HPC Secure Data Account General Use Guidelines and Information

The HPC secure data environment provides compute resources for secure data with minimum end-user overhead. The following guidelines ensure that the secure data stored with HSDAs remains secure. Please review the following information carefully, as failure to comply could result in the suspension or termination of your HSDA.

As a member of an HSDA, you are responsible for adhering to the use guidelines detailed below. If you have any questions, email hpc@usc.edu.

Guidelines

Enroll in Duo

All members of an HSDA must enroll in Duo two-factor authentication, which provides an extra level of security for your account. You can enroll in Duo at itservices.usc.edu/duo.

Access HSDA via USC Secure Network or VPN

The HSDA login node must be accessed from the USC wired network, the USC Secure Wireless network, or through the USC VPN AnyConnect client, available for download at itservices.usc.edu/vpn.

Secure Login/Head/Transfer Node

Hpc-login-pd.usc.edu is the only login/head/transfer node to be used with an HSDA, and only members of an HSDA can log into hpc-login-pd.usc.edu. This node is configured to create a secure environment that will automatically encrypt and decrypt secure data stored in your HSDA project directory, as well as your home directory HSDA environment dot files. You must use this head node for secure data transfers, editing, compiling, short tests, and submitting jobs to the clusters.

NOTE: When logging into hpc-login-pd.usc.edu, you will experience a delay in getting to the system prompt as the secure environment is being launched and your secure data mounts are activated.

For all data transfers, **scp** from Linux or Mac systems is the only command currently available. If you have additional needs, please email hpc@usc.edu.

Store All Secure Data in the HSDA Project Directory

All secure data should reside in the HSDA project directory. Secure data stored in a home directory is a security violation.

Additional Information

Secure Environment

The secure environment created upon logging in to the HSDA login node enables automatic encryption/decryption of all data stored in the HSDA project directory and any data written to your home directory. Exiting the login node will tear down this environment and terminate all user processes running on the login node.

Secure Compute Nodes

Currently, there are 200 compute nodes on the Infiniband cluster that are available for HSDA processing. These nodes are shared with all general account researchers and, as such, utilize the same rule sets.

Inactivity Timeout

There is a mandatory 20-minute inactivity timeout for a login session.

qint Command

Compute jobs require the creation of the HSDA secure environment to run jobs. To launch the secure environment for an interactive job, use of the **qint** command is required. It accepts all standard **qsub** options.

Example:

```
qint –A account_name [ -l nodes=x:ppn=y … ]
```

Batch jobs

Use qsub command to submit batch job scripts. Additionally, add the “hsda” property to resource requests. An example script:

```
#!/bin/bash
#PBS -l nodes=1:ppn=8:hsda
#PBS -A lc_xxx ## your account name
#PBS -N job_name
#PBS -j oe

cd $PBS_O_WORKDIR
#run job
```

For additional information on using any HPC account, including HSDAs, see the following links on the HPC website:

- New User Guide: hpcc.usc.edu/support/documentation/new-user-guide
- Frequently Asked Questions: hpcc.usc.edu/support/documentation/faq

- HPC Computing Workshops: hpcc.usc.edu/support/hpcc-computing-workshops

In addition, we are happy to assist you in person with any questions you may have during our office hours. The current office hours are listed on the HPC website at hpcc.usc.edu/officehours.

If you have any other questions, please email hpc@usc.edu.