TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

Alexander Grund
Center for Information Services and High Performance Computing (ZIH)

A Secure Workflow for Shared HPC Systems

10th EasyBuild User Meeting, Jülich
25th March 2025

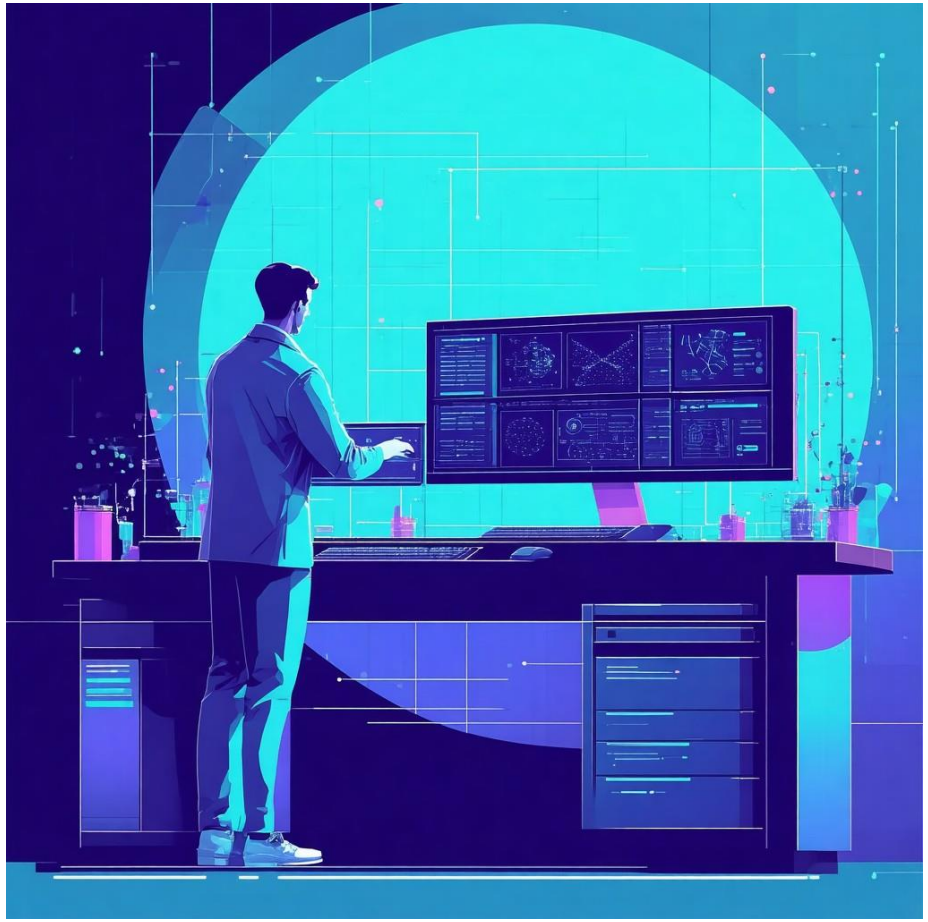
Motivation

