IBM Systems Lab Services

OpenShift Security Assessment

Overview

The OpenShift Security Assessment is designed to assess the security hardening status of a Red Hat OpenShift v4.x cluster running on Intel or Power. This service assesses a running cluster for over 115 security hardening recommendations derived from the CIS Red Hat OpenShift Container Platform(OCP) v4 Benchmark – v1.1.0. The 115 controls are universal security hardening settings for all deployments of Red Hat OpenShift Version 4.

Technical Details

Over 115 CIS Red Hat OpenShift Benchmark settings assessed are security hardening settings to be implemented on your Red Hat OpenShift Cluster. For example:

- Ensure that a unique certificate authority is used for etcd
- Minimize the admission of root containers
- Apply security context to your pods and containers

Common Use Cases

- An OCP Build team that would like to analyze their master OCP Cluster baseline to identify more security hardening settings to add to their build process
- An organization that would like to verify that the security settings of an OCP cluster are not compromised
- An organization that would like to verify the security hardening status of a particular OCP Cluster
- An organization that would like to compare how security settings differ between OCP clusters built in different environments,for example, comparing a PROD OCP cluster versus a QA or DEV OCP cluster
- An organization that would like security remediation recommendations provided with guidance on priority and ordering

Service Details

- Data analysis and report generation is done by IBM
- This service requires only a few hours of customer time to run a data collection script and to attend a Webex session to review the results of the assessment
- One or more clusters can be assessed, depending on contract terms
- The assessment only reads existing security settings, that is, no settings are altered on the assessment cluster

Engagement Process

- Consultant arranges prep call to discuss data collection process and to schedule Webex to review assessment results
- Client uploads encrypted tar file to BOX
- Consultant analyzes data and creates deliverables
- Consultant reviews results with client on Webex

Deliverables

1. Heat Map – (see Fig. 1) the spreadsheet provides a one page view of the results of the assessment.
2. Security Assessment Findings – (see Fig. 2) this PDF details the results of the assessment. Over 115 security assessment results are detailed in this document. The document provides a hyperlinked Table of Contents to quickly access any of the more than 115 security controls assessed

	A	B	C	D
1	**Control Number**	**Control Name**	**Finding**	**CIS SB Level**
2	1	Control Plane Components		
3	1.1	Master Node Configuration Files		
4	1.1.1	API Server Pod Specification Permissions	✔	1
5	1.1.2	API Server Pod Specification Ownership	✔	1
6	1.1.3	Controller Manager Pod Specification Permissions	✔	1
7	1.1.4	Controller Manager Pod Specification Ownership	✔	1
8	1.1.5	Scheduler Pod Specification Permissions	✔	1
9	1.1.6	Scheduler Pod Specification Ownership	✔	1
10	1.1.7	etcd Pod Specification Permissions	✔	1
11	1.1.8	etcd Pod Specification Ownership	✔	1
12	1.1.9.a	Container Network Interface Permissions - CNI	✔	1
13	1.1.9.b	Container Network Interface Permissions - SDN	✔	1
14	1.1.9.c	Container Network Interface Permissions - OVS	✔	1

Fig. 1 - An excel spread sheet will be provided that will indicate the result of each security control being assessed.

1.2.33 Ensure that the --encryption-provider-config argument is set as appropriate (Manual)

Profile Applicability:

- Level 1

Description:

Encrypt `etcd` key-value store.

Rationale:

`etcd` is a highly available key-value store used by Kubernetes deployments for persistent storage of all of its REST API objects. These objects are sensitive in nature and should be encrypted at rest to avoid any disclosures.

Impact:

When you enable `etcd` encryption, the following OpenShift API server and Kubernetes API server resources are encrypted:

- Secrets
- ConfigMaps
- Routes
- OAuth access tokens
- OAuth authorize tokens

When you enable `etcd` encryption, encryption keys are created. These keys are rotated on a weekly basis. You must have these keys in order to restore from an `etcd` backup.

Finding: ✖

Consultant comments:
Encryption is not enabled. This is what was detected:
```
EncryptionDisabled
Encryption is not enabled
```

Remediation:

Follow the OpenShift documentation for Encrypting etcd data | Authentication | OpenShift Container Platform 4.5

Default Value:

By default, `etcd` data is not encrypted in OpenShift Container Platform

References:

1. https://docs.openshift.com/container-platform/4.5/security/encrypting-etcd.html
2. https://docs.openshift.com/container-platform/4.5/operators/operator-reference.html#etcd-cluster-operator_red-hat-operators

Fig. 2 - "Encrypting the etcd key-value store at rest" is an example of one of the settings that gets assessed in this service.