Getting Started Guide for Predictive Science Academic Alliance Program (PSAAP) Users

Authors: Blaise Barney (LLNL), Rob Cunningham (LANL), Karen Haskell (SNL), Lilia Martinez (SNL)

May 22, 2014

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

Lawrence Livermore National Laboratory is operated by Lawrence Livermore National Security, LLC, for the U.S. Department of Energy, National Nuclear Security Administration under Contract DE-AC52-07NA27344.

Contact

Blaise Barney, Lawrence Livermore National Laboratory
925-422-2578
blaiseb@llnl.gov

User Information for Lawrence Livermore National Laboratory

Point of Contact: Blaise Barney, 925-422-2578, blaiseb@llnl.gov

Available Machine Resources

asc.llnl.gov/alliances/alliances_resources.php

Requesting an Account

See the "Requesting Tri-Lab Accounts" section at the end of this document.

Essential Information for Livermore Computing (LC) Users

- computing.llnl.gov**:** Covers everything users need to know for using LC's machines. Most pages are open to the world; those that aren't require authentication via a valid LC account.
- computing.llnl.gov/tutorials/lc_resources**:** A "getting started" tutorial that should be reviewed by all new users. Please distribute this URL to your center's users also.

Accessing LC Compute Resources

After account activation and receipt of LC's OTP password token, users access LC's computers with SSH. More information: computing.llnl.gov/tutorials/lc_resources/#Access

User Documentation

computing.llnl.gov
computing.llnl.gov/tutorials (especially the BG/Q and Linux clusters tutorials)

User Hotline Support

- Phone, Email and Walk-in: Monday through Friday, 8:00 am–noon, 1:00–4:45 pm PST
- Off-hours and weekends support provided by LC Operations staff
- Technical assistance: 925-422-4531 or lc-hotline@llnl.gov
- Passwords, accounts, forms: 925-422-4533 or lc-support@llnl.gov

Collaboration Tools

All LC users have access to these Atlassian collaboration tools:

- Confluence Wiki: https://lc.llnl.gov/confluence
- Jira Bug Tracker: https://lc.llnl.gov/jira
- Stash Source Code Manager: https://lc.llnl.gov/stash

User Training

LC provides online tutorials, hands-on workshops (both on-site and off-site) and seminars:
computing.llnl.gov/training

User Information for Los Alamos National Laboratory

Point of Contact: Rob Cunningham, 505-665-4444 x05704, rtc@lanl.gov or consult@lanl.gov

Available Machine Resources

asc.llnl.gov/alliances/alliances_resources.php

Requesting an Account

See the "Requesting Tri-Lab Accounts" section at the end of this document.

Essential Information for LANL High Performance Computing (HPC) Users

- All LANL user information is accessible via LANL cryptocard at: ssl-portal.lanl.gov. Instructions for accessing website are here: http://www.lanl.gov/projects/computing/web_hpc.html
- hpc.lanl.gov covers everything users need to know for using LANL HPC clusters. This entire site requires authentication via a valid LANL cryptocard. Please pass this URL along to users of LANL at your center.
- http://int.lanl.gov/projects/asci/training/Intro/: A "getting started" tutorial that should be reviewed by all new users. Requires cryptocard login. Please distribute this URL as well.

Accessing LANL Compute Resources

After account activation and receipt of LANL OTP password token, users access LANL HPC clusters with SSH. To reach the LANL clusters:

- ssh to the firewall/gateway: `wtrw.lanl.gov` and authenticate with your username and Cryptocard passcode
- Use ssh to reach a front-end node: `mp-fe.lanl.gov`, `mu-fe.lanl.gov`, etc
- For additional information and assistance, contact User Support

Computing Resources

http://hpc.lanl.gov/summary_table (requires cryptocard authentication)

User Training

LANL provides online tutorials, hands-on workshops (both on-site and off-site) and seminars: http://int.lanl.gov/projects/asci/training (requires cryptocard authentication)

