Access and Login to SuperMUC-NG

- Getting Access
- Login to SuperMUC-NG
  - Login with Secure Shell
  - 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 a SuperMUC-NG account need to apply for a project, and need to undergo a review process.

Use the following Online Proposal Forms:

- GCS test project on SuperMUC-NG (100.000 CPUh for usage evaluation, waiting time ca. 1 week)
- GCS regular project on SuperMUC-NG (max 35 Mio CPUh)
- GCS large scale project on SuperMUC-NG (more than 35 Mio CPUh, 2 regular calls in spring and autumn)
- Extension of a GCS compute project on SuperMUC

Interested researchers from Europe are invited to apply via PRACE.

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

Login to SuperMUC-NG

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 Manage-your-project form.

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

Login with 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 Manage-your-project 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.
- It is recommended to 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.
Reporting problems with Login

To report a problem use the `ssh` command with the `"-vvv"` option and include the verbose information when submitting an incident ticket to the Servicedesk 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 the password is also necessary after it has been newly issued, or reset to a starting value by a project manager or by LRZ staff. This assures that actual authentication is done with a password known only to the account owner.

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 dropdown 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. For a detailed explanation please see: Operational Concept for SuperMUC-NG. There are no longer projects which map to unix groups, but all users are members of the hpcusers unix group. Each user will have only one user account on the systems, via this account all assigned resources can be accessed. A user can be member of several projects which map to compute time and storage resources. The following commands show the time and storage budget for the current user:

```
$ module load lrztools
$ budget_and_quota
```

In a SLURM job the user can use the flag

```
#SBATCH --account=<project-id>
```

in order to book the used computing time to a project account.

Particular attention was paid to data handling: The model enables a user to seamlessly access their data in different projects for which they are validated. In addition to that, a user can share their data (WORK only!) with other users within the same project, by giving the project group access to their user directory within the project. See (FAQ: Sharing files with other users)

To get this model up and running, all users will obtain a new single user account on SuperMUC-NG. With this new user account, the user will be able access their data in projects to which they are assigned to. All old user accounts will be phased out together with decommissioning of the SuperMUC system. The password for the new account is the one that the user has most recently changed before the target date of December 1st, 2018. The expiration date of the new password will be that of the old one.

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.

By default, version 2019 (update 3) of the Intel Parallel Studio is loaded at login or when starting batch jobs. This is the recommended release for large-scale parallel programs. For compatibility with the installed software stack it may be necessary to switch to an older release using the following command:

```
module switch devEnv/Intel/2019 devEnv/Intel/2018
```

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 [SVN, GIT and Mercurial SuperMUC-NG User Guide](#)