MiniClusterTools Documentation

Repo: https://github.com/coyleej/MiniClusterTools

Author: Eleanor Coyle
Contact: ecoyle@azimuth-corp.com

Operating system and shell

These scripts were developed to work with both the server and desktop versions of **Ubuntu 18.04** and the `bash` shell. If you are using a different operating system or a different version of Ubuntu, you will likely need to make modifications. My goal is to maintain POSIX compliance in all of the shell scripts, but I make no promises.

Documentation notes

This documentation automatically pulls relevant information from a larger, actively updated document. As a result, some internal references point to information that is not included. A few broken links seemed a reasonable compromise to ensure up-to-date documentation.

Contents

Chapter 1

Setup Scripts

1.1 sshd_setup.sh

This setup is automated in the `sshd_setup.sh` file from MiniClusterTools repository.

1. Install `fail2ban` and `openssh-server` with `apt`. `fail2ban` will ban IPs that exceed 5 failed tries in 10 minutes. (Never modify `/etc/fail2ban/jail.conf`! Copy it into `jail.local` and modify that.)
2. We're required to display a banner message (option A) on the servers prior to login. It will be activated in a few steps. For now, we're just creating it.
   (a) Create the login banner file:
   `sudo touch /etc/ssh/sshd_banner`
   (b) Add the warning found in the MiniClusterTools repo.
3. Open `/etc/ssh/sshd_config` and change some `ssh` settings.
   The convention in this file is to have default settings commented out and to only uncomment something if you change the value! Note: We are making an exception to this convention for values the higher ups have explicitly requested.
   (a) Specify that all `ssh` access to the servers must use protocol 2 by adding the following right below the line `#Port 22`. (Completely unnecessary for `openssh 7.6+`, but including anyway.)
   `Protocol 2`
   (b) Change `LoginGraceTime` to `1m`
   This changes the allowable time between typing `ssh <server>` and entering a password.
   (c) Change `PermitRootLogin` to `no`
   (d) Uncomment `StrictModes` to `yes` (default value)
   (e) Change `MaxAuthTries` to `3`
   This allows three password attempts after typing `ssh <server>` before resetting.
   (f) Restrict who is allowed to remotely access the server. Add these lines below `MaxSessions`:

   ```
   DenyUsers root
   DenyGroups root
   AllowGroups users slurm
   ```

   Only groups `users` and `slurm` are able to `ssh` or `sftp`. All (human) users and the vulnerability scanner user should be placed in group `users` when creating their accounts! See chapter **??** for managing group membership.
   Technically the `Deny...` statements are redundant. `root` is already forbidden from using `ssh` because its password is disabled and locked.

(g) Change `IgnoreUserKnownHosts` to `yes`

(h) Uncomment `PermitEmptyPasswords` to `no` (default value)

(i) Uncomment `X11Forwarding` to `yes` (default value)

(j) Have it print the last login for `$USER` (NOTE: While the convention would suggest that `yes` is the default, someone typo'd. The default is actually `no`.)

`PrintLastLog yes`

(k) Uncomment `PermitUserEnvironment` to `no` (default value)

(l) Uncomment `Compression` to `delayed` (default value)

(m) Change `ClientAliveInterval` to `600`

(n) Change `ClientAliveCountMax` to `1`

(o) Display the banner text in between typing `ssh <user>@<server>` and password entry

`Banner /etc/ssh/sshd_banner`

(p) `UsePrivilegeSeparation sandbox` *is depricated starting from* `openssh 7.5`*!* Privilege separation is now mandatory. Because it is depricated and results in a warning when checking the configuration, we are not adding this line to the config file.

4. Check that `sshd_config` is valid and error-free:

   ```
   sudo sshd -t
   ```

5. Reload the daemon:

   ```
   sudo systemctl restart sshd
   ```

6. The code will remind you to manually add users to the `ssh`-approved group:

   ```
   sudo usermod -a -G <ssh-users> <username>
   ```

7. Test by logging in again.

1.2 login_banner.sh

You must configure `gdm3` as described below. These changes are automated in the `login_banner.sh` file.

