

Design and implementation of experimental data access security policy for HEPS container computing platform

Qingbao Hu^{1,*}, Jiping Xu¹, Yaosong Cheng¹, Qi Luo¹, and Shiyuan Fu¹

¹Institute of High Energy Physics, Chinese Academy of Sciences, Beijing, China

Abstract. China's High-Energy Photon Source (HEPS), the first national high-energy synchrotron radiation light source, is under design and construction. In the future, at the first stage of HEPS, it is predicted that 24PB raw experimental data will be produced per month from 14 beamlines. Faced with such a huge scale of scientific data and diverse data analysis environments in light source disciplines, the HEPS scientific computing platform was designed and implemented based on container mirroring and dynamic orchestration technology to provide HEPS users with a data analysis environment. In this article, a data security access strategy is designed and evaluated for a scientific computing platform to ensure the security and efficiency of data access for users in the entire process of data analysis. First, the general situation of HEPS is introduced. Second, the challenges faced by the HEPS scientific computing system. Third, the architecture and service process of the scientific computing platform are described from the perspective of IT, some key technical implementations will be introduced in detail. Finally, the application effect of data access security policies on computing platforms will be demonstrated.

1 Introduction

High Energy Photon Source (HEPS)[1] is an important platform for supporting original and innovative research in the fields of basic science and engineering science, has been in construction since 29 June 2019 in Beijing's Huairou District and will be completed in 2025. HEPS will be a storage-ring-based light source with a beam energy of 6 GeV and emittance less than 60 pm rad, which can provide high brilliance hard X-rays to several tens of experimental stations. HEPS project enables research in three key areas: spectroscopy, imaging, and diffraction. These areas of study utilize high-energy photons to investigate the electronic and atomic structures of materials, visualize internal structures, and analyze the scattering patterns to understand the arrangement of atoms or molecules within a material. In the future, HEPS will be the first high-energy synchrotron radiation light source in China. At HEPS, researchers will be able to observe the complex samples with more sensitive, finer, faster experimental tools, under conditions close to the actual working environment, thereby helping researchers obtain high-quality multidimensional, real-time, in-situ characterization of sample structure, as well as the dynamic evolution processes.

*e-mail: huqb@ihep.ac.cn

Table 1. Data volume of HEPS beamlines

Beamlines	Burst output (TB/day)	Average output (TB/day)
B1 Engineering Materials Beamline	600	200
B2 Hard X-ray Multi-analytical Nanoprobe (HXMAN) Beamline	500	200
B3 Structural Dynamics Beamline	8	3
B4 Hard X-ray Coherent Scattering Beamline	10	3
B5 Hard X-ray High Energy Resolution Spectroscopy Beamline	10	1
B6 High Pressure Beamline	2	1
B7 Hard X-Ray Imaging Beamline	1000	250
B8 X-ray Absorption Spectroscopy Beamline	80	10
B9 Low-Dimension Structure Probe (LODISP) Beamline	20	5
BA Biological Macromolecule Microfocus Beamline	35	10
BB pink SAXS	400	50
BC High Res. Nanoscale Electronic Structure Spectroscopy Beamline	1	0.2
BD Tender X-ray beamline	10	1
BE Transmission X-ray Microscope Beamline	25	11.2
BF Test beamline	1000	60
Total average:		805

2 The challenges of HEPS computing platform

Traditionally, experiment raw data are collected and stored on the hard drive of the local beamline server directly during beam time. Users have to manually copy a large amount of data from the local beamline disk to portable hard drives and then spend several months analyzing the data on personal computers to obtain few results that are suitable for publication, which severely limits the scientific research output of synchrotrons. With the rapid development of synchrotrons, new techniques increase the amount of raw data collected during each experiment. According to the estimated data rates (shown in Table 1) provided by beamline scientists, we predict that 24 PB of raw experimental data will be produced per month from 14 beamlines at the first stage of HEPS. With such a huge amount of data, it is very difficult to implement the traditional manual copying method on a personal computer for data analysis. Reduce the movement of large-capacity experimental data, provide the same data analysis environment as the user's personal computer, and implement the data generation and data analysis processes online, which is a new idea for modern light sources to provide services to users.

