Red Hat OpenShift 4.6, the Kubernetes Platform for Government

November 17, 2020 | by Matthew Bach

It’s an exciting time to be a Red Hat OpenShift user in the federal space. Version 4.6 of OpenShift, Red Hat’s 100% CNCF certified Kubernetes distribution, was just released and with it comes a number of enhancements focused on enabling our government customers to accelerate and expand their adoption of containers and DevSecOps. Let’s walk through those features and what they mean to our federal customers.

A COMPREHENSIVE FIPS APPROACH TO KUBERNETES

At Red Hat, we’ve made it our business to ensure our government customers are able to meet their compliance requirements in software systems and this remains true with Red Hat OpenShift Container Platform 4. FIPS validation is a critical part of meeting compliance in the government sector. If you’re evaluating a Kubernetes based distribution today, there are several key points you should consider that are critical to the success of remaining FIPS compliant.

1. Does the Kubernetes vendor include and support a Linux OS with FIPS enabled crypto? Choosing a vendor that directly supports both the Linux OS running in FIPS mode, and the Kubernetes distribution simplifies support and reduces risk.
2. Does the Kubernetes vendor actually test their platform with FIPS enabled crypto with every release? This is a significant, expensive investment that helps deliver compatibility and resiliency.
3. Has your Kubernetes vendor received 3rd party validation for their FIPS enabled solution or submitted it for validation by a 3rd party entity? While it’s common to use a 3rd party entity to test your submission in advance, this is distinctly different from actually receiving the stamp of approval from NIST.
4. Do the containerized components that make up the Kubernetes platform take advantage of the FIPS validated crypto or do they bypass it? If your Kubernetes distribution is claiming to be FIPS compliant, but critical components such as the Kubernetes Ingress are not for example, this is much like leaving the front door open.
5. Do the parts that round out a production Kubernetes platform correctly operate with FIPS enabled (ie Istio, etc)? Taking your Kubernetes cluster through an ATO can quickly be halted by the discovery that key workloads you plan to run do not work on top of a FIPS enabled cluster.
6. Does the Kubernetes platform support enabling FIPS mode for user workloads running in Kubernetes Pods, in addition to hosts?

Red Hat is unique in our commitment to answer a **resounding yes** to all of these questions in the delivery of OpenShift Container Platform. We believe in delivering a more secure Kubernetes platform for public sector organizations and choose to own this process rather than outsource and rely on others. Moreover, Red Hat’s unique technical approach integrates FIPS into the host Red Hat Enterprise Linux CoreOS platform, allowing delegation of all cryptographic functions of containerized components and user workloads. With Red Hat OpenShift, customers can more quickly and easily install in a multitude of environments with FIPS enabled to make a FIPS compliant platform in support of government compliance requirements.

MORE CHOICES FOR GOVERNMENT

Red Hat OpenShift 4.6 introduces automation purpose built to support the major public cloud government regions including AWS GovCloud and Microsoft Azure Government. This includes native integration with cloud provider services like network, storage, compute for auto-scaling and more. AWS GovCloud and Microsoft Azure Government are now integral to the engineering and QA process for OpenShift, meaning every release is validated for government cloud compatibility. This makes OpenShift a faster and easier way to stand up a “CNCF Kubernetes Conformance Program” certified distribution in a government cloud.

EXPANDING OPENSHIFT TO THE EDGE

Red Hat OpenShift 4.6 also brings support for full stack automation (IPI) of deployments to bare-metal hosts, expanding the possibilities for OpenShift in government use cases like HPC or edge computing. Bare metal significantly increases deployment options while maximizing performance benefits of customer hardware. An IPI installation of Red Hat OpenShift means you can quickly and easily have a supported cluster up and running on your own hardware – an experience that doesn’t require a public cloud provider. This makes it easier to integrate Red Hat OpenShift within your existing investments and processes, reducing risk and accelerating adoption.

This release enhances customer choice when deploying clusters, adding to the existing supported 3-node clusters that combine worker nodes with control plane nodes. Additionally, single node instances are on the roadmap for Red Hat OpenShift Container Platform.

Government networks traditionally span multiple locations that have varying bandwidth and connectivity. Through the lens of Kubernetes, this imposes a unique challenge as worker nodes must report status to the control plane frequently to ensure the desired cluster state is met. Furthermore, edge workloads tend to be constrained by size and therefore compute capacity. In those cases, we traditionally recommend a Red Hat Enterprise Linux + Podman + systemd approach, and when a management layer isn’t necessary, such an approach is optimal. This does however pose some challenges in how a system is managed as part of a fleet.