1. NVidia and Wayland will not get along if you modify the default `gdm` settings (read: you can't log in and the NVidia drivers get corrupted). Open `/etc/gdm3/custom.conf` and set:

   ```
   WaylandEnable=false
   ```

2. Create the following files and directories:

   ```
   sudo touch /etc/dconf/profile/gdm
   sudo mkdir /etc/dconf/db/gdm.d
   sudo touch /etc/dconf/db/gdm.d/01-banner-message
   ```

3. Open `/etc/dconf/profile/gdm` and add the following:

   ```
   user-db:user
   system-db:gdm
   file-db:/usr/share/gdm/greeter-dconf-defaults
   ```

4. Open `/etc/dconf/db/gdm.d/01-banner-message` and add the following:

   ```
   [org/gnome/login-screen]
   banner-message-enable=true
   banner-message-text='I have read & consent to terms in IS user agreement.'
   ```

5. Reconfigure `gdm3` and `dconf`.

   ```
   sudo dconf update
   sudo dpkg-reconfigure gdm3
   ```

6. Restart your computer for the changes to take effect.

1.3 unattended_upgrades.sh

Ubuntu by default will automatically download and install security updates but not security upgrades. We will use `unattended-upgrades` to automate the latter. It's preinstalled in 18.04 and can be configured in a single command.

Run `sudo dpkg-reconfigure unattended-upgrades` and follow the prompts. The whole process takes less than a minute. Detailed documentation can be found here.

If things ever go wrong, you may need to check the log files:
`/var/log/unattended-upgrades/unattended-upgrades.log`
`/var/log/apt`

By default `unattended-upgrades` runs randomly within a twelve hour block to smooth out demand on the mirrors. This is fine for our purposes and does not need modification.

1.4 set_password_policy.sh

1.4.1 Password policy

Passwords must be at least 15 characters long, with at least two upper case letters, two lower case letters, two numbers, and two special characters. They must expire after 60 days and contain at least two characters not in the previous password. Running `set_passwd_policy.sh` will automatically change these settings.

1. Change the password expiration settings. Open `/etc/login.defs` and set these variables:

   ```
   PASS_MAX_DAYS   60
   PASS_WARN_AGE   7
   ```

2. Set the password requirements. Open `/etc/security/pwquality.conf`. Negative values indicate that that number of the thing be present in a new password.

   ```
   difok = 2
   minlen = 15
   dcredit = -2
   ucredit = -2
   lcredit = -2
   ocredit = -2
   minclass = 4
   maxrepeat = 2
   usercheck = 1
   ```

3. Changes to `/etc/login.defs` only affect new users (source). You must also apply these changes to existing users: `sudo chage -M <days> <user>`

   The following code automates these changes (you can confirm changes with `sudo chage -l <user>`):

   ```
   userlist=$(grep "10[0-9][0-9]" /etc/passwd | cut -d ":" -f 1)
   for user in $userlist; do
       sudo chage -M 60 $user
       sudo chage -l $user | grep "Pass.*expire"
   done
   ```

1.4.2 HBSS

We must install HBSS and update the policies. The installation script is called in `set_passwd_policy.sh`. Contact me for the current installation script. If you wish to call it separately, do so with the following:

```
sudo bash <install>.sh -i && /opt/McAfee/cma/bin/cmdagent -c
```

Chapter 2

ML installation scripts

2.1 repo_download_w_some_install.sh

Downloads all of the necessary machine learning repos (pybind11, OpenBLAS, S4, MANTIS, and signac) and installs both MANTIS and Signac. Users must compile the other packages themselves.

2.1.1 MANTIS

Setup is automated in `repo_download_w_some_setup.sh` and consists of the following.

Note: MANTIS can (and will if you use the script) be installed prior to S4, but S4 is a required dependency. MANTIS will not work properly unless S4 is installed.

1. Clone MANTIS from github:

   ```
   cd /home/<admin>/Code
   git clone https://github.com/harperes/MANTIS.git
   ```

2. Make sure that the system `pip` is installed. If you skip this bit, then `sudo` won't find `pip3`...

   ```
   sudo apt install python3-pip
   ```

3. Install MANTIS to `/opt`

   ```
   cd MANTIS
   sudo pip3 install .  --target="/opt" --no-deps --no-dependencies
   ```

4. Open `/etc/environment`:

   Prepend `/opt/MANTIS` to the system path.

   Make sure that `/opt` has been added to PYTHONPATH.