HEPS computing center is the principal provider of high-performance computing and data resources and services for science experiments of HEPS. The mission of HEPS computing platform is to accelerate the scientific discovery for the characteristics of light source experiments through high-performance computing and data analysis. The computing platform needs to provide high-performance computing and data access capabilities to meet the storage, processing, and analysis requirements of spectral data, imaging data, and scattering data. The computing platform also needs to integrate multiple data analysis methods such as ptychography, tomography, CT, and X-ray photon correlation spectroscopy (XPCS), to meet the analysis needs of experimental data. In addition, in order to achieve efficient computing and data processing when processing large amounts of data and complex physical problem

scenarios, the platform needs to make full use of the advantages of huge resources and support resource scheduling functions across different nodes to provide computing efficiency that cannot be achieved by personal computers. At HEPS, the experimental data is associated with the experimental samples and experimental research objectives, and its experimental data is only open to the members of the experiment. Traditional high-energy physics data comes from detectors, and scientists in cooperative groups share experimental data. Unlike traditional high-energy physics computing and analysis scenarios, the HEPS computing platform must strictly control the data access rights of the computing and analysis environment to prevent unauthorised personnel from accessing experimental data. Therefore, when designing and building a HEPS computing platform, some security access strategies for HEPS massive experimental data need to be considered.

3 HEPS scientific computing platform

In response to HEPS user data analysis needs and experimental data characteristics, we designed a complete HEPS computing platform service process based on the goal of safe access to experimental data, which includes data ACL management, analysis tool selection, analysis environment creation, user identity management and secure creation of the user data analysis environment.

3.1 Data ACL management policy

The experimental data of the light source is large in volume and highly private. It is necessary to set strict data access permissions and provide efficient data access performance. Storage systems provide three different data access modes: block storage, file storage, and object storage.[2] Each data access mode has its own strengths and use cases. File storage offers a hierarchical structure and shared access for applications that work with files. File storage system, which supports POSIX semantics access, is the most common storage system in use today. The POSIX compliance provides a wide range of IO functions for applications to use. Typically POSIX storage is faster than object storage and is easier to manage data access permissions than block storage systems, which makes it a preferred choice for experimental data management of the light source. The POSIX filesystem Access Control List (ACL) provides a mechanism for defining fine-grained access permissions on files and directories.[3] It extends the traditional POSIX permissions model by allowing users to specify access controls for multiple users and groups beyond the owner, group, and others. When the experimental data is stored on disk, the HEPS data management system sets the corresponding owner and which users and groups can access it. Mount the experimental data file storage system in the data analysis environment, and only users in the access control list have permission to access the data. Therefore, when using the ACL mechanism of the POSIX file storage system, ensuring that users cannot forge the identities of other users in their respective analysis environment sessions is the key to the entire data security access process.

3.2 JupyterLab tool provides interactive data analysis through a webpage

In order to meet the diverse data analysis requirements in the three key areas of HEPS, the Jupyterlab scientific data analysis tool based on container technology is deployed on the HEPS scientific computing platform. JupyterLab[4] is the latest web-based interactive development environment for notebooks, code, and data. The software developers in different research areas of light sources can quickly integrate multiple methodological analysis environments into JupyterLab, which is convenient for users to quickly start the environment and

use these analysis tools through the browser anytime and anywhere. In the Jupyter ecosystem, JupyterHub is another important component, which allows multiple users to access and use JupyterLab or other computational environments simultaneously. It provides a centralized hub for managing and serving JupyterLab to users, and handles user authentication, resource allocation, and session management, enabling multiple users to work on the same computing platform securely. With the rapid development of cloud-native technology, JupyterHub deployed on k8s can leverage its scalable nature to support a large group of users and more stable services.[5]

3.3 HEPS data analysis environment creation

The creation of the HEPS data analysis environment is divided into two stages: creating container images and orchestrating container runtime environments. HEPS packages container images for different data analysis software applications based on specific use cases. These application software images are developed based on the underlying computing environment base image. This approach decouples the development of the computing environment functionality from the application software functionality. The computing environment-based image focuses on user identification and authentication, resource allocation and management, and provides logical script interfaces for configuring the system environment at the application software layer. The application software layer focuses on the development of software functionality. Container orchestration technology, such as Kubernetes, refers to the management and coordination of containerized applications and their underlying infrastructure. It involves automating the deployment, scaling, and management of containers across a cluster of nodes. JupyterHub deployed on the Kubernetes cluster, which is used to host and manage the different container image instances for multiple users. JupyterHub obtains user authentication identity information and launches corresponding image instances based on the user's selected application analysis scenario. It loads specific files, configures the user environment, mounts the user's home directory and experiment data directory, and allows the user to access the corresponding JupyterLab instance.

