users who value simplicity, stability, and compatibility with existing applications.

Pros:
- GKE v1 has a simpler architecture than v2
- Easier to set up and manage if you are new to Kubernetes
- Battle tested
- Less expensive for smaller workloads
- Best compatibility level

Cons:
- Limits your control over certain aspects of your Kubernetes cluster
- Vendor lock in
- Difficult to migrate from

CNI Chaining:
GKE has built-in support for Calico, providing a robust implementation of the full Kubernetes Network Policy API. GKE users wanting to go beyond Kubernetes network policy capabilities can make full use of the Calico Network Policy API.

GKE v2

GKE V2 is a new dataplane based on eBPF optimized for GKE and Anthos-based cluster networking.

Pros:
- A consistent user experience for networking in GKE and all Anthos clusters
- Real-time visibility of network activity
- eBPF-based dataplane for Linux nodes

Cons:
- Limits your control over certain aspects of your Kubernetes cluster
- Vendor lock in
- Difficult to migrate from
- Little to No third-party integration is allowed

CNI Chaining:
No support for any third-party CNIs.

BYOCNI is not supported on any version of GKE.

Rancher RKE

The Canal CNI

(Container Network Interface)

the default plugin that provides networking and security in a Rancher environment. It combines two popular open-source solutions, Calico and Flannel, to deliver a comprehensive networking and security solution for Kubernetes clusters.

Pros:
- Simplicity of Flannel's with the power of Calico
- Easy-to setup
- High performance

Cons:
Third party CNI's can be more complex to set up and manage compared to Canal.

Still unsure about which option exactly matches your needs? We have a dedicated community to assist you in getting started with cloud-native and Kubernetes. So don't hesitate and come ask us in our slack channel!

https://slack.projectcalico.org/

About Project Calico

Project Calico is an open-source project with an active development and user community. Calico Open Source was born out of this project and has grown to be the most widely adopted solution for container networking and security, powering 2M+ nodes daily across 166 countries.

Calico Open Source

Calico Open Source is a networking and security solution for containers, virtual machines, and native host-based workloads. Calico supports a broad range of platforms including Kubernetes, OpenShift, Docker EE, OpenStack, and bare metal services.

Whether you opt to use Calico's eBPF data plane, Linux's standard networking pipeline, or the Windows data plane, Calico delivers blazing-fast performance with true cloud-native scalability. Calico provides developers and cluster operators with a consistent experience and set of capabilities whether running in public cloud or on-premises, or on a single node or across a multi-thousand node cluster.

Calico Cloud for Container Security

Calico Cloud is the industry's only active security platform with full-stack observability. The fully managed, pay-as-you-go SaaS provides active security for cloud-native applications running on containers and Kubernetes. It enables organizations to prevent attacks using zero trust and to detect, troubleshoot, and automatically remediate exposure risks from security breaches across multi-cloud and hybrid deployments. Calico Cloud is built on Calico Open Source, the most widely adopted container networking and security solution.

Calico Enterprise for Kubernetes

Calico Enterprise extends the declarative nature of Kubernetes to specify security and observability as code for Kubernetes platforms. This ensures consistent enforcement of security policies and compliance and provides observability for troubleshooting across multi-cluster, multi-cloud, and hybrid deployments. Calico Enterprise is built on Calico Open Source, the most widely adopted container networking and security solution.

Tigera, Inc.

58 Maiden Lane, Fl 5
San Francisco, CA 94108
+1 (415) 612-9546 / www.tigera.io