1. Researchers require larger machines
   – Compute intensive methods
   – More / Longer analysis

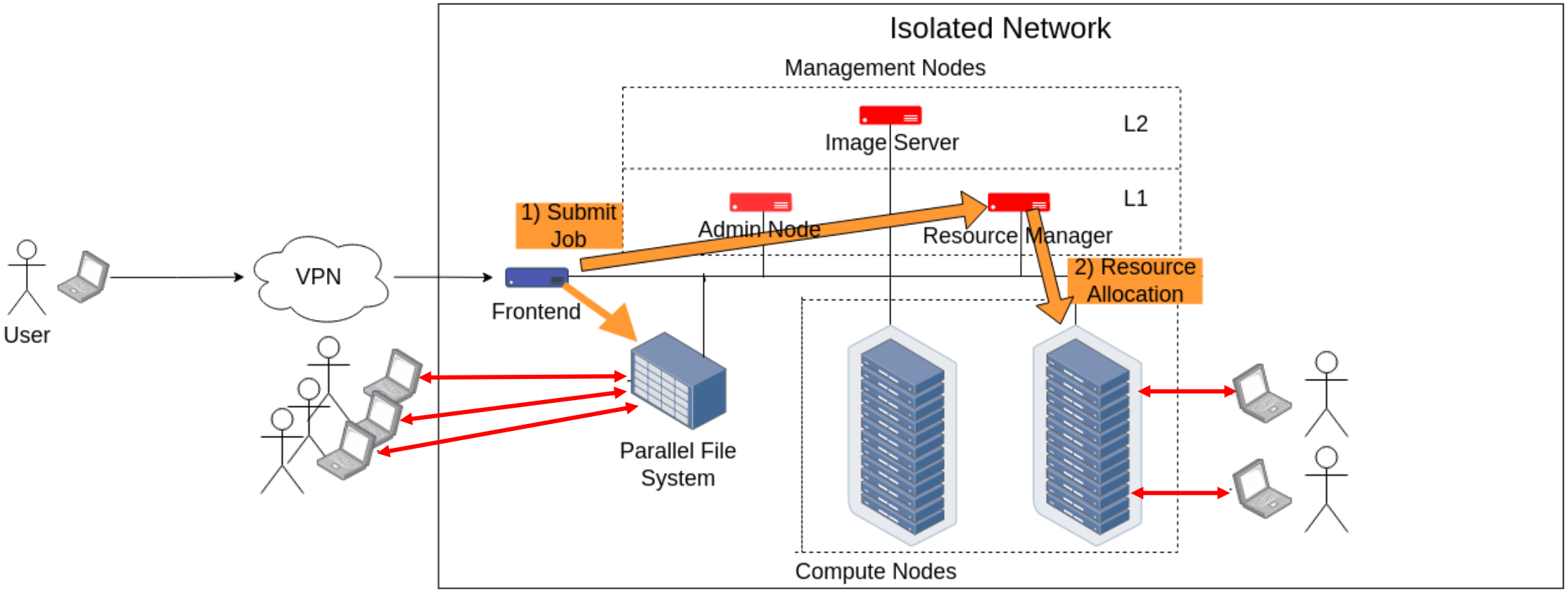
2. Shared infrastructure
   – Split responsibility
   – Cost reduction

➔ Move to HPC

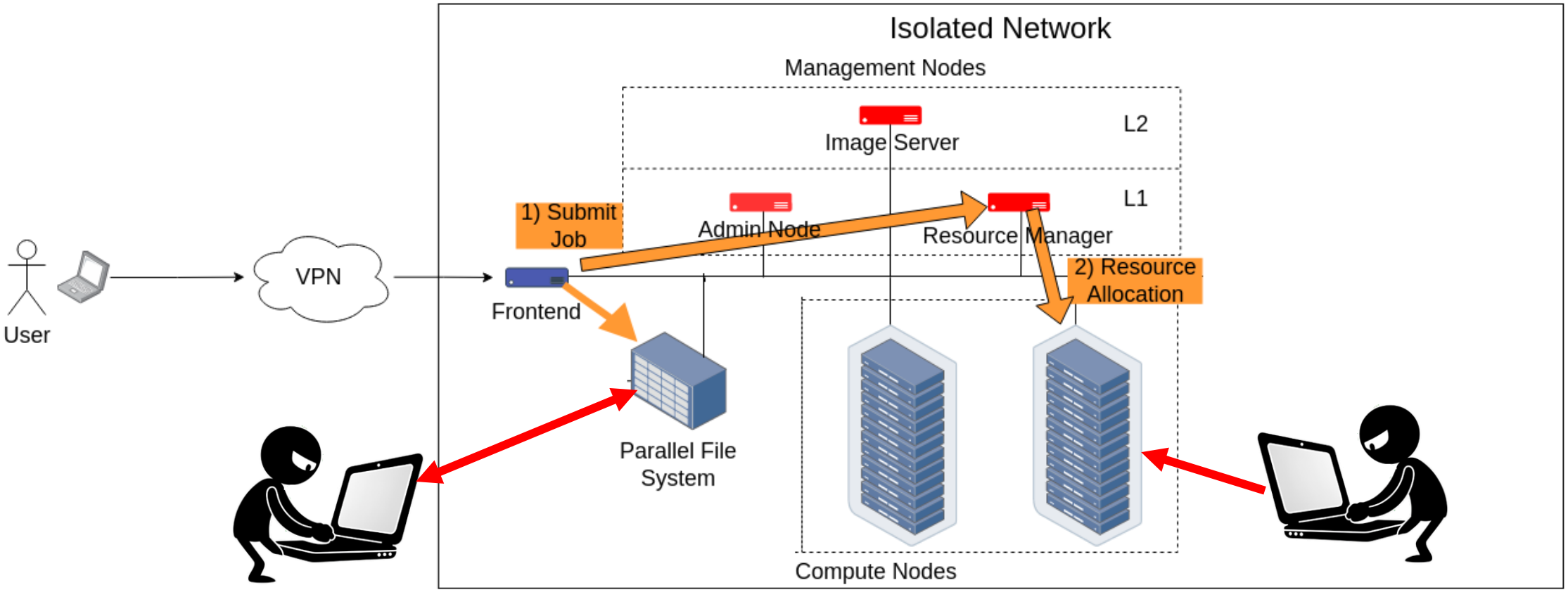
Sensitive Data needs to be secure!