3.4 User identity management

JupyterHub has completed the web-based user login and authentication method and mounted the POSIX file system to the JupyterLab container environment through orchestration technology. It requires a unified computing environment user management system to realize identity mapping between web page authentication and operating systems to ensure consistency of user identities between the web application layer and the operating system. At HEPS, LDAP cluster is used to centrally manage computing cluster user identity information and provides the web authentication method of the Oauth2.0 protocol. Kerberos5[6] server is used to verify the user's identity, and issues the user's Ticket Granting Ticket (TGT), which can be forwarded or obtain new tickets without re-entering their credentials and enabling seamless authentication across multiple servers. Based on the characteristics of krb5 tickets, a krb5 principal keytab file issuance management module open to specific access ranges is designed and implemented. This module can generate krb5 principal keytab file for any cluster user according to needs, which is used to create krb5 TGT for seamless authentication across different servers. At HEPS scientific computing platform, after a user passes the oauth2.0 authentication, JupyterHub accesses the keytab file issuance management module to obtain the user's keytab file. This keytab file is injected into the JupyterLab container as an environment variable to provide user's identity basis for different data analysis session environments.

3.5 Securely create the user data analysis environment

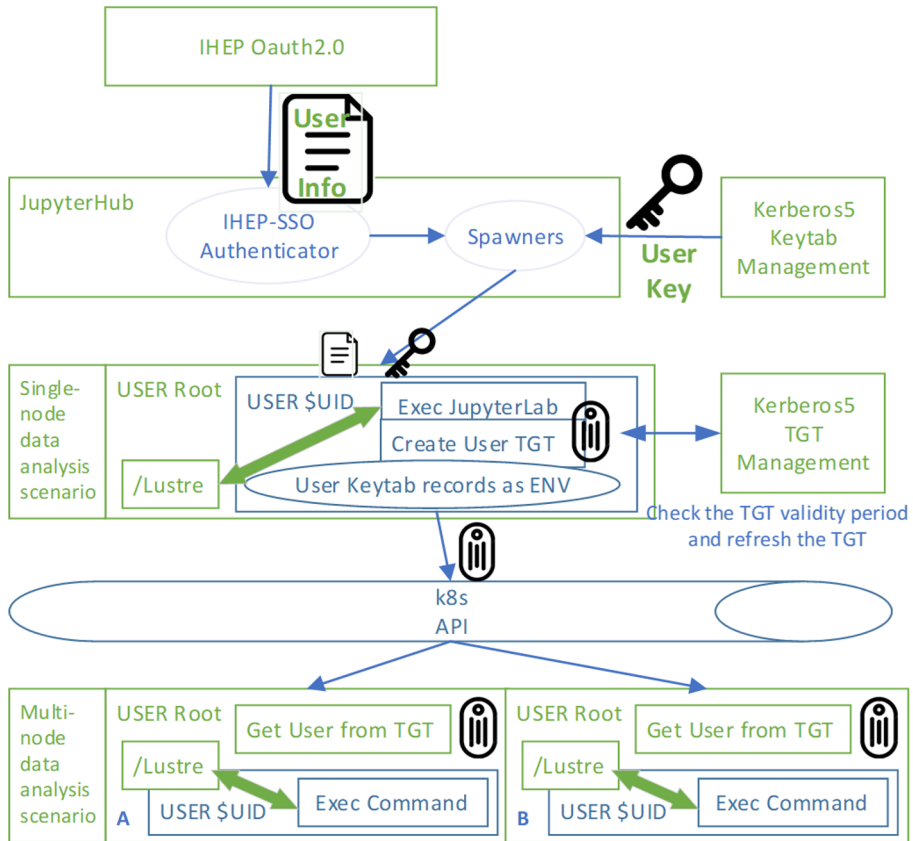
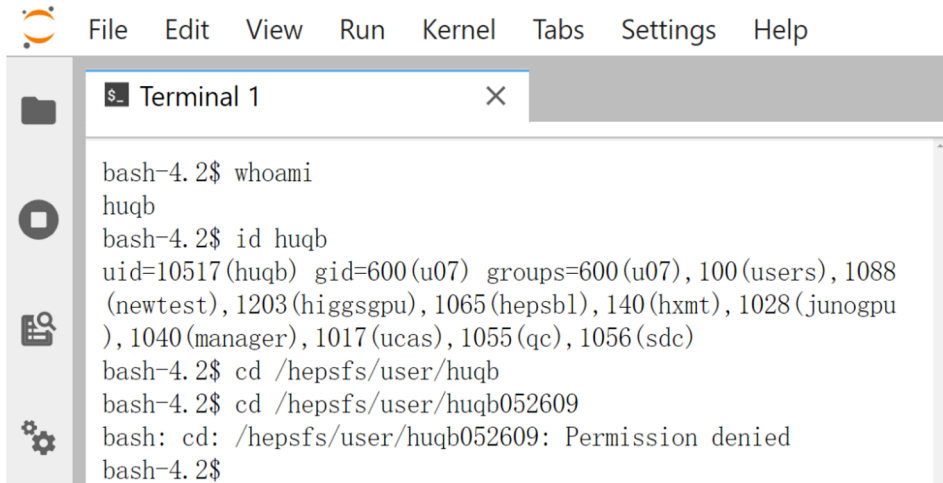