With our 4.6 release of Red Hat OpenShift, we’re now supporting remote worker nodes. This means a Red Hat OpenShift cluster can maintain its control plane in a highly available configuration somewhere centrally

located with predictable connectivity, while still managing worker nodes deployed at sites where network outages may occur. Rather than terminate workloads when a worker can no longer reach the control plane, an administrator can configure disruption tolerances that suit the environmental constraints and keep the applications and the mission running by significantly reducing the time-to-recovery when connectivity is restored.

OPENSHIFT COMPLIANCE OPERATOR

The OpenSCAP project provides tools for automated vulnerability checking, and has long been a staple in the Federal space for ensuring compliance of RHEL systems. Center for Internet Security (CIS) has also published guidance for Kubernetes with the CIS Kubernetes Benchmark. With Red Hat OpenShift 4.6, we’ve made it easier for customers to perform their compliance scans of the Red Hat OpenShift cluster by creating the Red Hat OpenShift Compliance Operator. The compliance-operator is an Red Hat OpenShift Operator that allows an administrator to run compliance scans and provide remediations for the issues found. The operator leverages OpenSCAP and CIS Kubernetes Benchmark under the hood to perform the scans. The Red Hat Compliance Operator accepts a declarative configuration created by administrators that can be stored in version control. The configuration is then used to scan the Red Hat OpenShift hosts, store the scan results, and if desired, remediate the hosts to be in compliance with the desired configuration.

IPV6

The United States Office of Management and Budget (OMB) have laid out guidelines and timelines for transitioning Federal Government networks from IPv4 to IPv6. With the ever increasing number of connected devices and web based application services, this is a necessary change to ensure IP space is available to meet mission requirements. Red Hat OpenShift Container Platform 4 offers two current options to meet this mandate today. Using a bare metal installation strategy, customers can deploy clusters that use IPv6 exclusively, or deploy with a secondary interface to achieve both IPv4 and IPv6 dual stack based communication. Additionally, Red Hat engineering has been working diligently upstream to extend the capabilities of the OVN (Open Virtual Networking) project to further enhance the software defined network capabilities that Red Hat OpenShift Container Platform offers our customers today.

EXTENDED UPDATE SUPPORT

Kubernetes, the upstream project which is at the core of OpenShift, historically releases roughly every 90 days. This is a difficult cadence for our enterprise customers to consume, and particularly our federal customers due to the time and effort it takes to accredit a federal system. Furthermore, the community typically does not maintain older releases, meaning security patches may not be available unless customers are on a newer release. Given the criticality of the mission workloads we support in federal, this represents a significant barrier to adoption for Kubernetes in the government space.

Red Hat has a history of easing the transitions between releases by supporting customers with long software lifecycles, providing security patches and bug fixes to products long after their open source project lifespan. This enables customers to maintain stability in their IT environments. Red Hat OpenShift 4.6 is the first Extended Update Support (EUS) release of Red Hat OpenShift 4. This comes with a lengthy 18 months of support taking systems out to March of 2022. This EUS version is intentionally aligned to the Red Hat Enterprise Linux 8.2 release. Additionally with this EUS release comes a guaranteed version of components that run on Red Hat OpenShift that are critical to a holistic container adoption. Red Hat provides a vendor supported full stack, giving you the fundamental tools you need to operationalize Kubernetes out of the box, including:

- Red Hat OpenShift Serverless
- Red Hat OpenShift Pipelines
- Red Hat OpenShift Service Mesh
- Red Hat OpenShift Logging
- Red Hat OpenShift Container Storage
- Red Hat Advanced Cluster Management for Kubernetes

OPENSHIFT DISCONNECTED UPDATE SERVICE

When government customers run sensitive workloads, regulations and security requirements mandate that application platforms be deployed in a disconnected, or air gapped network enclave. This poses a unique challenge for maintaining software updates in critical systems. With the 4.6 release we’ve added the ability to host the same update service that connected clusters use to determine what updates are applicable. For a connected cluster, this is normally a service hosted by Red Hat. With 4.6, customers can host this service on-prem, or alongside an air-gapped cluster in a local registry. Once the OpenShift Update Service is up and running on-premise, the disconnected clusters will receive an update notification in the OpenShift web console whenever an update is made available and can be applied to the cluster with the click of a button.

CONCLUSION

Our Public Sector customers run some of the most mission critical workloads in the world, and their unique requirements help set the standard for security and compliance. For OpenShift version 4.6, Red Hat has focused on features and functionality that support the use cases of our government customers, such as integration with government clouds, Edge computing, and disconnected environments. That’s why we’re calling the 4.6 release of Red Hat OpenShift Container Platform the “Kubernetes Platform for Government”. Red Hat OpenShift Container Platform 4 is the only fully automated, full-stack Kubernetes experience available today. This release enables government agencies adopting a DevSecOps transformation to build on a solid base of government-ready defaults, removing the heavy lifting required to meet a lot of government compliance requirements, and freeing teams to focus on delivering the solutions that bring real business value to their mission customers.