Contribution ID: **80** Type: **Short Talk**

Secure Command Line Solution for Token-based Authentication

Thursday, 20 May 2021 15:39 (13 minutes)

The WLCG is modernizing its security infrastructure, replacing X.509 client authentication with the newer industry standard of JSON Web Tokens (JWTs) obtained through the Open ID Connect (OIDC) protocol. There is a wide variety of software available using the standards, but most of it is for Web browser-based applications and doesn't adapt well to the command line-based software used heavily in High Throughput Computing (HTC). OIDC command line client software did exist, but it did not meet our requirements for security and convenience. This paper discusses a command line solution we have made based on the popular existing secrets management software from Hashicorp called vault. We made a package called htvault-config to easily configure a vault service and another called htgettoken to be the vault client. In addition, we have integrated use of the tools into the HTCondor workload management system, although they also work well independent of HTCondor. All of the software is open source, under active development, and ready for use.

Primary author: DYKSTRA, Dave (Fermi National Accelerator Lab. (US))

Co-authors: TEHERAN SIERRA, Jeny Lucia (Fermi National Accelerator Lab. (US)); ALTUNAY, Mine (Fermi National Accelerator Laboratory)

Presenter: DYKSTRA, Dave (Fermi National Accelerator Lab. (US))

Session Classification: Facilities and Networks

Track Classification: Distributed Computing, Data Management and Facilities