Contribution ID: **14** Type: **Oral Presentation**

A Self-service Authentication and Access System for Computing Cluster (Remote Presentation)

Friday, 29 March 2024 11:10 (20 minutes)

Keywords: cluster computing, account passport, secure shell (SSH), lightweight certificate, remote access, SSH tunnel

Advanced computing infrastructure such as high-performance clusters, supercomputers, and cloud computing platforms offer unparalleled computing capabilities and effectively support a multitude of computing requirements across diverse fields such as scientific research, big data analysis, artificial intelligence training and inference, and many more. Secure Shell (SSH) is a widely used method for accessing remote computing resources, It not only provides command-line tools, but also offers rich textual and graphical interfaces based on tunnel and port forwarding, allowing users to access components and services located on remote servers. Nowadays, there are numerous methods for remotely accessing computing resources, for example, utilizing a simple password, utilizing a password enhanced with VPN, utilizing a static password and a dynamic token provided by hardware, utilizing a public key in software or hardware, and utilizing a token provided by a mobile application. However, these methods have several drawbacks, including network inefficiency resulting from VPN, high costs associated with dedicated hardware, and security concerns such as brute-force attacks. These issues have caused not only a detrimental experience for users but have also burdened administrators with unwarranted maintenance tasks and complexities.

Addressing the aforementioned issues and aiming for efficient and secure access to computing resources, this paper proposed the establishment of an authentication chain consisting of a CSTNET Passport and an SSH lightweight certificate. CSTNET Passport is primarily utilized in web-based services and similar contexts, providing support for single sign-on and multi-factor authentication, thereby exhibiting robust security and user-friendliness. Nevertheless, its adaptability in non-web-based scenarios, particularly in SSH command line utilities, remains limited. An SSH lightweight certificate system eliminates the need for users to remember intricate passwords or engage in frequent password changes. Additionally, it circumvents the drawbacks associated with the decentralized deployment and long-term effectiveness of the public key system. This paper introduced an authentication and access model that effectively combines the initial login process using the CSTNET Passport with the subsequent login utilizing the SSH lightweight certificate, either directly or through multiple jumps. The model outlines procedures for users to issue lightweight certificates and configure SSH clients, as well as guidelines for administrators in configuring SSH daemons, mapping passport and local account pairs, and other related tasks. It facilitates on-demand authentication and access flows. To enhance security, the model restricts the time window, narrowing it from an unrestricted period to a specific time range designated by the user. This paper also introduced a dynamic firewall model that transparently acquires the network address of the browser client and the validity period of the certificate. It then forms IP address and time range metadata, and dynamically adds firewall policies. To enhance security, it narrows the scope of allowed IP addresses from any IP to a specific IP address or list based on whether the user possesses a public IP address or a NAT address. These two models substantially diminish the time and space windows available for network attacks. Moreover, they accomplish this enhancement without incurring extra expenses for additional software, such as VPNs, or hardware, like token cards.

Leveraging these models, this paper has developed a self-service authentication and access system, which comprises two integral parts: a web application subsystem and a toolset subsystem. The web application subsystem facilitates passport login, account mapping, certificate issuance, and status inquiry for both users and administrators. The toolkit, on the other hand, equips users with key generation, public key uploading, certificate downloading, and dedicated files within an SSH client. Additionally, it offers CA certificates and principal configuration tools for SSH login servers, while also providing optional SSH connection status profiling capabilities for administrators.

Leveraging open-source and free software solutions, such as Nginx, OpenSSH, and MobaXterm, the system software has been developed with a comprehensive utilization of HTTPS/TLS protocols, port multiplexing, and NJS scripts. It fully supports SSH command line operations, tunneling, and port forwarding in both direct and multi-hop modes.

Since 2023, the system has been successfully deployed to a cluster consisting of one login node and 20 computing nodes, effectively supporting self-service authentication and secure access for hundreds of users. The

system changes access from anytime and anywhere to on-demand access with various restrictions specified by users, and also transfers controls from administrators to users. Users have the ability to decide when and where to access the server with specified permissions. The system is easy to deploy, occupies fewer resources, does not introduce extra hardware costs, and can effectively increase the usability and security of computing resource. In future, this paper will focus on optimizing and strengthening the functionalities pertaining to firewall policies and SSH connections.

Primary authors: WANG, Jue (Computer Network Information Center, CAS); CAO, Rongqiang (Computer Network Information Center, Chinese Academy of Sciences); Mr LI, Kai (Computer Network Information Center, Chinese Academy of Sciences.); Mr WAN, Meng (Computer Network Information Center, Chinese Academy of Sciences.); Mr WANG, Xiaoguang (Computer Network Information Center, Chinese Academy of Sciences.); CHI, Xuebin (Computer Network Information Center, Chinese Academy of Sciences)

Presenter: CAO, Rongqiang (Computer Network Information Center, Chinese Academy of Sciences)

Session Classification: Network, Security, Infrastructure & Operations

Track Classification: Track 7: Network, Security, Infrastructure & Operations