Jenkins job authorization

Gavin McDonald is this still needed, or is this information incorporated in other pages/ newer states of Jenkins?

The Introduction

In 2017, the ASF Jenkins instance went through a few upgrades of both the OS (2.32.2 to 2.46.2) and its plugins. As a result, the way some jobs are authorized has changed (or been introduced).

With thanks to the patience, investigations and summary of Joan Touzet, find below some helpful information on job configurations for the ASF Jenkins instance. If needed, feel free to contact Infra for any clarifications.

The Details

If a job is running with the default authorization (runs as Jenkins' built-in SYSTEM user), the only option is to use the global credentials store. This means ASF Infra has to create the creds and manage them for you. This isn't scalable.

If you are running a classic Jenkins job, you can set the Authorization (https://builds.apache.org/job/jobname/authorization/) to run as a specific user and enter your own User ID. You can then add credentials you'd like to have in the job through your own credentials panel (https://builds.apache.org/user/userid/credentials/store/user/domain/_/). You can then bind these to environment variables through the job's Configuration. Be sure not to check the "Don't restrict job configuration" box unless you're absolutely sure you understand the security implications.

If you are running a Jenkins pipeline job, follow the same steps as for a classic Jenkins job just above, but you can't bind the credentials to an environment variable in the pipeline configuration. Instead, use a block of the form environment { AN_ACCESS_KEY = credentials('my-predefined-secret-text') } for a declarative pipeline job, or the withCredentials([$class: 'StringBinding', credentialsId: name, variable: 'foo']]) {} type block for a scripted pipeline.

If you are running a multibranch pipeline job, things are even easier. Each multibranch pipeline job gets its own credentials store which is automatically available within that job's scope. Add the credentials via the job's credential store page at https://builds.apache.org/job/jobname/credentials/store/folder/. Then access the credentials in the same way as above for a declarative or scripted pipeline.

Extra

For those of you using Matrix jobs and having trouble with downstream builds not running, please enable job Authorization for each of your parent and child builds.

More Info

For a more complete history of the above summary and the issues that led to it, see

INFRA-14134 - Cannot access newly created Jenkins credentials

INFRA-14222 - Qpid jenkins job "Qpid-BrokerForJava-MMS-TestMatrix" cannot start downstream project with warning about no associated authentication

See

for an example of an issue with Matrix builds.

Note that Jenkins release 2.46.3 mentions this:

Fix AccessDeniedException in "Build after other projects are built" when user has Discover permission but not Read. (issue 42707)

Therefore upgrading to 2.46.3 may cure the Matrix issue.

Screenshot Example