Motivation


Isolated Network
Management Nodes
L2
Image Server
L1
1) Submit Job
Admin Node
Resource Manager
2) Resource Allocation
VPN
User
Frontend
Parallel File System
Compute Nodes

Motivation


Isolated Network
Management Nodes
L2
Image Server
L1
1) Submit Job
Admin Node
Resource Manager
2) Resource Allocation
User
VPN
Frontend
Parallel File System
Compute Nodes

Challenges

Data on shared (global) filesystem:

Access by Admins with root access ➔Attacker can gain root
Access by other users

Data on Compute Nodes

Access by users on the same node ➔Insufficient access protection of temporary data
SSH access ➔Spoofed/compromised UID allows access

Software

Modules installed by Admins ➔Stored on global filesystem
Containers provided by users
System software / OS on node ➔Manipulated by previous users

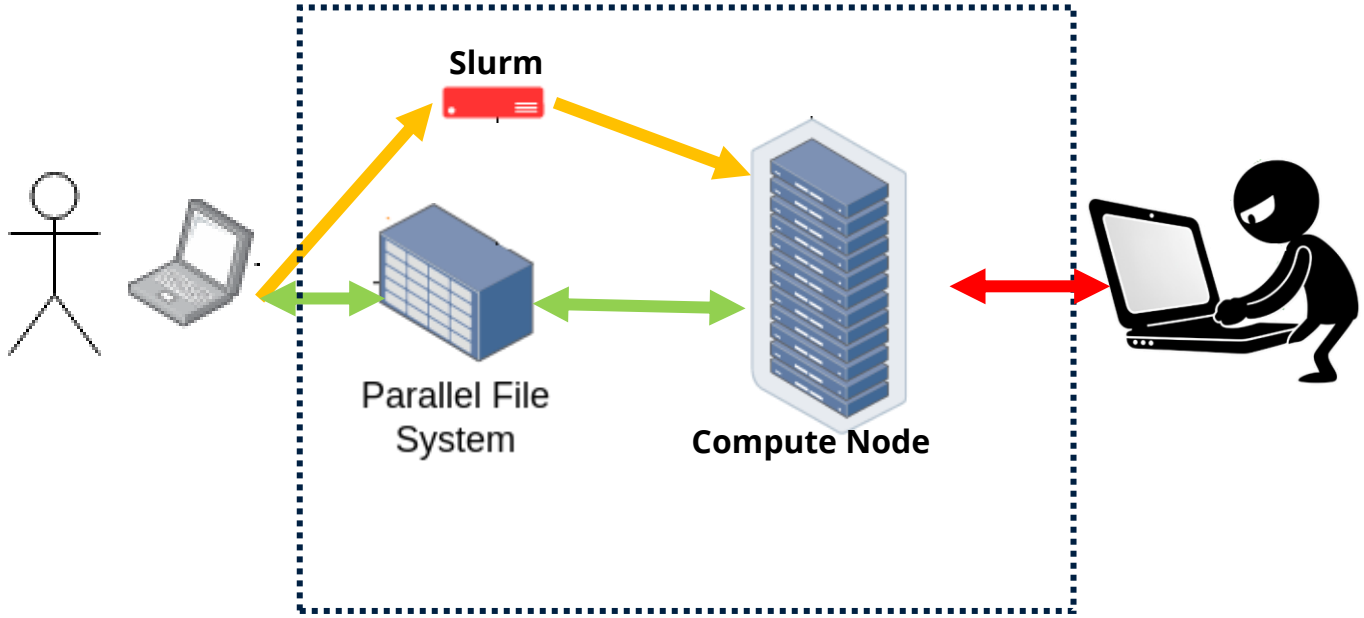
Solution

Generic Workflow

1. Protect data on global filesystem
2. Secure Node against unauthorized access
3. Ensure integrity of used software

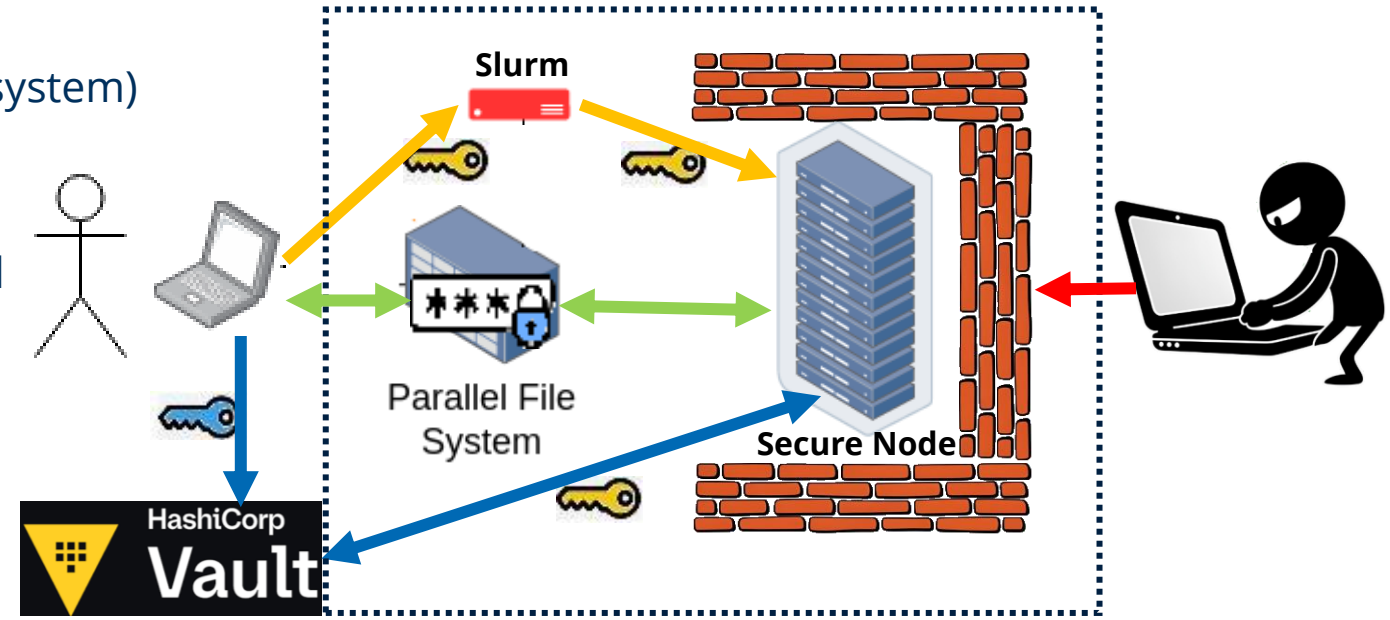
Assume secure…

– Image Server
– Boot process
– Local user system



Solution

1. **Isolated node**
   - No SSH access
   - Only known connections allowed (SLURM, filesystem)
   - Requires ***signed*** SBatch script
2. **Data resides in *LUKS* containers**
   - Transparent mount → Read & Write encrypted
   - Secure symmetric key generated
   - Data moves only in container
3. **Software provided in Singularity image**
   - Asymmetric encryption ensures authenticity
4. **Key transfer via KMS**
   - Single-use token in exchange for keys
   - Encrypted in SBatch script



Summary

Data confidentiality by encryption

— Only unencrypted on “Secure Client”

— Transparent en-/decryption during processing on “Secure Node”
  – No leaks
  – Compatible with existing workflows

No access to “Secure Node” by other users

— Ensured through signatures

— No modification of OS / scripts / …

— Data mount only accessible by intended user

Resistant to many user errors

— Scripts for secure key generation and encryption

— Short-lived access tokens instead of keys on HPC

References

— Nolte, Hendrik, Simon Hernan Sarmiento Sabater, Tim Ehlers, and Julian Kunkel.
"A Secure Workflow for Shared HPC Systems.“
In 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid), pp. 965-974. IEEE, 2022.

— Trevor Khwam Tabougua, GWDG presentation https://events.gwdg.de/event/415/