Access and Login to SuperMUC-NG

- Getting Access
- Login to SuperMUC-NG
  - Login with Secure Shell
  - Login via Grid Services using GSI-SSH
  - Reporting problems with Login
- Password Policies
- Changing password or login shell, viewing user account data
- User centered-usage model
- Programming Environment
- Moving data from/to SuperMUC
- Access to Subversion (SVN) and Git servers

Getting Access

Researchers who do not have an SuperMUC-NG account need to apply for a project, and need to undergo a review process. Use the Online Proposal Forms in

- Application for a project on SuperMUC-NG

Questions concerning the usage should be directed to the Servicedeck for SuperMUC-NG.

Login to SuperMUC-NG

Before you can login to SuperMUC you have to set your own password and accept the usage regulations.

Login with into the ID-Portal (https://idportal.lrz.de/r/entry.pl?Sprache=en) using your account and the start password that we have delivered to your project manager.

SuperMUC-NG uses login nodes for interactive access and for the submission of batch jobs. The login nodes have an identical environment, but multiple sessions of one user may reside on different nodes which must be taken into account e.g., when killing processes.

Two mechanisms are provided for logging in to the system; both incorporate security features to prevent appropriation of sensitive information by a third party.

Login with Secure Shell

Access via SSH (Secure Shell) is described in detail in the LRZ Document about SSH. In particular, the setup required to use private/public keys for access is described there. From the UNIX command line of the user's workstation the login to an LRZ account xxyyyzz is performed via:

<table>
<thead>
<tr>
<th>System part</th>
<th>Login</th>
<th>Architecture</th>
<th>Number of nodes behind the round-robin address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login node for SuperMUC-NG Phase 1</td>
<td>ssh -Y skx.supermuc.lrz.de -l xxyyyzz</td>
<td>Intel Skylake</td>
<td>3</td>
</tr>
<tr>
<td>Login nodes with connection to the tape archive</td>
<td>ssh -Y skx-arch.supermuc.lrz.de -l xxyyyzz</td>
<td>Intel Skylake</td>
<td>4</td>
</tr>
</tbody>
</table>

Note:

- The IP address of your front-end machine must be associated with a valid DNS entry, and must be known to us, otherwise your SSH request will not be routed. Additional entries or changes can be submitted via a modification request using the Online Proposal Form.
- LRZ Security Policies demand that the user's private SSH keys that are used to access the system from the outside world are locked and guarded with a non-empty passphrase, therefore it is not allowed to use an empty passphrase during the private key generation. We consider an empty passphrase as a violation of our security policies. Users disregarding this policy will be barred from further usage of LRZ systems.
- The SuperMUC-NG firewall permits only incoming SSH-connections i.e., ssh or scp from SuperMUC-NG to the outside world is disabled.
- The -Y option is required for tunneling of the X11 (windowing) protocol, it may be omitted if no X11 clients are required.
- Please add the List of ssh key fingerprints for SuperMUC-NG to ~/.ssh/known_hosts on your own local machine before logging in for the first time.
Login via Grid Services using GSI-SSH

An alternative way of accessing the SuperMUC is to use GSI-SSH, which is a component of the Globus toolkit and provides

- terminal access to your account
- a single sign-on environment (no repeated password entry required to access SuperMUC and other machines)

The Globus toolkit provides easy access to additional, handy functionality, including fast, secure file transfer with GridFTP. For more information, please read the LRZ Globus documentation, where you will also find details on how to use gsissh via GridMUC to connect to other parts of SuperMUC-NG.

Reporting problems with Login

To report a problem use the ssh or gsissh command with the "-vvv" option and include the verbose information when submitting an incident ticket to the Servicedeck for SuperMUC-NG.

Password Policies

Passwords must be changed at least once in 12 months. We are aware that this measure imposes some overhead on users, but believe that it is necessary on security reasons, having implemented it based on guidelines of BSI (federal agency for information security) and the IT security standard ISO/IEC 27001. You are able to determine the actual invalidation date for your password by logging into the ID portal (https://idportal.lrz.de) and selecting the menu item "Person -> view" or "Account -> view authorizations". In order to prevent being surprised by a password becoming invalid, you will be notified of the need to change your password via e-mail. Even if you miss the deadline for the password update, this only implies a temporary suspension of your account - you will still be able to log in to the ID portal and make the password change.

- Complete (German) text of the authentication regulations

Changing password or login shell, viewing user account data

The direct use of the passwd and chsh commands to change passwords and login shells, respectively, has been disabled.

Please use the ID-Portal instead:

- Log in to the web interface using your account and password.
- Toggle between English and German: use the little flags
- For changing your password, select "Self Services/modify password". In the main window you are then prompted for your old password once and for the new password (needs to have between 6 and 20 characters) twice.
- For changing your login shell select "Self Services/change login shell". For the platform "SuperMUC" select the new login shell from the drop-down menu. Please only use one of the following shells: bash, ksh, sh, csh, tcsh. Other shells may run into problems with the scheduler.
- The ID portal also offers functionality to view your user account data.

User centered-usage model

The usage model of SuperMUC-NG is user-centered. Each user will have only user account on the systems, via this account all assigned projects can be accessed. Particular attention was paid to data handling: The model enables a user to seamlessly access his or her data in different projects for which he/she is validated. In addition to that, a user can share his or her data with other users within the same project, by giving the project group access to his or her user directory within the project.

The user must select:

- in which project the consumed cpu-hours of the batch job are accounted
- where large datasets are to be stored (i.e., where, in the filesystem WORK)
- the location of the archived datasets in the tape archive

LRZ provides a command to assist users:

- [source] workon info: displays information about groups, quota and budget about all projects the user is assigned to
- source workon [-q] <project>: displays information about the specified project and sets the following environment variables which can be used in subsequent scripts. With -q only the variables are set. (example: source workon pr12xf)

WORK: containing the path the WORK directory of the specified project (example: /gss/work/pr12xf-c/di12faq2)
DSM_CONFIG: containing the path of the configuration for the tape archive (example/etc/adsm/dsm.opt_pr12xf)
ACCOUNT: for which project the cpu-hours and resource are to be accounted (example: pr12xf)
Programming Environment

For controlling other settings and gaining access to the software stack the Modules of the HPC Systems are used. You are strongly urged to read that document, because some additional configuration on your side may be needed and/or required to reliably perform environment setup within batch jobs.

Moving data from/to SuperMUC

FTP access to the high performance systems from outside is disabled for security reasons. You can use:

- globus
- scp
- sftp
- GridFTP

Access to Subversion (SVN) and Git servers

The SuperMUC firewall permits only incoming SSH-connections. You can use port forwarding to establish a connection between the subversion server and SuperMUC-NG,

- Details for Access to SVN and GIT from SuperMUC-NG