

UNCLASSIFIED



RED HAT OPENSIFT CONTAINER PLATFORM 4.12 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 2, Release 1

24 July 2024

Developed by Red Hat and DISA for the DOD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION	1
1.1 Executive Summary.....	1
1.2 Authority.....	1
1.3 Vulnerability Severity Category Code Definitions	1
1.4 STIG Distribution.....	2
1.5 SRG Compliance Reporting	2
1.6 Document Revisions	2
1.7 Other Considerations	2
1.8 Product Approval Disclaimer	3
2. ASSESSMENT CONSIDERATIONS	4
2.1 Security Assessment Information - Applicability.....	4
2.2 Security Assessment Information – Compliance Operator	4
2.3 Security Assessment Information - OC Client and Client Tools	5
2.4 Security Assessment Information – External Identity and Access Management.....	5
2.5 Security Assessment Information – External Central Logging	6
2.6 Security Assessment Information – Advanced Cluster Security	7
3. CONCEPTS AND TERMINOLOGY CONVENTIONS	8
3.1 OpenShift Container Platform Overview	8
3.2 OpenShift Container Platform Components	8
3.3 Linux Containers	10
3.4 Red Hat CoreOS	11
4. GENERAL SECURITY REQUIREMENTS.....	13
4.1 Hardening of Integrated External Services	13
4.2 Content Sources: API Object Sources, Code Repositories, Container Image Repositories...	13
4.3 Disaster Recovery and Continuity of Operations.....	13

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2

LIST OF FIGURES

	Page
Figure 3-1: The OpenShift Control Plane Components, Including Primary Control Plane Services..	9
Figure 3-2: The OpenShift Worker Components	10
Figure 3-3: OpenShift’s Primary Container Engine Components	11

1. INTRODUCTION

1.1 Executive Summary

The Red Hat OpenShift Container Platform 4.12 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DOD) information systems. This document is meant for use in conjunction with other STIGs and SRGs, such as the AAA SRG, Central Log Server SRG, Network Infrastructure Policy STIG, and other appropriate SRGs and STIGs.

This STIG applies to the Red Hat product OpenShift version 4.12. It assumes this product is installed and configured in accordance with the documented installation instructions provided by Red Hat. This STIG also assumes delegation of certain security control implementation to external, integrated enterprise systems, including a central identity and access management system, central logging management system, and others as noted below.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that “all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be [...] configured [...] consistent with applicable DOD cybersecurity policies, standards, and architectures.” The instruction tasks that DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at <https://cyber.mil/>. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from <https://public.cyber.mil/>.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA

implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (<https://www.niap-ccevs.org/>) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<https://csrc.nist.gov/groups/STM/cmvp/>) IAW federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (<https://www.disa.mil/network-services/ucco>) IAW DODI 8100.04.

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information - Applicability

This STIG is not intended to provide technical guidance for all portions of the OpenShift Container Platform 4.x. The OpenShift Container Platform is a complex software system, and this STIG is applicable only to:

- A subset of the potential set of components available for use in and with the OpenShift Container Platform; all applicable subcomponents are part of default installation per the installation instructions provided with the platform.
- The x86 instruction set/CPU architectures supported by the OpenShift Container Platform.
- OCP installations that use Red Hat CoreOS as the underlying operating system.

Users of OpenShift Container Platform may apply this STIG in deployment scenarios outside the scopes noted above with appropriate tailoring. For users that use additional, optional, third-party, or other system components that are not provided by a default installation of the OpenShift Container Platform, it is possible the efficacy of the controls provided by this STIG could be affected by these components. Security assessors should inventory these components and perform an impact assessment of each and apply any security controls required by these components.

For users that deploy or operate OpenShift Container Platform on alternative instruction set/CPU architectures supported by the OpenShift Container Platform such as IBM Z-series, ARM, or others, security assessors should evaluate the impact on controls that depend on underlying kernel and machine configuration parameters.

