Implementation of zero trust security strategy in HEPS scientific computing system

Qingbao Hu, Jiping Xu, Yaosong Cheng, Qi Luo

huqb@ihep.ac.cn, Institute of High Energy Physics, CAS

1. Introduction

Traditionally, data centers provide computing services to the outside world, and their security policies are usually separated from the outside world based on firewalls and other security defense boundaries. Users access the data center intranet through VPN, and individuals or endpoints connected through remote methods receive a higher level of trust to use computing services than individuals or endpoints outside the perimeter. But this approach to security design is never ideal. Zero Trust security is based on de-peripheralization and least-privilege access, which protects intranet assets and services from vulnerabilities inherent in the network perimeter and implicit trust architecture.

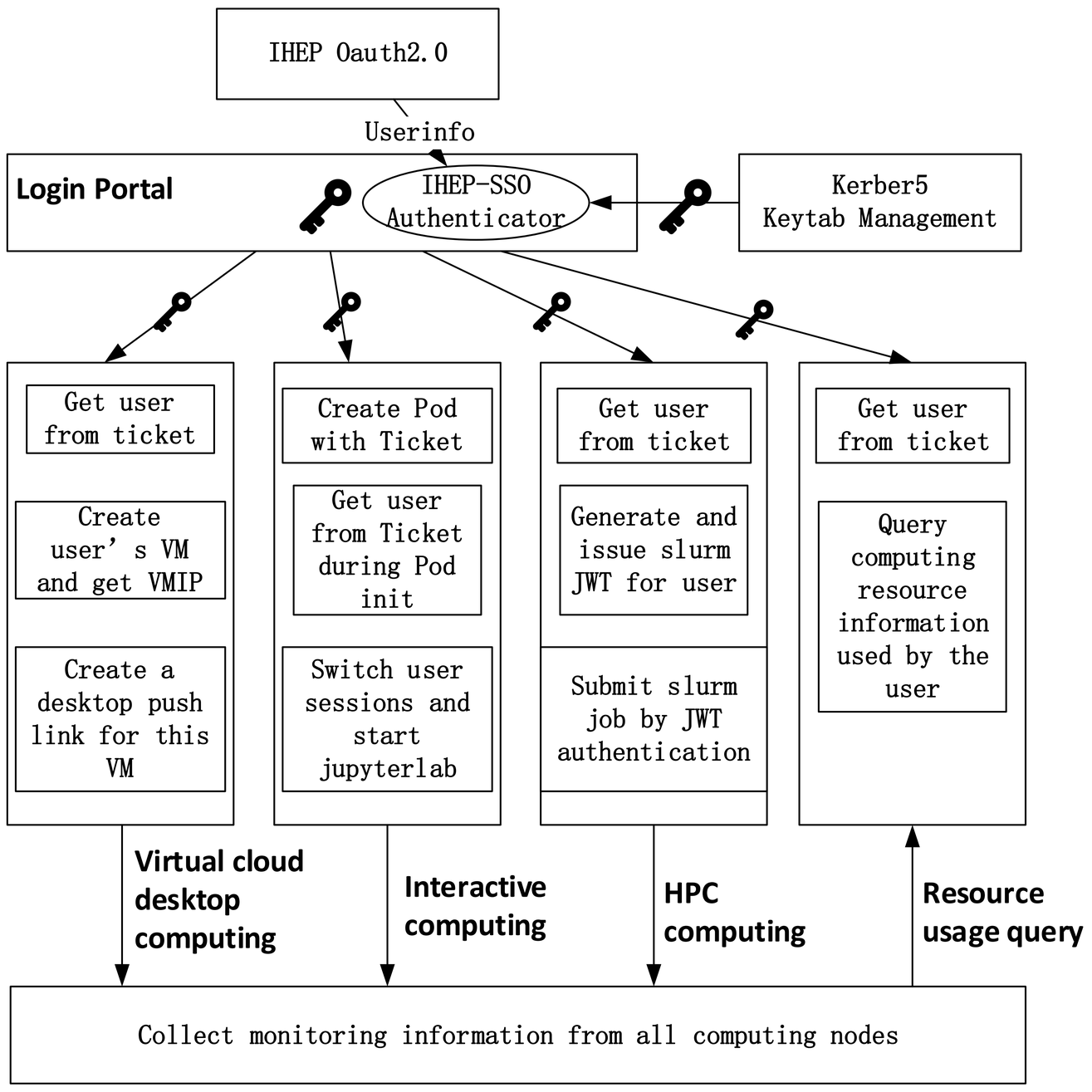
To meet the diverse data analysis needs of light source users, the HEPS scientific computing system provides an interactive computing service model for external network users. Users can directly access computing resources through web pages by multiple computing services, which include virtual cloud desktop services, interactive computing services, and HPC computing services. In these service models, how we refer to the zero-trust security idea, has become very urgent to realize the minimum permission access between various services of the computing system and improve the security level of the system environment. Based on the zero-trust security strategy, this poster designs an inter-service communication mechanism based on user identity tokens. During the function call process between different services, service permissions are allocated based on the token user identity to achieve fine-grained management of service permissions and ensure the Cybersecurity of HEPS scientific computing systems.

2. Design and implementation

The HEPS interactive computing platform provides users with a login portal based on the web page. Users use IHEP accounts based on oauth2.0 to log in to the web and use computing services. As a module that independently implements the identity recognition service function, the login module is responsible for the user's first identity recognition and identity ticket acquisition functions. Users use this module to call other modules that provide specific computing service functions to use computing services.

Users use the virtual cloud desktop computing service process: The virtual cloud desktop service manages computing resources based on OpenStack, provides computing services to users in the form of virtual machines, and enables users to directly operate virtual machine desktop services based on the web by pushing the desktop video streaming protocol. When users use the computing service, they use the ticket as additional information to access the cloud desktop service web address. After the cloud desktop service module parses the ticket to determine the user's identity, it establishes a stable virtual machine desktop video stream with the user's web interface, making the user's access personal. virtual machine desktop resources.

Users use the interactive computing service process: The interactive computing service manages resources based on Kubernetes, provides computing services to users with container access, and provides data analysis functions based on jupyterLab. When the user uses the computing service, the ticket is used as additional information to create the container environment. When the container image is started, the current user's uid/gid identity is switched based on the incoming ticket, and the jupyterLab service process is started as the current user. Restrict users' access rights when using computing services.



Users use the HPC batch computing service process: The HPC batch computing service manages resources based on Slurm and provides computing services by submitting batch jobs. When users use this computing service, they first exchange the user's corresponding JWT file based on the user's identity ticket and then use JWT to submit the HPC job, thereby realizing the function of limiting the user's identity in the job submission process.

User query resource usage process: When users use HEPS computing resources, the resource information they occupy will be recorded in detail and the query function will be provided through the interface. When the user uses this service, the ticket is used as an additional attribute to query the resource monitoring information. After verifying the user's identity, the module returns the resource monitoring information used by the user and some shareable public information.

3. Conclusion

Based on the kerberos5 ticket authentication method, the HEPS computing platform has designed and implemented an identification scheme based on krb5 ticket. Based on the user ticket management mode, the Web application layer and other computing service providing modules realize the independent authentication function of user identity. Each service module allocates service permissions based on user identity to achieve fine-grained management of service permissions and ensure the network security of the HEPS scientific computing system.