SETOSS: Multi-Tenant HPC with Security Enhanced Linux on TOSS

Lindsey Whitehurst, T. D'Hooge, J. Foraker (LLNL)

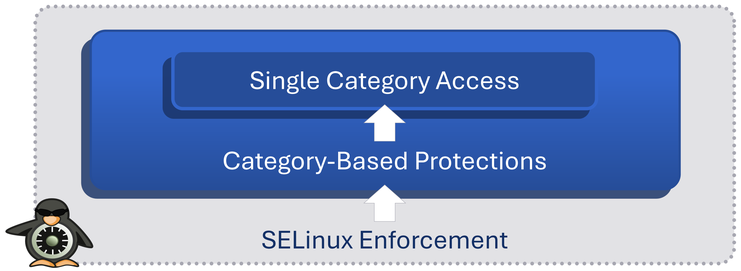
High-performance computing (HPC) systems often waste resources, increase costs, and slow down projects because traditional setups separate security zones and require dedicated clusters for each project.

The SETOSS (Security Enhanced Linux on TOSS) project solves this by testing a new way to run TOSS HPC clusters using SELinux in Multi-Category Security (MCS) mode. This allows multiple projects to securely share HPC resources, ensuring strict data separation while improving efficiency and reducing costs.

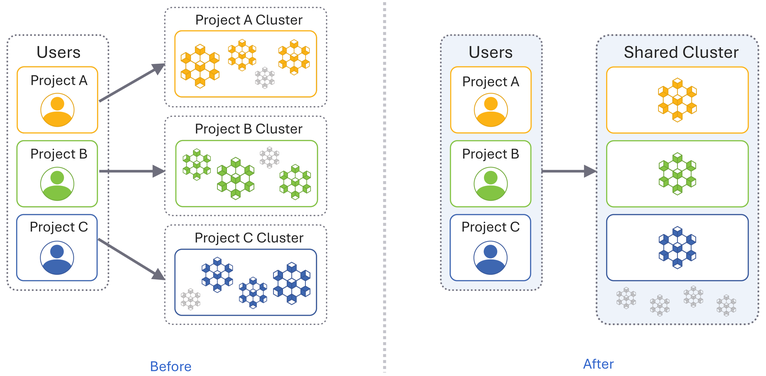
This is a 2-year project funded at 1FTE.

Goals

Access Structure



Cluster Architecture



Security Features

Access Control and Administration	• Strict Login Controls: Linux security features ensure only authorized groups gain access. • Centralized Administration: A single admin team oversees all categories, minimizing the risk of data mixing.
Zero-Trust Security Enforcement	• Zero-Trust Security: Kernel-level mandatory access control ensures strict, zero-trust enforcement. • Unified Policy: A single security policy is consistently applied across all nodes.
Infrastructure Isolation	• Job Isolation: User-Based Firewall [1] prevents unauthorized cross-category access. • Secure Networking: InfiniBand networks are partitioned and secured by category assignment. • Restricted Access: Fileservers are accessible only from within the cluster.

[1] https://github.com/mit-llsc/UserBasedFirewall

Testing Strategy

Infrastructure as Code Testing:

- Critical for foundational system integrity: validates Ansible logic for SETOSS role.
- Tools: Ansible Molecule, GitLab CI.

Per-Job Testing:

- Essential for job-level security, validating Slurm job isolation and enforcing strict firewall rules to prevent cross-category data leaks.
- Tools: Slurm Prolog, User Based Firewall.

Manual Testing:

- Critical for comprehensive system validation, ensuring SELinux enforcement, policy integrity, filesystem labeling, and data separation are uncompromised.
- Tools: Restorecon, manual checks.

Conclusions

The SETOSS initiative demonstrates the feasibility of running TOSS HPC clusters as multi-category systems using SELinux in MCS mode. LLNL's experience with scalable HPC architectures, security zone management, and SELinux was critical in the development of this initiative. By addressing the challenges of resource underutilization and security, SETOSS paves the way for more efficient and secure HPC systems, ensuring that computational resources are optimized for advanced research.

Next Steps

- Evaluate and incorporate emerging and cloud technologies
- Enhance integration with HPC schedulers to optimize resource allocation and job scheduling
- Improve user experience through further SELinux abstractions

SETOSS uses LLNL's expertise in HPC and security to deliver a secure multi-tenancy solution, facilitating larger jobs on shared resources while enforcing strict data protection

Lawrence Livermore National Laboratory

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-POST-2004324

National Nuclear Security Administration