Contribution ID: **360**   Type: **Talk**

Fermilab's Transition to Token Authentication

Tuesday 22 October 2024 17:09 (18 minutes)

Fermilab is the first High Energy Physics institution to transition from X.509 user certificates to authentication tokens in production systems. All of the experiments that Fermilab hosts are now using JSON Web Token (JWT) access tokens in their grid jobs. Many software components have been either updated or created for this transition, and most of the software is available to others as open source. The tokens are defined using the WLCG Common JWT Profile. Token attributes for all the tokens are stored in the Fermilab FERRY system which generates the configuration for the CILogon token issuer. High security-value refresh tokens are stored in Hashicorp Vault configured by htvault-config, and JWT access tokens are requested by the htgettoken client through its integration with HTCondor. The Fermilab job submission system jobsub was redesigned to be a lightweight wrapper around HTCondor. For automated job submissions a managed tokens service was created to reduce duplication of effort and knowledge of how to securely keep tokens active. The existing Fermilab file transfer tool ifdh was updated to work seamlessly with tokens, as well as the Fermilab POMS (Production Operations Management System) which is used to manage automatic job submission and the RCDS (Rapid Code Distribution System) which is used to distribute analysis code via the CernVM FileSystem. The dCache storage system was reconfigured to accept tokens for authentication in place of X.509 proxy certificates. As some services and sites have not yet implemented token support, proxy certificates are still sent with jobs for backwards compatibility but some experiments are beginning to transition to stop using them. There have been some glitches and learning curve issues but in general the system has been performing well and is being improved as operational problems are addressed.

Primary authors: DYKSTRA, Dave (Fermi National Accelerator Lab. (US)); LITVINTSEV, Dmitry (Fermi National Accelerator Lab. (US)); MENGEL, Marc (Fermi National Accelerator Lab. (US)); ALTUNAY, Mine (Fermi National Accelerator Lab. (US)); BHAT, Shreyas (Fermi National Accelerator Lab. (US)); WHITE, Stephen (Fermi National Accelerator Lab. (US))

Presenter: SMITH, Nick (Fermi National Accelerator Lab. (US))

Session Classification: Parallel (Track 4)

Track Classification: Track 4 - Distributed Computing