Guide for OpenShift 3.11 SCAP content

To support OpenShift deployments in regulated environments, Red Hat has been developing SCAP and Ansible based security automation content. This content is currently available here: https://nvd.nist.gov/ncp/checklist/866.

The SCAP-based configuration evaluation does not alter system settings.

Any discovered bugs should be reported to https://github.com/ComplianceAsCode/content/issues

STEP 1: INSTALL TOOLS AND CONTENT

Usage of the security automation content requires OpenSCAP (for configuration scanning) and Ansible (for remediation capabilities). Install these components on all OpenShift Master(s) and Node(s) by running the following command:

```
$ sudo yum -y install openscap-utils ansible
```

The security automation content can be downloaded through the ComplianceAsCode project which will be needed for all Master(s) and Node(s):

```
$ wget \
https://github.com/ComplianceAsCode/content/releases/download/v
0.1.43/scap-security-guide-0.1.43.zip
```

The content is downloaded as a zip file, and will need to be unarchived:

```
$ unzip scap-security-guide-0.1.43.zip
```

The files to use for the scan in the zip file are:

- **ssg-ocp3-ds.xml**
  SCAP Datastream file

- **roles/ssg-ocp3-role-opencis-master.yml**
  Ansible playbook for Master nodes

- **roles/ssg-ocp3-role-opencis-node.yml**
  Ansible playbook for nodes

STEP 2: PERFORM CONFIGURATION SCAN

Prior to performing a configuration evaluation ensure OpenSCAP installed on the OCP masters and nodes. The scan can be run manually, through a job, or from Red Hat Satellite.

To run a scan on the OpenShift Master node:

```
$ sudo oscap xccdf eval --profile \
xccdf_org.ssgproject.content_profile_opencis-master \
--report master-report.html \
--oval-results \
/path/to/ssg-ocp3-ds.xml
```

To run a scan on non-master nodes:

```
$ sudo oscap xccdf eval \
--profile xccdf_org.ssgproject.content_profile_opencis-node \
--report node-report.html \
--oval-results \
/path/to/ssg-ocp3-ds.xml
```

Pass/fail states will be displayed on the command line.

HTML reports will also be generated (`master-report.html`, `node-report.html`) which are used as a human readable interfaces to view why certain rules passed and others failed.

MORE ABOUT THE COMPLIANCE AS CODE REPO

Compliance as code readme:
https://github.com/ComplianceAsCode/content/blob/master/README.md

Red Hat OpenShift 3 profiles
https://github.com/ComplianceAsCode/content/tree/master/ocp3/profiles

Red Hat OpenShift XCCDF and OVAL
https://github.com/ComplianceAsCode/content/tree/master/applications/openshift