

# Docker and Kubernetes Security

## Frankfurt

Integration health checks will automatically perform the following security checks for the Frankfurt release.

1. pod\_root: Pods must not run as root in Frankfurt. Example of how to configure a Docker not to run as root.
  - a. **JIRA** <https://jira.onap.org/browse/ID-423?gerritIssueStatus=All#gerrit-reviews-left-panel>
  - b. **Reference multicloud change** <https://gerrit.onap.org/r/c/multicloud/azure/+81884/1/azure/docker/Dockerfile>
  - c. **VID's change** <https://gerrit.onap.org/r/c/vid/+84526>
2. Java debug wire protocol (jdwp) port (port 6379) must be closed (onap-dcae-redis-0, onap-dcae-redis-1, onap-dcae-redis-2, onap-msb-eag-57f7ccb568-ht7h6, onap-msb-iag-6f8f449bd7-d582t, onap-vnfsdk-566786f85f-m9q9b 8000)
  - a. Update the test to exclude false positives reported by the project teams (redis default port = jdwp default port (6379)).
3. nodeport\_ingress: HTTP ports must be migrated to HTTPS.
  - a. Review the list of the current 20 HTTP ports to determine which ones are necessary (robot, portal-sdk, portal-app, message-router, dmaap-bc, log-kibana, log-es, dmaap-dr-prov, cli, consul-server-ui, sniro-emulator, refrepo, uui, config-binding-service, dashboard, netbox-nginx, music-tomcat, cds-blueprints-processor-http, aaf-fs). The aaf-fs port is a known exception.
  - b. Upgrade test to exclude those HTTP ports.

## CIS Benchmarks



CIS\_Docker\_Benc...mark\_v1.2.0.pdf



CIS\_Kubernetes\_...mark\_v1.4.1.pdf