Code Scanning Tools and CI

This section is focused on describing how CI is connected to our different scanning tools and how the code scan generates the resulting reports.

Currently, we have 3 code scan tools linked in our Jenkins CI:

	NexusIQ	WhiteSource	Sonarcloud
URL	https://nexus-iq.wl.linuxfoundation.org/assets/index.html#/management/view/organization/a044ccf18614413dbe45464a5524f784	https://saas.whitesourcesoftware.com/	https://sonarcloud.io/organizations/onap/projects
Purpose	License and vulnerability	License and vulnerability	Code coverage from testing
Access	Automatic for all committer groups. Not in a group? Contact support.linuxfoundation.org with LFID	On case basis. Contact support.linuxfoundation.org and provide email address to send the invitation to.	Automatic if part of the ONAP GitHub org Contact support.linuxfoundation.org for GitHub invite (Include GitHub ID)
Jenkins	https://jenkins.onap.org/view/CLM/ All projects must have Nexus IQ scans: https://docs.releng.linuxfoundation.org/projects/global-jjb/en/latest/jjb/lf-maven-jobs.html#maven-clm	https://jenkins.onap.org/view/WhiteSource/ Only few projects are implemented. Rest of the projects is still under discussion. https://docs.releng.linuxfoundation.org/projects/global-jjb/en/latest/jjb/lf-whitesource-jobs.html	https://jenkins.onap.org/view/All-Sonar/ All projects must have Sonar scans: https://docs.releng.linuxfoundation.org/projects/global-jjb/en/latest/jjb/lf-maven-jobs.html#lf-infra-maven-sonarcloud
Frequency and triggers	Once per week (Saturdays) Via Gerrit comments: run-clm	Once per week (Saturdays) Via Gerrit comments: run-whitesource	Via Gerrit comments: run-sonar
Overall process	Example job: https://jenkins.onap.org/view/CLM/job/aai-aai-common-maven-clm-master/ ▪ The job triggers a "clean install dependency:tree com.sonatype.clm:clm-maven-plugin:index" ▪ A separate step invokes the Nexus IQ scanner using a Jenkins plugi	Example job: https://jenkins.onap.org/view/WhiteSource/job/aai-aai-common-whitesource-scan-master/ • The job runs a "clean install" of the code • A separate step downloads and runs White Source's Unified Agent to scan the code	Example job: https://jenkins.onap.org/view/All-Sonar/job/aai-aai-common-sonar/ • The job runs a "clean install" of the code • A separate step runs "org.sonarsource.scanner.maven:sonar-maven-plugin:3.7.0.1746:sonar" to process the sca
Quality Gates	High thread violations need to be addressed and investigated in case they are false.	Currently this is not a release blocker. The reports are being used for testing purposes.	Quality Gate must be above 55% to pass. Test coverage is managed by tech teams
Example report	https://nexus-iq.wl.linuxfoundation.org/ui/links/application/onap-aai-aai-common/report/356ad44fd6724db292a4daa53e50a1c2	https://saas.whitesourcesoftware.com/Wss/WSS.html#!project;id=1387312	https://sonarcloud.io/dashboard?id=onap_aai-aai-common