5. Create or activate an s4py environment.

6. Test the install. Navigate to the MANTIS `tests` directory and type:

   ```
   python -m unittest
   ```

2.1.2 Signac

Setup is automated in `repo_download_w_some_setup.sh` and consists of the following.

1. Clone Signac from github and check out the develop branch:

   ```
   cd /home/<admin>/Code
   git clone https://bitbucket.org/glotzer/signac.git
   cd signac
   git checkout develop
   ```

2. Make sure that the system `pip` is installed. If you skip this bit, then `sudo` won't find `pip3`...

   ```
   sudo apt install python3-pip
   ```

3. Install MANTIS to `/opt`

   ```
   sudo pip3 install .  --target="/opt" --no-deps --no-dependencies
   ```

4. Open `/etc/environment`:

   Make sure that `/opt` has been added to PYTHONPATH.

2.1.3 S4

`repo_download_w_some_setup.sh` downloads the necessary machine learning repositories (pybind11, OpenBLAS, and S4), but compiling is left to the user.

Please refer to Eric Harper's S4 installation instructions. If you have access to the MANTIS folder, you can direct your browser to `file:///home/<User>/<PathToSyncFolder>/MANTISBIBLE/S4Documentation/html/install.html`. If not, please see the harperes S4 repository on github.

Chapter 3

Monitoring and maintenance scripts

3.1 Propagate changes to entire cluster

If you wish to make a change affecting the entire cluster, such as manually updating the whole cluster, installing the same package on all machines, or updating `slurm.conf`, the following framework allows you to do so. Working examples in the MiniClusterTools repository are `update_upgrade_cluster.sh` and `distribute_slurm_conf.sh` (section 6.3).

Note: `ssh` keys are recommended but not required.

```
sshkey='/dev/null'
admin='admin'
remote_IP=('server1' 'server2' 'server3')

# Propagate updated slurm.conf to the rest of the cluster
for IP in ${remote_IP[*]}
do
        rsync -au --fake-super -e "ssh -i $sshkey" "/etc/slurm-llnl/slurm.conf" \
                $admin@$IP:/home/$admin/
        ssh -i $sshkey -t $admin@$IP 'sudo cp slurm.conf /etc/slurm-llnl/slurm.conf; \
                sudo chown slurm: /etc/slurm-llnl/slurm.conf'
done
```

3.2 check_passwd_expiry.sh

Returns a warning if the user's password expires in 7 or fewer days.

3.3 downtime.py

Used for monitoring downtime. It is a modified version of script created by waleedahmad. The original version can be found on waleedahmad's github page.

3.4 Syncthing

3.4.1 Summarize syncthing usage

The `synthing_usage.sh` script in the MiniClusterTools repository reports the size of all directories in the syncthing folder. It generates a report on all directories. It does *not* message users; see section 3.4.2 if you wish to set up automatic messaging.

3.4.2 Automated messages about syncthing usage

If you wish to automatically message users, you'll need the `synthing-usage` script in the MiniClusterTools repository.

1. Copy `syncthing-warning` into `/usr/share` on the servers. Add eye-catching ASCII art if desired.
2. Open `/etc/bash.bashrc` and append the following.

```
if [ -f /usr/share/syncthing-warning ]; then
        . /usr/share/syncthing-warning
fi
```

Chapter 4

Files

Descriptions of all files in the `files` directory. Other sections cover the usage of each where relevant.

4.1 banner_text*.txt

The long and short versions of the banner text displayed when logging in. Which message is displayed depends on the login method. See sections 1.1 and 1.2 for details.

4.2 cgroup.conf

A `cgroup.conf` example file in case `install_slurm.sh` fails to properly make it's own.

4.3 s4py.yml

Used to create the `s4py` environment in conda. Contains all the packages required to install our ML tools (chapter 2).

4.4 test_sbatch.sh

Test if slurm is working properly by submitting a simple job with `sbatch`. Contains the `sleep` command to keep it in the queue longer.