User Support—ICN Consulting Office

- Phone, Email and Walk-in: Monday through Friday, 8:00 am–noon, 1:00–5:00 pm MST
- Off-hours and weekends support provided by LANL Operations staff
- Technical assistance: 505-665-4444 option 3 or consult@lanl.gov
- Cryptocard, accounts, forms: Frances Castellano, 505-665-1371, fea@lanl.gov or Lori Kelley, 505-665-1517, lorik@lanl.gov

User Information for Sandia National Laboratory

Point of Contact: Karen Haskell, khaskel@sandia.gov

Available Machine Resources

asc.llnl.gov/alliances/alliances_resources.php

Requesting an Account

See the "Requesting Tri-Lab Accounts" section at the end of this document.

Essential Information for LANL High Performance Computing (HPC) Users

- http://hpc.sandia.gov provides basic information about Sandia HPC systems; these web pages are open, though some links require authentication with the Sandia CRYPTOCard.
- https://computing.sandia.gov covers everything users need to know for using Sandia's HPC clusters. This entire site requires authentication with a Sandia CRYPTOCard. Information for specific platforms can be found under the "Platforms" tab.

Accessing SNL Compute Resources

After account activation and receipt of your Sandia CRYPTOCard, users access cluster login nodes with SSH. To reach Chama or Glory:

- Connect to Sandia Secure Restricted Network (SRN) via gateway: ssh <sandia-username>@srngate.sandia.gov
- Read the "WARNING NOTICE TO USERS" message; then enter your CRYPTOCard password
- From Welcome menu, select "kinit" to Acquire kerberos credentials and enter Kerberos password, then select "ssh" to establish an SSH connection
- Enter desired system name, e.g. "chama" or "chama-login[1-8]," or "glory" or "glogin[1-2]"
- A Workload Characterization (WC) ID is required to run batch jobs; request WC ID from your Sandia contact, and use it as your "account" for batch job submissions.

Computing Resources

computing.sandia.gov/platforms (requires CRYPTOCard authentication)

User Support—HPC OneStop

- Sandia HPC OneStop Portal at https://computing.sandia.gov (requires CryptoCARD authentication)
- Phone: Monday through Friday 8:30 am–4:30 pm Mountain, (505) 844-9328 or (505) 845-2243 Option 8
- Email: HPC-Help@sandia.gov
- Off-hours and weekends support provided by Sandia Operations staff for emergencies only

Requesting Tri-Lab Accounts

All PSAAP accounts for Tri-lab compute resources must be requested through the web-based SARAPE account request system at http://sarape.sandia.gov. Note that SARAPE is domain restricted to participating PSAAP centers, so it must be accessed from your university's network (utah.edu, stanford.edu, etc). When you access SARAPE, you will begin the account request process by entering a valid email address, which needs to be in your university's domain. Following this, you will need to complete the request form. Most fields are self-explanatory, but some useful hints are provided below:

- Step 2: Requestor's Manager's Info: this pertains to your PSAAP center's designated SARAPE processing agent - that is, the person within your center who authorizes your center's account requests.

- Step 3: Select the Lab where you would like an account and the available machines will appear. If you mouse-over the blue "i" icon next to the machine name, additional information about that machine will appear.

- Step 4:Additional information: For the required "Justification" box, please indicate the name of your PSAAP center and what your work will pertain to.

Following completion of the form, your request will be reviewed by your center's SARAPE processing agent, and if approved, it will then be sent to the Lab(s) where you requested an account. The review and approval process at each Lab varies, but averages about one week for US citizens. Non-US citizens are required to submit additional paperwork, initiated after the SARAPE request is received at the host site, and requires additional approvals. Processing time for these also varies, between one and three months.

Passwords/Tokens

Each laboratory has its own tokens and/or passwords for access to its resources, so if you have accounts at multiple sites you will receive them separately. After accounts are approved and issued, each laboratory has its own process for providing/sending your password and/or token.

Training

All laboratories require users to take online cyber security training on an annual basis. If this required training is not completed, machine accounts will be deactivated.

Account Reauthorization

All three laboratories require annual reauthorization of existing accounts. You will be notified via email regarding this process when your account renewal date approaches.