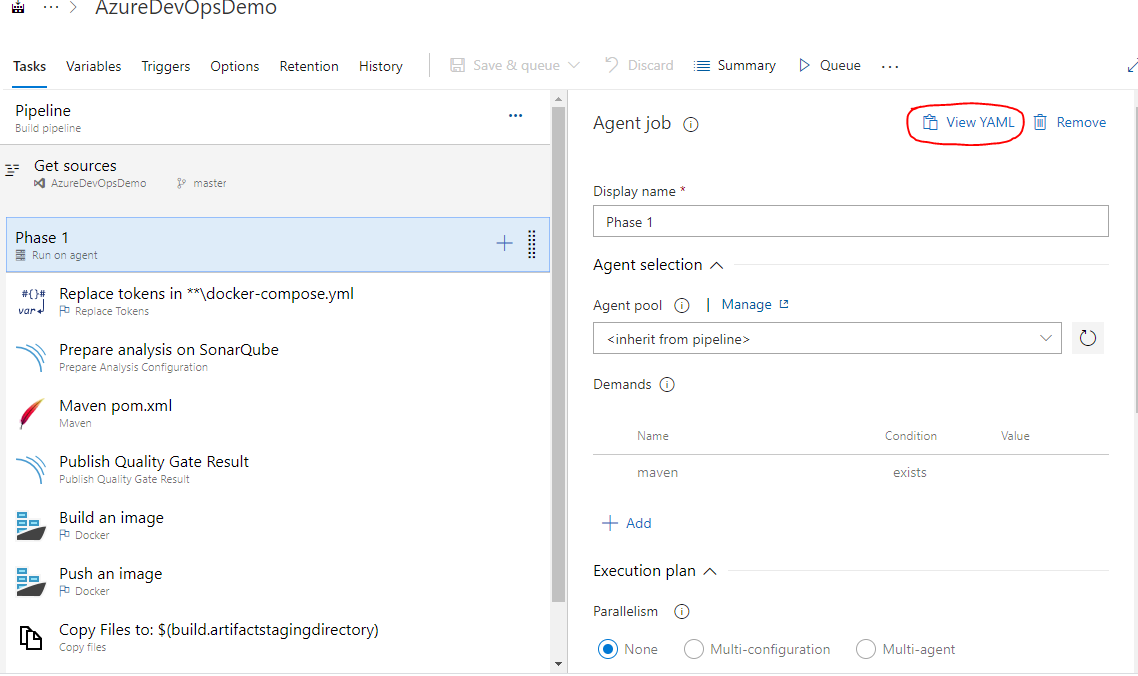
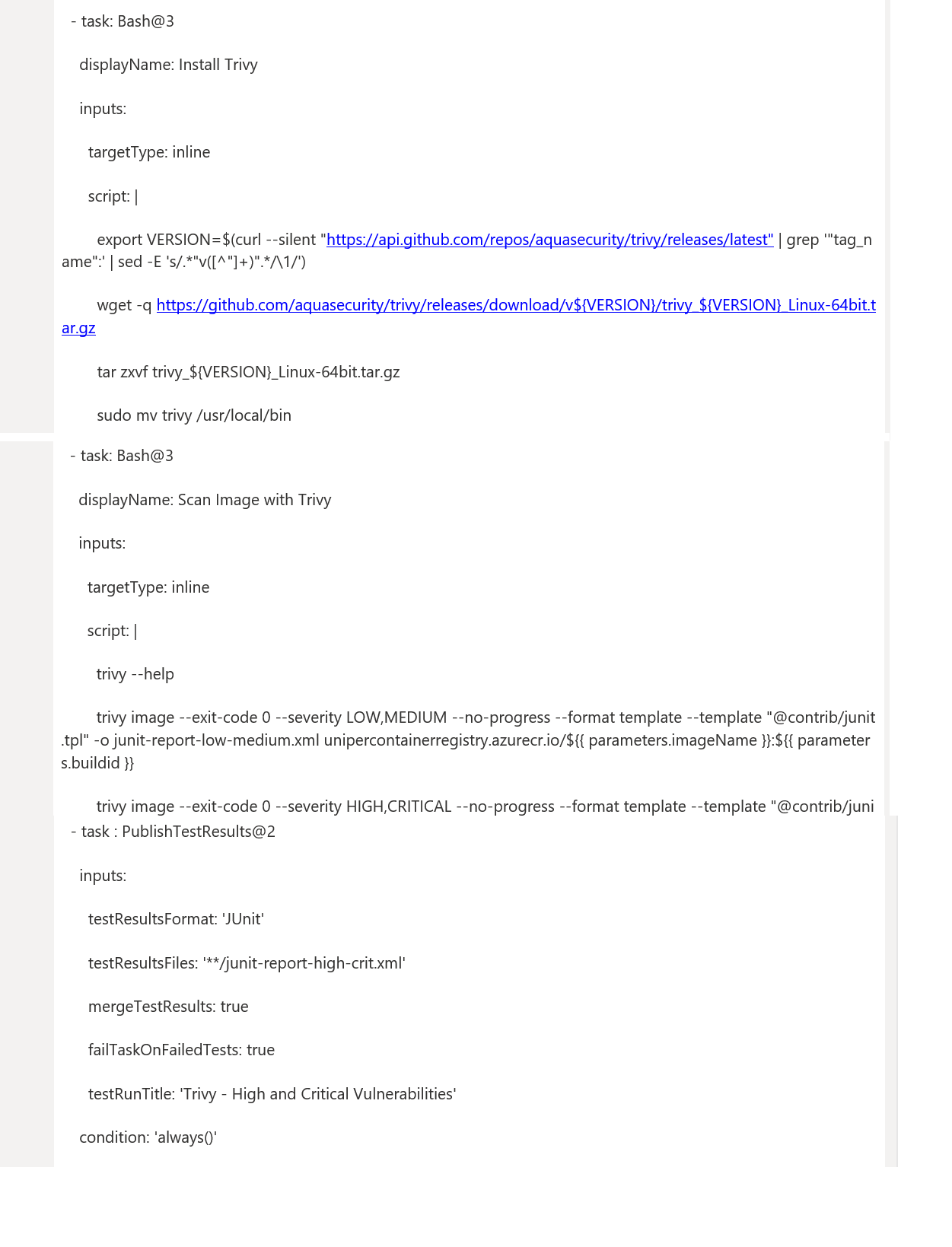
# Container security scan during Azure-DevOps build using Trivy

Trivy is a comprehensive security scanner. It is reliable, fast, extremely easy to use, and it works wherever you need it.

It is highly recommended to scan your docker container image for vulnerabilities during the execution of your build pipeline. You can include the trivy container security scanner in your build pipeline as follows:

* Prerequisites: your build pipeline should be available in yaml format. If you have a visual build pipeline you can retrieve the corresponding yaml code as shown by the picture below.  
  
* Search for the docker build step in your pipeline and insert the trivy scan steps   
  You can download the scan steps here: 

Now when the scan runs, two files will be output, junit-report-low-medium.xml which contains all our results for low and medium vulnerabilities, and junit-report-high-crit.xml which contains all our results for high and critical vulnerabilities. These are output to the disk of the build agent.

Firstly, we’re telling each task our report is in a JUnit format and the files we want to publish are called junit-report-low-medium.xml and junit-report-high-crit.xml. Secondly, we find our main difference between the two tasks - failTaskOnFailedTests - this pretty much does what it says on the tin. If it’s set to true the task will fail the build if any test failures are found and if it’s set to false, it won’t.

* Run your build pipeline. You should see a scan result similar to this one:

