Title:

Rethinking Interactive HPC Resource Access: Enhancing Security and Flexibility

Abstract:

The traditional approach to accessing HPC resources relies on login nodes and SSH connections authenticated through POSIX Identity and Access Management (IAM). While this method has served the community well, it presents significant challenges in today's landscape of cybersecurity threats and evolving user needs, such as maintaining a secure shared login node or managing identity life-cycle. This Birds of a Feather (BoF) session aims to explore innovative approaches to modernize interactive HPC resource access with CLI, addressing the dual goals of enhancing security and increasing service customization flexibility for users. Emerging practices, such as SSH signed keys, offer a promising alternative to traditional login names and passwords, mitigating risks associated with credential theft by enabling more advance authentication flow like multi-factor authentication. Virtualized login nodes, implemented as containerized environments, could allow user-defined environments with for instance advanced debugging capability, AI stacks or a higher integration with IDE while improving isolation, scalability of users, and individual session management. Additionally, the generation of temporary POSIX accounts from OpenID Connect (OIDC) tokens could seamlessly integrate modern federated and non-local identity providers, reducing administrative overhead and attack surfaces. The session will showcase existing solutions, discuss opportunities for innovation, challenge classic IAM HPC and login nodes workflow and highlight the potential benefits of these new approaches. Attendees will hear from practitioners actively exploring these paradigms, sparking discussions on how the community can collectively advance this shift and benefit for a common solution. We invite participants to contribute their ideas, share experiences, and help shape a future where interactive HPC resource access is not only more secure but also more adaptable to the diverse and continuously evolving needs of its users.

Organiser:

CSCS has implemented MFA by introducing SSH services and SSH-signed keys [1] as the sole method for accessing login nodes. BriCS has adopted a similar approach, enhancing user management by generating POSIX accounts [2] on login to eliminate the need for manual identity management. Additionally, HPE has introduced the concept of User Access Node (UAN) [3], which function as on-demand containers for login nodes.

Maxime Martinasso (CSCS), Sadaf Alam (BriCS), Isa Wazirzada (HPE)

[1] SSH service: https://confluence.cscs.ch/display/KB/3.+Connecting+to+CSCS+systems+through+MFA

[2] BriCS IAM: https://docs.isambard.ac.uk/user-documentation/guides/login/

[3] HPE UAN:

https://support.hpe.com/hpesc/public/docDisplay?docId=crs8033_6en_us&docLocale=en_US

Agenda:

To kick off the session, we will have three brief 5-minute presentations introducing key concepts: the CSCS SSH service, BriCS identity management approach, and the HPE User Access Node (UAN) concept. Following these presentations, we will present a list of thought-provoking questions to ignite discussion and encourage debate:

- How can HPC centers transition away from POSIX IAM while ensuring secure and seamless data ownership models?
- What steps are required to integrate modern authentication methods, such as biometric authentication (e.g., Face ID), into login workflows for HPC resources, and what challenges must be addressed?
- What technical and operational considerations are needed to provide containerized login instances that support session management, user customization, and scalability?
- What security measures are necessary to ensure the safe deployment of arbitrary containers as login sessions?
- Which HPC centers are willing to collaborate on establishing common principles and developing shared solutions for modernizing IAM and resource access workflows?
- What strategies can be implemented to transition users from traditional permanent resource-provider-managed identities to temporary, session-based access models? How can user adoption and satisfaction be measured during this shift?