Kubernetes for the public sector

Red Hat OpenShift and evolved security and compliance for Kubernetes

A zero-trust approach to Kubernetes infrastructure

In five years of running and supporting Kubernetes workloads in production, Red Hat has learned three very important lessons. First, defaults have inertia, meaning many of the settings used on day one will find their way into production. Second, reducing complexity is key to security. There are thousands of flag permutations to be set in Kubernetes. Studies show that most security breaches are tied to end-user configuration changes.[1] Reducing cognitive overhead is critical to a good security practice. Finally, good ops is good security. When every machine is unique, the level of system complexity grows and increases the potential for human error. Once we reduce complexity, we can automate and scale.

Red Hat has made a conscious effort to improve Red Hat® OpenShift® Container Platform in response to these lessons. This datasheet focuses on two important considerations, our approach to Federal Information Processing Standards (FIPS) validation and our strategic move to develop Red Hat Enterprise Linux® CoreOS.

Red Hat Enterprise Linux CoreOS: Kubernetes-managed operating system

Red Hat Enterprise Linux CoreOS is a specialized distribution of Red Hat Enterprise Linux, optimized for running Linux containers on Kubernetes. Red Hat Enterprise Linux CoreOS is an optimal container host: minimal system usage, more secure, less mutable, up-to-date, and fully managed. Because it is based on Red Hat Enterprise Linux, Red Hat Enterprise Linux CoreOS inherits a mature, comprehensive delivery and support model with a robust ecosystem. Red Hat Enterprise Linux CoreOS is not a standalone operating system, but rather a component of Red Hat OpenShift distributions.

Minimal

Red Hat Enterprise Linux CoreOS contains only what is required to run Linux containers on Kubernetes, and removes Red Hat Enterprise Linux platform components that are unnecessary for that purpose. Additional operating system and application services can only run as isolated, containerized workloads. This allows the host to be largely read-only, locked-down, and to start only a minimal set of system services.

Less mutable and more secure

Red Hat Enterprise Linux CoreOS is a downstream distribution of Red Hat Enterprise Linux and a host OS that meets the guidelines of National Institute of Standards and Technology (NIST) Special Publication 800-190 to reduce the attack surfaces for a container platform. Specifically, NIST 800-190 states, "a container-specific host OS is a minimalist OS explicitly designed to only run containers, with all other services and functionality disabled and with read-only file systems and other hardening practices employed."[2] As part of OpenShift, the use of Red Hat Enterprise Linux CoreOS has allowed Red Hat to deliver this recommended, highly secure model.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

1 *Panetta, Kasey. "Is the cloud secure?" Gartner, Oct. 2020.*

2 *Souppaya, Murugiah, John Morello, and Karen Scarfone. "NIST Special Publication 800-190: Application Container Security Guide," National Institute of Standards and Technology, Sept. 2017.*

Red Hat Enterprise Linux CoreOS is designed to prevent out-of-band changes that might affect application behavior and security from persisting across node restarts. The installation and boot processes use installer-generated, declarative configuration to bootstrap the operating system to a cryptographically verifiable, known-good state. The initial state mounts /usr as read-only to prevent runtime modification of the system binaries, while kernel-based container isolation of applications and services using technologies like SELinux and cgroups prevents application changes from modifying the operating system. All persistent operating system modifications of Red Hat Enterprise Linux CoreOS must be made through role-based access control (RBAC), protected application programming interfaces (APIs), or redeployment of the hosts via the same verifiable ignition processes.

Up-to-date and fully managed

Red Hat OpenShift Container Platform version 4 incorporates Red Hat Enterprise Linux CoreOS as a streamlined platform for automated operations of the underlying host operating system. Red Hat Enterprise Linux CoreOS is coupled to OpenShift Container Platform by design, so you can manage and automate the deployment of underlying container hosts. This includes node configuration and deployment, automated OS upgrades, and updates across clusters, as well as other configurations driven from Kubernetes operators and Kubernetes custom resource definitions (CRDs).