For users that deploy or operate OpenShift Container Platform on mixed-host operating systems where worker nodes are based on the RHEL general purpose operating system in lieu of Red Hat CoreOS, these worker nodes should be independently assessed against the relevant STIG for the RHEL operating system.

This STIG does not apply directly to tenant applications, although it may affect the security posture of these tenants, limit their configuration and usage, or provide implemented security controls to these tenants. Security assessors should inventory these tenants and perform an impact assessment of each and apply any security controls required by these components.

2.2 Security Assessment Information – Compliance Operator

The OpenShift Container Platform provides a Compliance Operator as an auxiliary component that may be optionally installed and configured by system administrators. The Compliance Operator allows OpenShift Container Platform administrators to describe the required compliance state of a cluster and provides them with an overview of gaps and options to remediate them. It is recommended that system administrators use this compliance operator to assist correct application of controls provided in this STIG. More information about the OpenShift Container Platform Compliance Operator can be found in Red Hat's OpenShift documentation at https://docs.openshift.com/container-platform/4.12/security/compliance_operator/compliance-operator-release-notes.html. Additional information about operators may be found in Red Hat's

OpenShift documentation at <https://docs.OpenShift.com/container-platform/4.12/operators/index.html>.

This STIG was tested and developed using both manual application of the included security controls and automated means as applied via the OpenShift Container Platform Compliance Operator. While recommended, the use of the compliance operator is not strictly required. System owners may opt to apply this STIG using either process and will achieve comparable results. Users should refer to the OpenShift Container Platform Compliance Operator for instructions on use of this facility.

2.3 Security Assessment Information - OC Client and Client Tools

The OpenShift Container Platform's primary control mechanism is via an application programming interface (API), which can be interacted with several ways and typically through either the platform's internal web console component or command line tools. Red Hat provides a dedicated command line interface tool, commonly known as "oc," which allows system administrators and users to query, modify, update, and delete API objects and other common functions, including complex multistep processes or integrating with client-local, cluster-remote, or system-external resources. More information about the OpenShift Container Platform command line tools, including the oc client, can be found in Red Hat's OpenShift documentation at https://docs.OpenShift.com/container-platform/4.12/cli_reference/index.html.

This STIG uses a command line tool to interact with OpenShift Container Platform via its API, and multiple requirement checks and fixes are implemented via use of the oc CLI tool. In most cases, the use of the CLI tool is optional and an alternative means to interact with the system is available (web console, OpenShift Container Platform Compliance Operator, Red Hat Advanced Cluster Manager, ansible roles and extensions, alternative API tools). System Administrators may opt to use these alternative tools in appropriate settings; for example, when managing multiple instances of the OpenShift Container Platform in a consistent fashion. This STIG was written and tested using the oc CLI as the primary means of interacting with the OpenShift Container Platform API.

2.4 Security Assessment Information – External Identity and Access Management

This STIG delegates certain security controls to an external Identity and Access Management system; delegated controls are out of scope of this STIG. Security controls in this STIG ensure the correct integration of this external system, but thereafter rely on the security capabilities of this system. The Identity and Access Management system that OpenShift Container Platform 4.x integrates with must provide the following capabilities:

- Identification of temporary or inactive users: Users that have not logged into the OpenShift Container Platform within a designated, organizationally defined period must be identified by the external Identity and Access Management system, and organizationally defined remedial actions must be taken.
- Auditing of user accounts: Users with access to the OpenShift Container Platform must be audited via the external Identity and Access Management system for creation of new accounts, modification of existing accounts, or deletion/removal of user accounts.

- Enforcement of invalid login attempt limits: User attempts to log in to the OpenShift Container Platform that fail must be handled by the external Identity and Access Management system, and organizationally defined remedial actions must be taken.
- Notice and consent: The external Identity and Access Management system must present all users accessing the OpenShift Container Platform with organizationally defined notice and consent notices on login events and deny access if the notice and consent is not accepted by the user.
- Multifactor Authentication: The external Identity and Access Management system must require all users accessing the OpenShift Container Platform in normal operations (except as DR and COOP processes require) to present multiple, independent authentication factors, verify these factors, and deny access if any factors are not deemed verified in accordance with organizationally defined policy.
- Password Policy Enforcement: The external Identity and Access Management system must enforce organizationally defined password usage policies including the reuse of passwords, minimum length requirements, and complexity requirements.
- PKI user identity mapping: The external Identity and Access Management system must map the authenticated identity extracted from a user's PKI certification credential to the individual user or group account provided during PKI-based authentication to the OpenShift Container Platform.
- (SSH) Key management: The OpenShift Container Platform requires initial configuration of nodes via SSH. This STIG may require the creation and use of SSH keys as an underlying function of certain privileged operations using the oc debug CLI. Under these conditions, the execution environment for these operations must protect these keys. In cases where SSH keys are used, appropriate organizationally defined key management must be employed to protect or control use of these keys.
- Role and Privilege Changes: When device, host, user, or other roles or security-relevant attributes change, the external Identity and Access Management system must remove, delete, or render inoperable all associated and currently active authorizations to the OpenShift Container Platform.

The product allows the use of several supported providers including Active Directory, LDAP, and others. This STIG was tested and validated using the Keycloak open-source single sign-on application and its internal identity provider via the OpenShift Container Platform's OIDC provider.

2.5 Security Assessment Information – External Central Logging

This STIG delegates certain security controls to an external Log Collector and Management system; delegated controls are out of scope of this STIG. Security controls in this STIG ensure the correct integration of this external system but thereafter rely on the security capabilities of this system. Security Assessors should ensure the choice of Log Collector and Management system that OpenShift Container Platform 4.x is integrated with provide the following capabilities:

- Log Access: The external central logging provider must provide access controls and services for appropriate users to search, locate, and recover logs, log metadata, and activity records. The OpenShift Container Platform produces log and audit information based on its operations, and the external log system must be configured to parse and process the log

records produced by the controller for effective investigation of security exceptions, diagnostics, incident response, or other events.

- **Log retention:** The external central logging provider must retain access, activity, and audit logs per organizationally defined policy. This STIG and the OpenShift Container Platform provide for limited system-based log retention, but system-based storage or other resource limits associated with the OpenShift Container Platform may be insufficient to maintain sufficient log or audit records that central logging systems are equipped to retain.
- **Notification of failure:** The external central logging provider must notify log administrators under organizationally defined failure conditions. This includes failure to connect to or receive log messages from the integration OpenShift Container Platform.

The product allows the use of supported central logging providers including Splunk and others.

2.6 Security Assessment Information – Advanced Cluster Security

Red Hat recommends use of the Red Hat Advanced Cluster Security, which provides a Kubernetes-native architecture for platform and application security, allowing DevOps and InfoSec teams to operationalize security.

Red Hat recommends a runtime security posture management component such as Red Hat Advanced Security or another similar component. Security Assessors may use Red Hat Advanced Cluster Security to aid in the assessment and enforcement of controls provided in this STIG. This STIG was not tested using Red Hat Advanced Cluster Security and does not require its use.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 OpenShift Container Platform Overview

OpenShift Container Platform is an application development and hosting platform built around the characteristics of Linux container technologies and Kubernetes to simplify management of large-scale distributed application systems across a full development, security, and operations lifecycle.

The platform includes a special-purpose operating system that can manage compute, network, and storage resources provided by various infrastructure providers including bare-metal hosts, virtual machines and virtualization platforms, private and public self-managed cloud services, or public and hyperscale cloud services. Platform components are implemented using a diverse range of technologies drawing from dozens of languages and frameworks and hundreds of open-source projects. Platform components are generally packed, deployed, and managed as Linux containers.

