

面向高能物理异构计算平台的无认证安全文件共享设计与实现

Monday, 25 August 2025 14:20 (20 minutes)

现代高能物理研究依托于大规模、异构的计算与存储基础设施，其数据分析流程的复杂性对用户交互的便捷性和协同工作的效率提出了前所未有的挑战。高能物理研究所的计算平台是一个集成了HTCondor、Slurm等多种作业调度系统以及LUSTRE、EOS、CVMFS等异构存储资源的典型大规模科研计算环境。传统基于命令行的交互模式在新一代科研人员面前日益显得低效与不便。ink-Interactive ANalysis worKbench (INK) 平台，通过将VSCode、Jupyter等分析工具容器化Web化，为用户提供了现代化的交互式分析体验。本文着重阐述了在INK平台基础上设计并实现的一种新型文件共享功能，其核心目标是在保障数据安全的前提下，为用户提供一种“即时生成、无需认证”的便捷数据分享。设计了精细化的安全机制来解决无认证访问带来的潜在数据泄露风险。当用户选择共享文件时，动态创建包含签名令牌的临时访问URL，采用基于JSON Web Token (JWT) 的方案，将授权信息编码在令牌中。任何通过该链接发起的访问请求，都必须首先通过FastAPI网关的令牌校验。网关会验证令牌的签名、时效性和其中编码的权限规则，只有完全合规的请求才会被转发至后端的xrootd服务执行。这种将授权策略与访问凭证绑定的无状态验证模式，既避免了要求终端用户进行繁琐的身份认证，又实现了对共享资源的强安全管控。

Summary

Primary authors: 欧, 歌 (高能所); SHI, Jingyan (IHEP); BI, Yujiang (IHEP)

Presenter: 欧, 歌 (高能所)

Session Classification: 科学数据存储与管理

Track Classification: 科学计算技术及用户交流