Chapter 5

Slurm installation and setup

This setup works on Ubuntu 18.04 and Ubuntu Server 18.04.
The following will be installed in this setup guide:

- MPI: OpenMPI version 2
- Slurm 17.11.2-1 (slurmctld, slurmd, slurmdbd)
- Authentication and digital signatures: MUNGE
- Database: MariaDB

5.1 Reference materials

This guide was constructed from the following references and my own experiences:
Slurm admin quick-start
Slurm official documentation
`man slurm-wlm-doc` for Slurm 17.11.2-1build1
Slurm man pages and configuration file index
Slurm multi-core support
Slurm download and addons list
Slurm configuration (Niflheim)
Slurm database (Niflheim)
Slurm-gpu github

5.2 Note on hyperthreading

From the slurm documentation on hyperthreading:

> If your nodes are configured with hyperthreading, then a CPU is equivalent to a hyperthread. Otherwise a CPU is equivalent to a core. You can determine if your nodes have more than one thread per core using the command "scontrol show node" and looking at the values of "ThreadsPerCore".
>
> Note that even on systems with hyperthreading enabled, the resources will generally be allocated to jobs at the level of a core (see NOTE below). Two different jobs will not share a core except through the use of a partition OverSubscribe configuration parameter. For example, a job requesting resources for three tasks on a node with ThreadsPerCore=2 will be allocated two full cores. Note that Slurm commands contain a multitude of options to control resource allocation with respect to base boards, sockets, cores and threads.
>
> (NOTE: An exception to this would be if the system administrator configured SelectTypeParameters=CR_CPU and each node's CPU count without its socket/core/thread specification.

In that case, each thread would be independently scheduled as a CPU. This is not a typical configuration.)

If `SelectTypeParameters` is set to `CR_CPU` or `CP_CPU_Memory`, slurm will treat each thread as a CPU and completely disregard which core a thread is on. If it is set to `CR_Core` or `CR_Core_Memory`, slurm can assign multiple threads to a core but will not assign multiple jobs to the same core. If it is set to `CR_ONE_TASK_PER_CORE`, slurm assigns one task per core regardless of the number of threads available.

5.3 Basic Slurm set up

1. If you intend to set up a database on its own high speed drive, mount the drive now.
2. Make sure that OpenMPI is installed. If not, install it with

   ```
   sudo apt install libopenmpi2 libopenmpi-dev openmpi-common openmpi-doc
   ```

3. Download the MiniClusterTools repo if you haven't already. It contains a slurm installation script.

   ```
   git clone https://github.com/coyleej/MiniClusterTools.git
   ```

4. Run `install_slurm.sh`. It automates much of the setup. The following explains what it does.

   ```
   bash install_slurm.sh
   ```

   (a) Set five variables for the cluster name, controller information, and backup controller. If there is no backup controller, leave `backupname="NULL"`. The script will handle this automatically.

   (b) Create Munge user with `uid` and `gid` of 399. (Can be any *unused* value between SYS_UID_MIN and SYS_UID_MAX, which are defined in `/etc/login.defs`).

   ```
   mungeUID=399
   sudo groupadd -g $mungeUID munge
   sudo useradd -r -u $mungeUID -g $mungeUID munge
   sudo usermod -d /nonexistent munge
   ```

   (c) Make sure the system clock is set to the proper timezone and that your system clock is correct:

   ```
   sudo timedatectl set-timezone America/New_York
   timedatectl
   ```

   (d) Check that `nvidia-driver-430` or newer is installed so that slurm can find the GPUs.

   i. Check that we're using the Ubuntu `graphics-drivers` PPA. If we aren't:

   ```
   sudo add-apt-repository ppa:graphics-drivers/ppa
   sudo apt update
   ```

   ii. Use `apt` to purge anything older than `nvidia-driver-430`.

   iii. Use `apt` to install `nvidia-driver-430` if you purged an older driver.

   (e) Install OpenMPI if it is not presently installed:

   ```
   sudo apt install libopenmpi2 libopenmpi-dev openmpi-common openmpi-doc
   ```

   (f) Install MUNGE, SLURM, MySQL, MariaDB, and cgroup-tools:

   ```
   apt install munge libmunge-dev libpam-slurm slurmd slurmdbd slurm-wlm-doc
   cgroup-tools mariadb-common mariadb-server
   ```

   (g) If the node in question is the control node or the backup control node:

   ```
   sudo apt install slurmctld slurm-wlm slurmdbd
   ```

   Otherwise:

   ```
   sudo apt install slurm-client
   ```

   (h) User prompts will gather some information on GPUs.