OpenShift uses an API-driven model for leveraging resources via cloud access model. It has a strong focus on flexibility and scalability while providing resource and application tenant isolation.

3.2 OpenShift Container Platform Components

OpenShift Container Platform is built from a large collection of special-purpose components. OpenShift Container Platform is a subscription product built on the foundations of an open-source community project Kubernetes with numerous enterprise features added. It combines hundreds of upstream projects into an integrated, streamlined product. Each product component also has a specific purpose with a well-defined scope.

Many of the core platform components make up a control plane for the management of application development and hosting, as well as management of the platform itself. The control plane component comprises multiple services implemented as containerized applications and deployed on Red Hat CoreOS. Multiple independently clustered or duplicated, load balanced, or stateless instances of these services may be deployed across multiple hosts for high availability, redundancy, or other purposes.

Figure 3-1: The OpenShift Control Plane Components, Including Primary Control Plane Services

(Other Control Plane Services Are Not Shown Here)

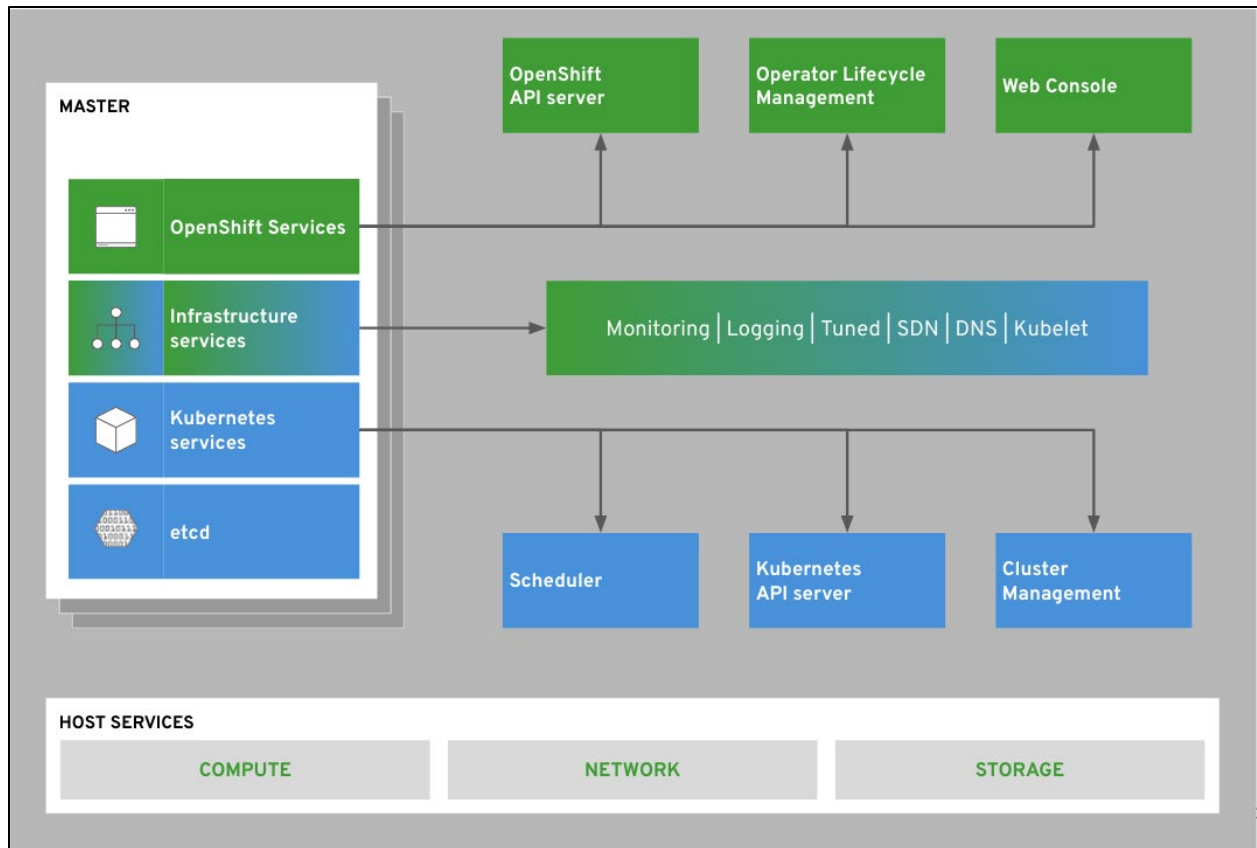


Figure 3-2: The OpenShift Worker Components
(Worker Services May Vary for Each Worker Instance;
Other Workers Services Are Not Shown Here)



3.3 Linux Containers

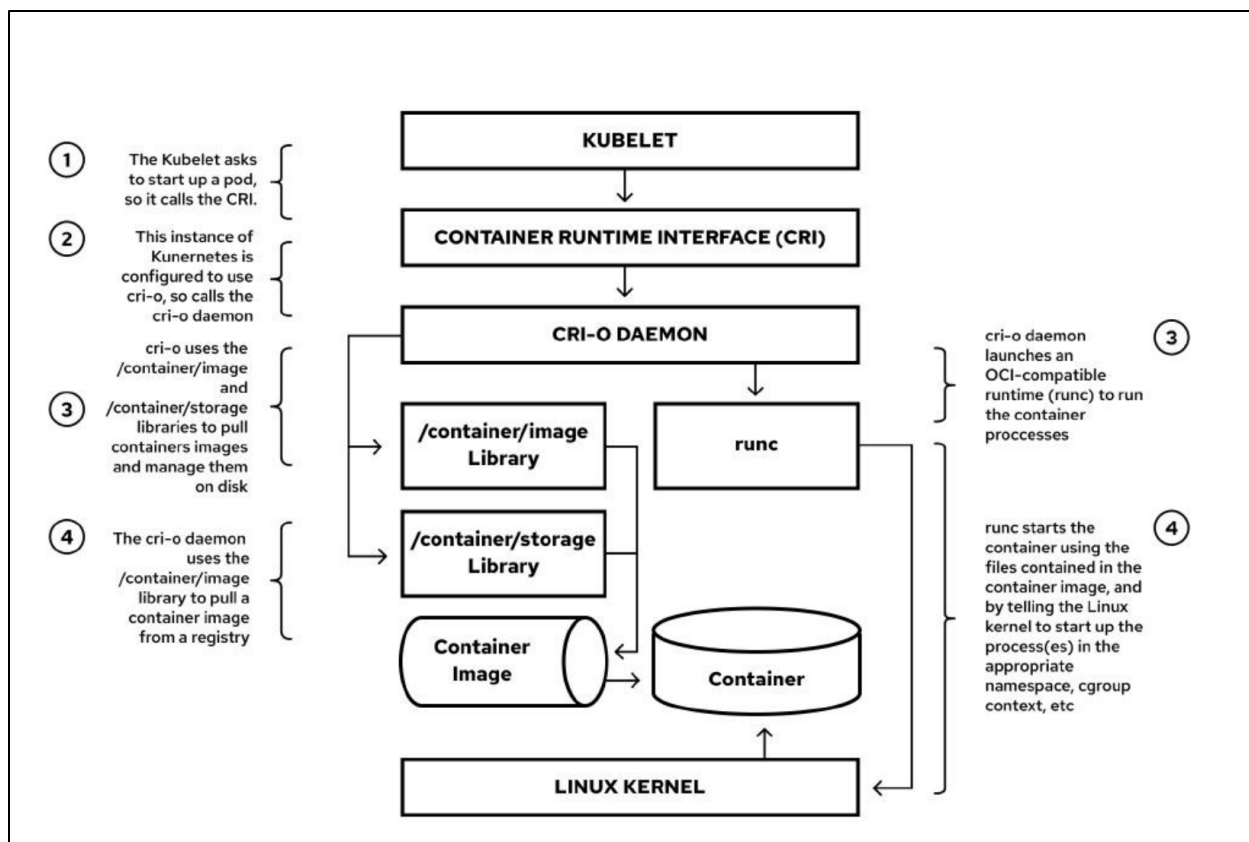
The OpenShift Container Platform uses Linux containers as a primary means of managing the services it is composed of as well as tenant applications. Containers serve multiple roles, and their functions can be viewed from multiple perspectives.

