OpenShift compared to the Sidero Platform

OpenShift Platform Overview

OpenShift is a Platform-as-a-Service (PaaS) that has evolved into a Kubernetes distribution. It adds additional features, and relies heavily on Kubernetes operators to run. It attempts to provide a complete enterprise ready platform, that addresses all the requirements of enterprises with respect to software development and operations. Openshift is available on Amazon, Azure, and GCP as a managed service, or can be customer deployed and managed on those platforms, plus VMware and bare metal. It does not support ARM architectures.

Sidero Platform Overview

Sidero is a platform designed for Kubernetes, and delivers an opinionated, secure vanilla Kubernetes deployment. It allows complete control and flexibility in the choice of Kubernetes deployments, while ensuring a secure and reliable base and automating operational practices. It runs on all major cloud providers, Vmware, Hyper-V, bare metal, and ARM architectures, including single-board computers such as Raspberry Pi.

Principles

Sidero Platform

The Sidero platform is built upon Talos Linux, which was designed from the start to be a secure, minimal platform for Kubernetes. Except for the Linux kernel, all OS components have been excluded, or rewritten just to support Kubernetes. All OS file systems are immutable, and all management is done via a gRPC API - there is no SSH, no console, no telnet, no package manager. This means the attack surface is very small. All OS and Kubernetes configurations are set to secure defaults. Controllers exist to manage Kubernetes at the operating system level, meaning that even if Kubernetes itself is down or the cluster

has not yet started, the OS will react to commands to resolve or diagnose Kubernetes issues. Updates are purely image based, and thus atomic and easy to control. Talos Linux is updated about every 2 months, always shipping with the latest stable Linux kernel and Kubernetes versions (currently 5.15 and 1.22, respectively)

A Talos Linux cluster only supports Talos Linux members, which allows the cluster to automate a variety of maintenance tasks, as Talos Linux presents APIs designed for such Kubernetes and OS operations. Things like creating consistent snapshots of etcd, or updating the cluster OS or Kubernetes version are simple Talos API commands.

Talos Linux installs a minimal OS and secure Kubernetes, but, because it installs vanilla Kubernetes, it provides a great deal of flexibility in what other components to employ: Talos allows the adoption of any desired CNI, logging system, CI/CD pipeline, etc. It also delivers the ability to tweak the kernel and OS low level parameters.

Talos Linux supports all scale of environments, from deploying in a Docker container on a developer's machine, to a Raspberry Pi and other SBCs, through hypervisors and large scale datacenter machines and cloud instances. Having a consistent OS and Kubernetes deployment across all platforms and all parts of the development lifecycle, with consistent API management, allows confidence that code promoted from development to production will work reliably.

Sidero Labs is committed to open-source, and working with our community. Our core developers are active in our Slack community, and very responsive. Because Sidero is small, we can be agile - features and contributions from community members are often released within weeks.

The Sidero platform distributes a fully validated, vanilla (but secured) Kubernetes deployment. This means no lock in. The Kubernetes setup you deploy on Talos Linux will work on other platforms. (Note that the reverse is not always true - because of the security configuration and hardening of the Sidero platform, some CSIs and other components may not run on Talos Linux, as they depend on provably insecure features.)

OpenShift

OpenShift was a PaaS that predated Kubernetes, that has been adapted to the Kubernetes world. It now incorporates Red Hat Enterprise Linux CoreOS (RHCOS) as the underlying OS for control plane nodes, which offers some immutable file systems, but was not initially designed for Kubernetes, and thus still installs ssh, systemd, and rpm package manager. This means that OpenShift's attack surface is larger. Perhaps more significantly, it means that OpenShift and its nodes still have the expectation that a systems-administrator will SSH into them for some management tasks. This has the advantage that it is consistent with historical methods of Linux administration, and so may impose less of a paradigm shift on systems admins. However, it is at odds with the controller based, cattle-not-pets paradigm of Kubernetes itself, which is the model adopted by Talos Linux.

OpenShift uses the same model as RedHat Enterprise Linux - it is based on an open source project, but the commercially supported version uses older versions with security and

other fixes backported to them. OpenShift currently still uses version 4 of the Linux kernel. An OpenShift cluster mandates RHCOS for the control plane, but supports either RHCOS or RHEL for the worker nodes.