   (i) Configure the control node, if applicable.

i. Make sure that `/var/spool/slurmctld/` and `/var/log/slurm-llnl/` exist. If not, create them with `mkdir`.

ii. Make sure that slurm is the owner of these directories. If not, use `chown slurm: <dirname>`.

iii. Make sure that the permissions on these directories are set to `755`. If not, use `chmod`.

iv. Check that `/var/log/slurm-llnl/slurmctld.log` exists and is owned by slurm. Otherwise, create it using `touch` and `chown`.

v. Create the Linux default accounting file.

```
sudo touch /var/log/slurm-llnl/slurm_jobacct.log
sudo chown slurm:  /var/log/slurm-llnl/slurm_jobacct.log
sudo touch /var/log/slurm-llnl/slurm_jobcomp.log
sudo chown slurm:  /var/log/slurm-llnl/slurm_jobcomp.log
```

(j) Configure the compute nodes. See this site for further details.

i. Create the `slurmd` spool directory with the correct ownership.

```
mkdir /var/spool/slurmd
chown slurm:  /var/spool/slurmd
chmod 755 /var/spool/slurmd
```

ii. Create the log files:

```
touch /var/log/slurmd.log
chown slurm:  /var/log/slurmd.log
```

iii. Create the pid files (only need `slurmctld.pid` on the control node):

```
touch /var/log/slurm-llnl/slurmd.pid /var/log/slurm-llnl/slurmctld.pid
chown slurm:  /var/log/slurm-llnl/slurmd.pid /var/log/slurm-llnl/slurmctld.pid
```

iv. View the physical configuration (sockets, cores, real memory, etc.) of each of the compute nodes with the command `slurmd -C`, and update this information in `slurm.conf`.

v. Set the `State` of the node as UNKNOWN (slurm assigns BUSY or IDLE) or FUTURE.

vi. It may be a good idea to assign weights to the compute nodes. All things being equal, jobs will be allocated the nodes with the lowest weight. The enables prioritization based upon hardware parameters such as GPUs, RAM, CPU clock speed, CPU core number, CPU generation. (more info)

vii. It may be a good idea in the future to uncomment `TmpFS=` in `slurm.conf`. (`/tmp` is the default; can change to e.g. `/scratch`.) You can add `TmpDisk=xxxxx` to each compute node line, where `xxxxx` is the size of the temporary file system.

(k) Create spool directories:

```
mkdir -p /var/spool/slurm/d
mkdir /var/spool/slurm/ctld
chown slurm:  /var/spool/slurm /var/spool/slurm/d /var/spool/slurm/ctld
```

(l) Create a `gres.conf` file.

Inside this file, add a line for each GPU available on that node as follows: `Name=gpu Type=<type> File=/dev/nvidia#`. (Confirm numbers with `ls -l /dev/nvidia*`.) See the documentation for more options.

(m) Copy `cgroup.conf.example` into `cgroup.conf` and make the following changes:

i. `ConstrainCores=no`

ii. `ConstrainRAMSpace=yes` (change from no)

iii. You may also want to include `MemSpecLimit` and `ContrainKmemSpace`. (reference material)

(n) Adjust the grub configuration. Open `/etc/default/grub`
Add `cgroup_enable=memory swapaccount=1` to `GRUB_CMDLINE_LINUX` line.
Run `update-grub`.

(o) Check the node configuration as detected by slurm by typing `slurmd -C` into the command line. Adjust the appropriate line of the COMPUTE NODES section of the `slurm.conf` file to match.

(p) Retrieve the configuration files:

i. Determine your version of slurm by typing `dpkg -l | grep slurm`. It should report version 17.11.2-1build1.

ii. Obtain the code directly from the command line with:
`wget https://github.com/SchedMD/slurm/archive/slurm-17-11-2-1.tar.gz`

iii. Extract the files. The example configuration files are in `<unzipped-slurm>/etc/`. Copy all example config files into `/etc/slurm-llnl/`

(q) Copy `slurm.conf.example` to `slurm.conf` and change the following. With `install_slurm.sh`, the backup controller information is not modified if `backupname = "NULL"` (the original setting).