- From the operating system perspective, a container is a process that runs in a sandbox isolated from other processes outside its sandbox. A Linux host creates this sandbox using standard Linux kernel features such as namespaces, control groups (cgroups), and SELinux.
- From the system administrator perspective, a container is an application that is portable across different environments. This application is deployed, unchanged, on different cloud providers, bare-metal services, and virtualized hosts.
- From a developer perspective, a container is a way to package an application including potentially all its dependencies. Containers provide a universal packaging format independent of a programming language runtime.

A container is a running Linux process and is serviced in the OpenShift Container Platform via container runtime, a container engine, and a container registry. These components are responsible for creating containers from stored container images as held in container registries and realizing the

Linux process in accordance with the configuration metadata attached to each container image (config.json) as limited by the policies enforced by OpenShift Container Platforms via its default Security Context Constraints (SCCs) and Pod Security Admission Controller.

Figure 3-3: OpenShift's Primary Container Engine Components



3.4 Red Hat CoreOS

Red Hat Enterprise Linux CoreOS is a specialized distribution of Red Hat Enterprise Linux, optimized for running Linux containers on Kubernetes. This STIG requires the use of Red Hat CoreOS for the deployment of the OpenShift Container Platform; however, Red Hat Enterprise Linux may be used for worker nodes if secured in accordance with other hardening guidance.

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.

This STIG is intended to use Red Hat Enterprise Linux CoreOS capabilities to prevent out-of-band changes that might affect application behavior and security from persisting across node restarts. 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 such as SELinux and cgroups prevents application changes from modifying the operating system. This STIG provides control implementations made through the OpenShift Container Platform's role-based access control (RBAC), protected APIs, or redeployment of the hosts via the same verifiable ignition processes.

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.

Red Hat Enterprise Linux CoreOS hosts only allow modification of some system settings at installation time, and this STIG requires these settings to be configured prior to installation and deployment of the Red Hat OpenShift Container Platform. Because installation is a potentially complex operation and a deployment could consume significant resources, it is highly recommended that system owners and administrators review this STIG and implement required controls prior to installation when possible.

4. GENERAL SECURITY REQUIREMENTS

4.1 Hardening of Integrated External Services

OpenShift Container Platform must use several external services, as noted in section 2.1. The deployment and management of these services is outside the scope of this STIG. All services used by OpenShift Container Platform should be hardened to an appropriate level via a well-defined risk management framework (RMF), including the use of associated STIGs as applicable. Failure to do so may allow compromise of data, managed systems, user operations, or other impacts via lateral attacks from these integrated systems.

4.2 Content Sources: API Object Sources, Code Repositories, Container Image Repositories

OpenShift Container Platform relies on external declarative content, which is used to configure the platform itself, deploy and manage platform subcomponents, deploy and manage tenant application components, and other functions. This declarative content is generally not executable in nature but may have substantial impact on the functional behavior of the platform. This STIG requires the validation of the source of this declarative content, but additional, external processes for generating, maintaining, validating, and verifying the behavior of this content should be used.

4.3 Disaster Recovery and Continuity of Operations

The OpenShift Container Platform provides internal mechanisms to enable high availability, but more complex operations for DR and COOP are outside the scope of this STIG. These operations normally require significant planning, people, and processes outside a single product.

For best operations of the platform internal capabilities for DR and COOP, system operators should follow the best practices for implementing HA capabilities as provided in Red Hat's OpenShift Container Platform documentation.