Figure 1. The complete user login and container creation process on HEP computing platform

In order to cope with the analysis needs of users with different computing power scales, the computing platform supports a single-container data analysis environment for ordinary computing power and a parallel data analysis data environment for multi-container collaborative computing. By logging in to JupyterHub, users start a single-container user data analysis environment represented by JupyterLab and inject environment variables that identify the user's identity. During the process of starting the container, the identity management module of the computing environment base image will identify the current user information through environment variables, obtain userid, group list, and other information by accessing the User identity management module, and create corresponding users and groups in the container environment. Then, start JupyterLab as a user and provide data analysis services to users through the web page. Through the above process, users can access the POSIX file system based on the user's uid and gid identities during the entire life cycle of using the interactive analysis environment, ensuring the security of data access. In addition, in order to provide multi-container collaborative analysis scenarios, when starting the JupyterLab container, the Kubernetes service account credentials will be injected. The credentials authorized users can directly access the kube-apiserver according to the analysis needs and start several containers for collaborative analysis. When starting these container environments for collaborative data



```
File Edit View Run Kernel Tabs Settings Help
Terminal 1
bash-4.2$ whoami
huqb
bash-4.2$ id huqb
uid=10517(huqb) gid=600(u07) groups=600(u07), 100(users), 1088
(newtest), 1203(higgsgpu), 1065(hepsb1), 140(hxmt), 1028(junogpu
), 1040(manager), 1017(ucas), 1055(qc), 1056(sdc)
bash-4.2$ cd /hepsfs/user/huqb
bash-4.2$ cd /hepsfs/user/huqb052609
bash: cd: /hepsfs/user/huqb052609: Permission denied
bash-4.2$
```

Figure 2. The application effect of data access security policies on computing platforms

analysis, the environment variables that record user identities in the JupyterLab container and user's ssh-key file will also be injected into the collaborative container. The collaborative container is also based on the identity management module of the computing environment base image, configures the analysis environment, and runs the data analysis program as a user, ensuring the security of experimental data access. The IP address list of these collaborative containers will be sent to the user's JupyterLab container after these containers are created, and the user can access these collaborative containers directly with ssh-key from JupyterLab container. The complete user login and container creation process is shown in Figure 1.

4 Summary and conclusions

The HEPS computing platform has been deployed in the test environment and is available to users. It currently supports multiple data analysis applications in the fields of spectroscopy, diffraction and imaging. As shown in Figure 2, after the user enters the interactive interface, he or she can directly access the experimental data based on the user's identity, ensuring the access security of the experimental data.

References

- [1] HEPS, <http://english.ihep.cas.cn/heps/ah/bi/>, online, accessed on 20-Sep-2023
- [2] Object vs. File vs. Block Storage: What's the Difference, <https://www.ibm.com/blog/object-vs-file-vs-block-storage/>, online, accessed on 20-Sep-2023
- [3] KV, Aneesh Kumar, Andreas Grünbacher, and Greg Banks. "Implementing an advanced access control model on Linux." Linux Symposium. 2010.
- [4] JupyterLab, <https://github.com/jupyterlab/jupyterlab>, online, accessed on 20-Sep-2023
- [5] Z2jh, <https://z2jh.jupyter.org/en/stable/>, online, accessed on 20-Sep-2023
- [6] Leipold C. Kerberos[J]. Linux Journal, 1999, 1999(68es): 30-es.