When you set up your Red Hat Enterprise Linux CoreOS hosts, you can only modify some of the system settings. This controlled immutability allows OpenShift Container Platform to store the latest state of Red Hat Enterprise Linux CoreOS systems in the cluster, so it is always able to create additional machines and perform updates based on the latest Red Hat Enterprise Linux CoreOS configurations. Updates are delivered via container images and are part of the Red Hat OpenShift update process. When deployed, the container image is pulled, extracted, and written to disk, and the bootloader is modified to boot into the new version. The machine will reboot with rolling updates to ensure cluster capacity is minimally impacted.

Supported security standards and compliance

Red Hat Enterprise Linux CoreOS supports important security standards such as FIPS-enabled Linux to ensure OpenShift Container Platform can meet government regulation requirements, which simplifies support and reduces risk. Red Hat is committed to delivering a secure Kubernetes platform for any public sector organization. Red Hat tests the Red Hat Enterprise Linux CoreOS platform with NIST-validated FIPS cryptographic modules with every release, which helps ensure compatibility and resiliency. Moreover, Red Hat's technical approach integrates FIPS into the host Red Hat Enterprise Linux CoreOS platform, allowing you to delegate cryptographic functions of containerized components and user workloads.

In summary

Red Hat OpenShift delivers the right model at the right time as government agencies aggressively move mission-critical workloads to Kubernetes. Red Hat Enterprise Linux CoreOS delivers all of the characteristics required to deliver a more secure, resilient, and scalable infrastructure for Kubernetes. Our FIPS approach is comprehensive enough to satisfy the security requirements of public sector organizations and agencies.

2 *Refer to the latest Red Hat OpenShift Container Storage 4 release notes for supported platforms.*

Common questions and misconceptions

Why didn't Red Hat OpenShift 4 continue using Red Hat Enterprise Linux for all hosts?

- Red Hat determined that Red Hat Enterprise Linux CoreOS delivered a better model for hosts than Red Hat Enterprise Linux. We reviewed support cases, all possible permutations of flags and labels, human error, and other factors that were part of configuring Red Hat Enterprise Linux for OpenShift. We removed these unknowns by making the OS an implementation detail of the cluster itself.

How can I take advantage of the strengths of Red Hat Enterprise Linux in the accreditation process?

- It is critical to achieve accreditation for the entire platform instead of treating the operating system as a separate entity. Red Hat Enterprise Linux CoreOS is based on Red Hat Enterprise Linux and contains fewer packages that can be exploited. The OS is embedded in, synchronized with, and operated by the Kubernetes platform.
- Even though OpenShift and Red Hat Enterprise Linux CoreOS are coupled, Red Hat Enterprise Linux CoreOS uses the same basic constructs as Red Hat Enterprise Linux and is based on the same kernel, packages, configuration items, and other implementation details. System administrators and security teams (ISSOs and ISSMs) are already familiar with these components.

How can I use traditional security tools on Red Hat Enterprise Linux CoreOS, such as antivirus and scanning software?

- If malware scanners are required beyond those delivered in Red Hat OpenShift, vendors that support Kubernetes and cloud platforms are recommended to support you in meeting this requirement. Red Hat Enterprise Linux CoreOS incorporates alternative tools for malware prevention.
- OpenShift Container Platform 4.6 and later versions include the file integrity operator which uses Advanced Intrusion Detection Environment (AIDE), a utility that creates a database of file hashes on the system and then uses that database to detect and generate alerts on file integrity and system intrusions.
- Where traditional tools are strictly required, Red Hat Enterprise Linux CoreOS may support these as container- or cloud-based services. For example, virus scanners may run as privileged containers with access to the underlying platform. Scans of static content may also be performed out-of-band on specialized services such as an external container registry or isolated physical host.
  - Red Hat is working with its extensive hosted software vendor and independent software vendor (HSV/ISV) ecosystem to adapt third-party tools to use within Red Hat Enterprise Linux CoreOS as parts of the trusted core operating system or as container-based payloads that can be isolated and managed by the platform.