i. `ClusterName=Marvel`

ii. `ControlMachine=<name>`

iii. `ControlAddr=<IP>`

iv. `BackupController=<name>`

v. `BackupAddr=<IP>`

vi. `ProctrackType=proctrack/cgroup`

vii. `TaskPlugin=task/cgroup`

viii. `InactiveLimit=600`

ix. `NodeName=thanos`

x. `Nodes=thanos`

xi. `PartitionName=CEM`

xii. Remove `Procs=1` and replace it with `CPUs=128`. (On a multi-core/hyperthreaded system, slurm uses the number of threads as the number of CPUs)

xiii. Add a RESOURCES section just above COMPUTE NODES with the following: `GresTypes=gpu`.

xiv. Also under the RESOURCES section, add `LaunchParameters=send_gids`. This has `slurmctld` look up the user name and group ids instead of the individual nodes and prevents the "couldn't chdir" error. This is the default setting in newer versions of slurm.

xv. In the COMPUTE NODES, add the following to each node containing one or more GPUs. # is the number of available GPUs on that node: `Gres=gpu:#`. Insert this just before `State=UNKNOWN`.

xvi. In the SCHEDULING section, set the default memory per node at 1000 MB. (Slurm's default is ALL, which will not allow multiple jobs simultaneously.)
DefMemPerNode=1000

xvii. Change the location of the slurm PID files to the following:
`SlurmctldPidFile=/var/run/slurm-llnl/slurmctld.pid`
`SlurmdPidFile=/var/run/slurm-llnl/slurmd.pid`

xviii. Modify `slurm.conf` so that the nodes can be rebooted while slurm is running. Change the reboot program to `RebootProgram="/sbin/reboot"`.

xix. Change when a DOWN node will be returned to service. The default (`0`) is that nodes will remain down until the admin manually changes the state. We will change this to `1`, meaning that the nodes will be restored to service if it is reponding, has a valid configuration, and was not manually set as DOWN.
`ReturnToService=1`

xx. Check that `StateSaveLocation=/var/spool/slurm/ctld`. This directory should already exist, but doublecheck to make sure.

xxi. Check that `FastSchedule=1` and `SchedulerType=sched/backfill` (default settings).

xxii. Set the consumable resources (1 and 2): `SelectType=select/cons_res`

xxiii. You must also select what is allowed as consumable resources. In `slurm.conf`, set `SelectTypeParameters=CR_Core_Memory`.
NOTE: If you use memory as a consumable resource, you *must* set the `RealMemory` parameter.

NOTE: If CPUs are a consumable resource, Slurm has no notion of sockets, cores, or threads. On single- and multi-core systems, CPU refers to cores. On a multi-core/hyperthread system CPU refers to threads.

xxiv. Because both CPUs and Memory are consumable resources, you *must* set `OverSubscribe=NO` to prevent jobs from conflicting with one another. Strange behavior will occur if `OverSubscribe=YES`, as jobs will conflict with one another.

xxv. Configure the partitions in `slurm.conf`, for example:
`PartitionName=xeon8 Nodes=a[070-080] Default=YES DefaultTime=50:00:00 MaxTime=168:00:00 State=UNKNOWN`
In the SCHEDULING section of the `slurm.conf` file, set `EnforcePartLimits=YES`. This will reject jobs that exceed a partition's size and/or time limits when they're submitted.
Things to keep in mind for the future (***not setting these up***):

- Partitions may overlap so that some nodes belong to several partitions.
- Access to partitions is configured in `slurm.conf` using AllowAccounts, AllowGroups, or AllowQos.
- If some partitions (e.g. big memory nodes) should have a higher priority, set this in `slurm.conf` using the multifactor plugin: `PartitionName ... PriorityJobFactor=10 PriorityWeightPartition=1000`

xxvi. By default, slurm propagates all user limits from the submitting node (see `ulimit -a` to the batch jobs. Configure `slurm.conf` so that the locked memory limit isn't propagated by uncommenting and setting as follows:
`PropagateResourceLimitsExcept=MEMLOCK`
(We haven't done the following, but if you have imposed any non-default limits on the login nodes in `/etc/security/limits.conf` or `/etc/security/limits.d/*.conf`, you probably want to prohibit these by setting: `PropagateResourceLimitsExcept=ALL`
See the slurm documentation for available options.)

xxvii. Do NOT modify `#PluginDir`! Doing so causes slurm to crash. Slurm defaults to:
`usr/lib/x86_64-linux-gnu/slurm-wlm`

(r) Start `slurmd` and, if applicable, `slurmctld`.

```
sudo systemctl start slurmd
sudo systemctl start slurmctld   # if applicable
```

You will get a warning or error if `slurmd -C` failed and the code autofilled the laptop values.