OpenShift attempts to provide a complete environment for an Enterprise PaaS, in the form of Red Hat OpenShift Container Platform. (This is what is generally meant by "OpenShift". It is possible to deploy a more limited product, OpenShift Kubernetes Engine, which is generally just the operating system and Kubernetes, but it is not well documented - the expectation is that customers will purchase the Container Platform.) The OpenShift Container Platform bundles in a variety of other tools to deliver what Redhat considers a complete PaaS:

- developer console,
- prometheus/grafana monitoring
- Centralized policy management
- JBoss web server
- SSO
- log aggregation and management via Elasticsearch and Kibana integrated with Fluentd for log collection
- OpenShift workspaces
- OpenShift Virtualization (lets OpenShift manage and use both containers and VMs with Kubernetes, using KubeVirt)
- Kubernetes-native continuous integration/continuous delivery (CI/CD) pipelines based on Tekton
- OpenShift GitOps: An opinionated workflow integrating git repositories based on Argo CD
- Serverless based on Knative
- Service Mesh based on Istio, Jaeger and Kiali;

OpenShift mandates the use of the CRI-O container runtime; a specific CSI; limits the choice of CNIs, etc. There are advantages to this delivery of a complete environment, but some users report it is heavy-handed and overly-burdensome for many environments. One complaint is that there is a non-trivial amount of time spent administering, securing and updating components that may not even be in use in a given environment. Further, in order to deliver the complete PaaS, OpenShift modifies Kubernetes, and migration to vanilla Kubernetes on other platforms is generally impossible.

Installation and Updates

Because the Sidero platform runs on Talos Linux, which is designed solely around running Kubernetes, it is very quick and simple to create a Kubernetes cluster. A new secure cluster can be created from scratch in about 5 minutes, and controlled upgrades (maintaining high availability during the upgrade process) take about 10 minutes.

Talos Linux relies on controllers and declarative configurations, in the same manner as Kubernetes.

OpenShift installation and upgrades take much longer. Installation can take up to a week, and an upgrade of even a minimal 3 node cluster will take at least an hour. This is partially due to the fact that OpenShift comes with many more components, which are bundled in the upgrades - with a Sidero cluster, upgrades are atomic.

OpenShift also relies on machine configurations and a controller to manage server state, but because nodes can have files changed by other mechanisms (admins using SSH, etc), it is less robust, and will generally mark nodes "degraded" when there is a difference between running and desired state, rather than enforcing the correct configuration, as Talos Linux does.

License and cost

(Prices accurate as of December, 2021)

Talos Linux is completely Open Source, and can be used for free. Enterprise support is available, and priced simply depending on the number of worker nodes. The number of CPUs or cores per node does not matter.

For reference, the cost to obtain 24 x 7 support for Talos Linux on:

- A cluster with 20 x 8-core worker nodes: $45,000 per year.
- A cluster with 100 x 8 core worker nodes: $100,000 per year

Fully managed Talos clusters are available on all supported environments.

OpenShift can not be run without a support contract. Pricing for licensing is a complex endeavour based on sockets, vCPUs, features selected, and use of nodes. See https://www.redhat.com/en/resources/self-managed-open-shift-sizing-sub-guide.

For reference, the cost to obtain 24 x 7 support for OpenShift Container Platform is:

- A cluster with 20 x 8-core worker nodes: $645,000 per year.
- A cluster with 100 x 8 core worker nodes: $3,200,000 per year

Fully managed OpenShift clusters are available only on cloud (AWS,GCP, Azure) environments.

Summary

Red Hat OpenShift Container Platform is a mature offering, which provides a complete supported Platform as a Service offering. It commands a premium price point, but may be appropriate for enterprises that require a single vendor solution, and that wish to use all the integrated components of the OpenShift platform..

The Sidero Platform is a newer, more modern entrant into the space. It offers more flexibility, and allows customers to deploy just the Kubernetes components needed for their intended use of the platform. It supports spanning a cluster across disparate networks or cloud providers. It provides comprehensive support for the operating system and Kubernetes, but support for other components (CI/CD tools, for example) should be obtained from the vendors of those tools. Sidero is best suited for enterprises that are deploying Kubernetes either in a more limited role than a full PaaS; that are comfortable with (or prefer) other tools than those included in Red Hat OpenShift Container Platform, or those looking for a more cost-effective solution.