STONE DOOR GROUP

OpenShift security drives enterprise IT to adopt Linux containers

Mike McDonough, Hybrid Cloud Architect
@MikeMcDTN

Published May 2019

ABSTRACT

OpenShift offers an industry leading set of features to integrate Linux containers into an Enterprise IT environment. The OpenShift platform is built on a solid and secure foundation comprised of technologies like Linux containers, RHEL, and Kubernetes. It provides the tools and capabilities required to ensure container integrity, the key requirement for container security, enabling Enterprise IT organizations to adopt Linux containers quickly compared to in-house developed container solutions.

INTRODUCTION

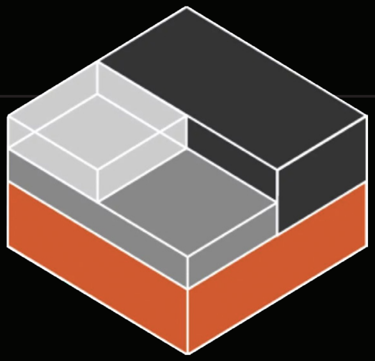
Red Hat's OpenShift container application platform is accelerating Linux container adoption because it specifically addresses the needs of enterprise IT organizations.

Up until recently, IT teams had to build numerous custom solutions on top of containers so that they could be used effectively in large scale, production environments. Those solutions were resource- and time- intensive to create and support. It was also problematic for IT security as they did not provide a standardized or validated answer for container security. While mega-scale cloud hosting providers had the resources to make containers work, the approach was not viable for the majority of businesses.

With OpenShift, containers are ready for any enterprise. The OpenShift platform builds on the secure foundation provided by Linux containers. It enables IT teams to manage containers at scale, while providing the controls and visibility required by large organizations. Built on the very best open source projects, the OpenShift platform is tested and validated for use in production environments. Untested, home-brewed container solutions are no longer the only option for organizations wanting to scale. As you read on, you will see how OpenShift empowers any organization to deploy containers securely, and in ways that support both your current investments and future strategies.

BACKGROUND

Operating system (OS)-level virtualization (aka containers) has been widely available for nearly 20 years. FreeBSD 4.0 included this capability with its "jail" mechanism in March 2000. Solaris Containers was released to the public in 2004 with a beta build of Solaris 10. Linux Containers (LXC) brought the first, complete container implementation to Linux in 2008.



Though these technologies succeeded in virtualizing the OS, they were not widely adopted in mainstream IT organizations because they lacked key features and capabilities required to integrate containerization into enterprise IT environments.

In 2014, Google's release of Kubernetes, an open-source container orchestration system, added a tremendous amount of functionality to Linux containers as now containerized applications could be deployed, scaled, and managed. However, enterprise IT adoption of Linux containers still faced major hurdles as Kubernetes and Linux containers did not fully address key requirements from enterprise IT security.

Linux containers provided application isolation but did not address security concerns that are created by eliminating many of the physical and virtualized hardware boundaries which used to be the basis for security domains. With containers, servers and even virtual machines can no longer be used to easily identify access and control points. Instead, a more nuanced view on securing applications, and the enterprise, is required.

The Solution - OpenShift Container Platform

OpenShift provides a robust, productized Linux application container platform with a rich feature set based on the needs of Enterprise IT.

HARDENED AND TESTED

OpenShift provides a comprehensive and cohesive container solution built around hardened and tested versions of leading open source software. It addresses functional requirements from development and IT operations teams, while meeting the needs of Enterprise IT Security teams. For this reason, OpenShift has achieved a reputation of being the solution security-minded organizations rely on to manage business-critical applications.

Container security should be thought of in terms of container integrity. Unlike bare metal servers or virtual machines, real or virtual hardware separation is not the basis for Linux container security.

OpenShift helps ensure container integrity by answering these three key questions:

- Is the container hosting environment secure?
- What content (application) is running in the container?
- Does the container platform integrate with Enterprise IT controls, processes, services, and systems?

RED HAT® OPENSHIFT® Container Platform

SECURE OPERATING ENVIRONMENT

All of the software which makes up the OpenShift platform is tested and supported by Red Hat, the world's leading provider of open-source solutions. Red Hat conducts functional, performance, and security vulnerability testing to ensure that OpenShift meets enterprise IT requirements. If a security issue is identified in an upstream project, Red Hat will evaluate the issue, notify OpenShift customers, and make the appropriate updated software available.

Components and services which make up the OpenShift platform are configured securely by default. The bundled Certificate Authority enables services to leverage HTTPS for network traffic encryption by default. User logins to the OpenShift platform are granted minimal permissions. OpenShift services run inside containers on the host systems, bringing the security advantages of containers to the platform itself.

OpenShift runs on Red Hat Enterprise Linux (RHEL) which supplies a robust and secure foundation for the platform, as depicted in Figure 1. Furthermore, OpenShift is designed to work with a secure RHEL configuration. Security-Enhanced Linux (SELinux) mode must be enabled on each RHEL host running OpenShift. SELinux enforces access control security policies, including mandatory access controls (MAC). MAC helps protects the system from attackers or flawed applications. Seccomp is also supported, allowing administrators to limit syscalls on a host or container basis.