Why do Red Hat Enterprise Linux CoreOS and Red Hat Enterprise Linux have different support life cycles?

- Red Hat Enterprise Linux CoreOS is not a standalone operating system and is not intended to be used outside of OpenShift Container Platform. It is part of Red Hat OpenShift and shares the support life cycle of that product.
- Sharing the Red Hat OpenShift life cycle makes it easier to apply up-to-date common vulnerabilities and exposures (CVE) fixes. CVE fixes are delivered in Red Hat OpenShift z-stream releases.
- Red Hat Enterprise Linux CoreOS provides a short but well-defined life cycle to encourage good security practices for patching and updating while decreasing costs associated with maintenance and operations. It fosters use of continuous security processes and compliance regimes and eliminates risks associated with use of older software components.

How can I use custom "gold images" that provide my agency with required security add-ons?

- The MachineConfigs in Red Hat Enterprise Linux CoreOS are API objects that serve as a gold image equivalent but provide more repeatability as the operating system is patched and updated. By encoding these MachineConfigs in compliance baselines for common security standards such as NIST 800-53, Red Hat can provide the equivalent of a gold image for these baselines that users do not need to maintain independently.

Why doesn't Red Hat Enterprise Linux CoreOS include certain packages needed for certification?

- Red Hat Enterprise Linux CoreOS minimizes the attack surface and the potential vulnerabilities present by reducing the base set of packages to the bare essentials. If a package is not required to optimally run Linux containers on Kubernetes, then it is not present. If needed, additional packages can be used via container-based payloads that can be isolated and managed by the platform.
- Certification and accreditation for Red Hat Enterprise Linux CoreOS should only be considered in the context of larger systems which include the payloads, external monitoring and auditing, and other components needed to provide security assurances. These packages and associated capabilities can be made available.

How do I accredit Red Hat Enterprise Linux CoreOS?

- Red Hat Enterprise Linux CoreOS should be managed and accredited as part of Red Hat OpenShift. Assessors should rely on the vendor assertions, security state, and management life cycle.
- Red Hat Enterprise Linux CoreOS is not a general purpose operating system like Red Hat Enterprise Linux, but rather a subset of Red Hat Enterprise Linux, and should not require the same controls for user access and life-cycle management as a general purpose operating system.

What if security requires a backdoor for scanning or remediations, such as an SSH key left on the system?

- Red Hat Enterprise Linux CoreOS uses a cloud-native, zero-trust security model and considers any uncontrolled or unmanaged access as a potential vulnerability. The preferred approach to making updates more repeatable across the entire cluster is to use APIs and RBAC. This approach helps prevent one-off or out-of-band changes that often result in configuration drift. Red Hat's vendor support will remediate issues by issuing new releases that replace existing systems.
- Additionally, OpenShift Compliance Operator automates compliance scanning and remediation, eliminating the need for SSH or other scanning backdoors. OpenShift Compliance Operator uses standard Kubernetes and OpenShift APIs, accessed via RBAC controls, to execute scans of Red Hat Enterprise Linux CoreOS nodes against provided security content automation protocol (SCAP) baselines. It can optionally remediate certain compliance violations using MachineConfigs and the MachineConfig operator.

The bottom line

In order to reap the benefits of moving to a Kubernetes platform like Red Hat OpenShift, organizations must embrace technical approaches that focus on security from the start and are aligned with Kubernetes and Linux containers. Red Hat Enterprise Linux CoreOS is not a general purpose operating system and is not available outside of Red Hat OpenShift. It provides only what is necessary to optimally run Kubernetes and containers and to be managed along with the platform. It is more secure by default and prevents the type of access that made earlier systems vulnerable.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#F26269_1220

Copyright © 2020 Red Hat, Inc. Red Hat, the Red Hat logo, and OpenShift are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.