OpenShift increases the security provided by Linux containers by allowing administrators to further control permissions granted to containers at a fine-grained level. OpenShift Security Context Constraints (SCC) limit container actions and access to resources. SCCs allow administrators to control conditions such as running of privileged containers, SELinux context of the container, user ID, and capabilities that can be requested.

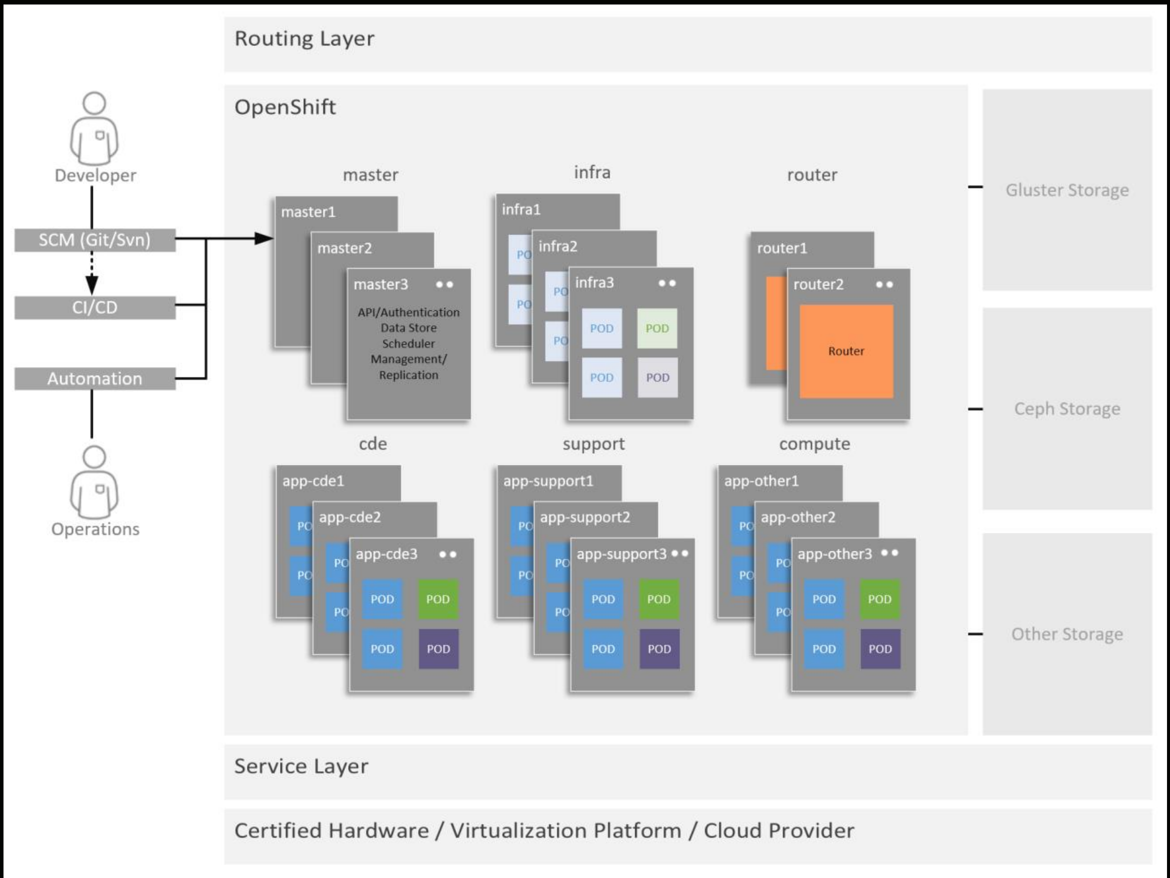


Figure 1 - Core OpenShift Architecture

SECURE CONTAINER CONTENT

Red Hat OpenShift has multiple options for secure container content starting with the Red Hat Container Catalog. Red Hat's Container Catalog offers certified, trusted container images which greatly minimize the risk of consuming content from outside an organization. Red Hat's Container Catalog helps enterprise organizations leverage popular technologies such as Java and Node JS without the danger of downloading content from public registries. The Catalog features both open source and commercially licensed software.

Many organizations will want to conduct additional scanning and verification of container content to ensure that the container image or content does not contain software which is vulnerable to attack. To meet this requirement, OpenShift supports content and image scanning at multiple points in the container lifecycle process.

Container images in OpenShift's internal container image registry can be scanned using the OpenSCAP scanner capabilities in Red Hat CloudForms. Alternatively, OpenShift can be configured to utilize an external container registry with built-in scanning capabilities, such as Red Hat Quay. Quay provides for static analysis of vulnerabilities in containers. Third party container registries are also supported, enabling OpenShift to integrate with Artifactory, Nexus, or registries offered by popular cloud hosting providers (e.g. Amazon, Azure, and Google.)

OpenShift's bundled container image registry can be utilized as the primary storage location for container images or it can function as a cache for container images to help lower container startup time. In either case, OpenShift's image verification capabilities based on digital signatures of images can be utilized to validate image integrity and provide non-repudiation. Using the Image Policy Admission Plug-in, policies can be set to allow only images from known, trusted sources with a valid digital signature to run on the OpenShift platform.

INTEGRATION WITH ENTERPRISE IT

Change control management is a vital process for both IT and quality management. OpenShift is built around the premise of "infrastructure as code" (IaC). With IaC, infrastructure definition and configuration can go through the same process as application code, including version control and automated testing. IaC facilitates control and auditing of environments. When fully implemented, it can eliminate "configuration drift" helping ensure application and platform configurations don't deviate from IT Security baselines.

OpenShift supports integration with enterprise identity services including LDAP, Google, and OpenID for user authentication. Projects are the primary vehicle for controlling access to resources by users. Projects build on Kubernetes namespaces, providing content, container, and even network isolation between communities of users. A role based access control (RBAC) framework handles authorization decisions for all OpenShift API requests, including project access. OpenShift's RBAC framework can be configured at a fine grained, per project basis, enabling organizations to effectively implement access based on the principle of least privilege (PoLP).

Application delivery is only as secure as the network that delivers it and its data. As Figure 2 shows, containers running on OpenShift communicate over a Software Defined Network (SDN). Multiple SDN plug-in's are available: ovs-subnet (flat network between pods), ovs-multitenant (network isolation between namespaces), or ovs- network policy (policy controlled network traffic between pods).

Third party SDN plug-ins (Flannel, Nuage, Kuryr) can also be utilized. OpenShift administrators are able to change container network traffic behavior to meet IT security requirements by simply specifying the appropriate SDN plug-in.

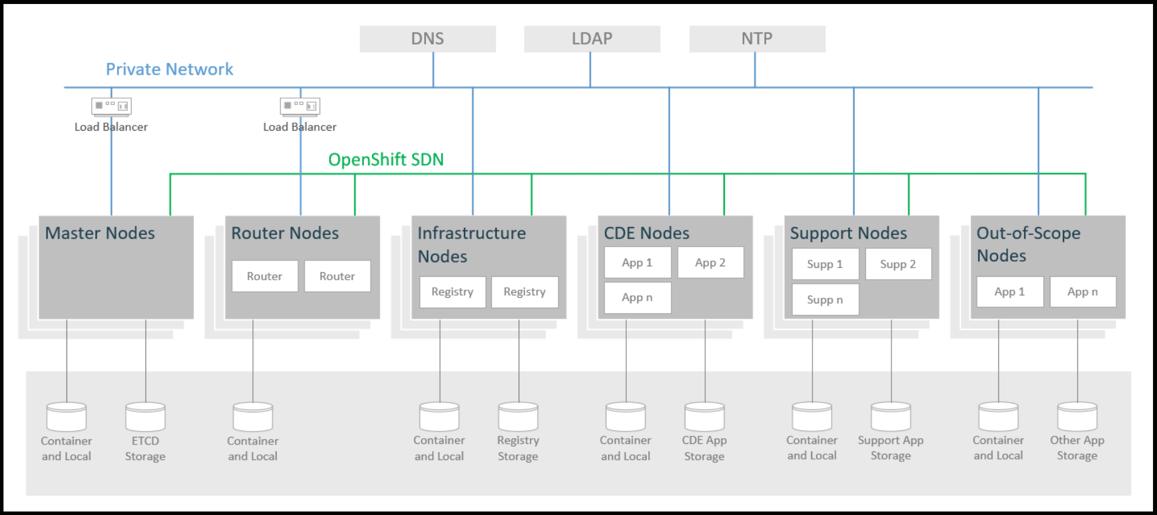


Figure 2 - High-level OpenShift Network Topology

OpenShift includes the flexible and scalable Elasticsearch, Fluentd, and Kibana (EFK) stack to provide centralized logging and analytics functions. The EFK stack processes log messages from all OpenShift components, along with log messages from applications running in containers. OpenShift can forward log messages to 3rd party, external logging platforms like Splunk via the industry standard syslog protocol. Logging data can also be sent to external Elasticsearch services.

ABOUT THE AUTHOR

Mike McDonough | Hybrid Cloud Architect, Stone Door Group

Mr. McDonough consults with enterprise IT organizations on advanced infrastructure and information security topics with a focus on cloud technology and emerging technology. He has helped businesses across a wide range of industries, including alternative energy, finance, retail, and travel, successfully implement Red Hat's OpenShift container application platform.

ABOUT STONE DOOR GROUP

SDG is a certified solutions integrator that bridges the implementation gap between the world's leading technology providers and enterprises needing to transform their applications, infrastructure, and people to DevOps best practices. Stone Door provides a fully-integrated managed service, including consulting, license reselling, cloud hosting, and training. Online at www.stonedoorgroup.com.

SDG is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards. Consequently, any forward-looking statements are not predictions and are subject to change without notice. While SDG has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, SDG is not responsible for any errors or omissions, or for the results obtained from the use of this information. SDG reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.