(s) Removes the extracted folder. The downloaded compressed folder is left untouched.

(t) End of installation script.

5. Check that the `NodeName` line matches the output of `slurmd -C`. If `slurmd -C` fails to execute properly, `install_slurm.sh` autofills with the values for an Oryx Pro.

6. Resolve any errors that popped up when running the installation script.

(a) If the daemon(s) failed to start, type `systemctl status <daemon>`. If slurm can't find nodes or a machine name, fix the `slurm.conf` and try again.

(b) If slurm complains that it doesn't have permissions to access a directory, you probably forgot `sudo` when starting slurm.

(c) If slurm isn't starting because it is missing directories, manually create those directories, set `slurm` as the owner, and try again.

(d) If slurm claims to be missing any configuration files (`*.conf`), see if it exists in `/etc/slurm-llnl` as `*.conf.example`. If it does, copy it, modify it, and try again. If it doesn't exist, refer to the source code on github for `your version of slurm` and copy it where it needs to go.

(e) If slurm can't find the GPUs, make sure that the system can see the GPUs and that you have an appropriate Nvidia driver.

(f) If it's still not working, start slurm manually (section **??**) to see more detailed error messages.

7. *At present the script only handles local setup.*

   (a) `slurm.conf` – Nodes and partitions on remote machines must be added manually. The rest of the file is the same, so all that will be required is copy/pasting the node and partition information. Add `NodeAddr=<IP>` just after `NodeName=<name>` to all of the compute nodes.

   (b) *Copy the proper munge key* into `/etc/munge`, then restart the `munge` and `slurmd` daemons.

8. If you installed slurm with `install_slurm.sh`, `cgroup.conf` will be the same on all nodes and all the `gres.conf` files will be setup appropriately. If you did not use the script, make sure that `cgroup.conf` is the same on all compute nodes and add `gres.conf` files as necessary.

9. Restart the node.

10. Check that munge is setup properly.

    (a) If munge is already running, stop it with `systemctl stop munge`.

    (b) Check that the following files/directories are owned by `munge` instead of `root`: `/etc/munge`, `/usr/bin/munge`, `/usr/sbin/munged`, `/var/lib/munge`, `/var/log/munge`, `/var/run/munge`

    (c) Create a munge key on the control node with `sudo /usr/sbin/create-munge-key`. (Ubuntu may have already done this for you.)

    (d) On the controller, make sure the munge key (`munge.key`) is in `/etc/munge/munge.key` and change the owner to munge.

    (e) Copy the key from the control node to all existing compute nodes:
    `sudo scp /etc/munge/munge.key admin@compute-node:/home/<admin>/`

    (f) On the compute nodes, move the `munge.key` into `/etc/munge`. Make sure that it is owned by `munge` with file permissions `400`.

    (g) Make sure that munge is enabled and (re)start it on all machines:
    `sudo systemctl start munge`

    (h) Check if munge is running by typing `systemctl status munge`.

    (i) Test munge:
    Generate a credential on stdout:
    `munge -n`
    Check if a credential can be locally decoded:
    `munge -n | unmunge`
    Check if a credential can be remotely decoded:
    `munge -n | ssh <admin>@<node> unmunge`
    Run a quick benchmark:
    `remunge`

11. Start slurm. Don't worry about enabling the daemons just yet; that will happen later.

    ```
    sudo systemctl start slurmctld   # Control node
    sudo systemctl start slurmd   # Compute nodes
    ```

12. Test that the job submission is working. The submission command is `sbatch <script-name>`. To check the status of the job, type `squeue`. Output will be written in the same folder as the script. Refer to section **??** for an explanation of the SBATCH directives.

    The following test script is also available in the MiniClusterTools repository as `files/test_sbatch.sh`:

```
#!/bin/bash
#SBATCH --job-name=example
#SBATCH --nodes=1
#SBATCH --ntasks-per-node=1
#SBATCH --cpus-per-task=1
#SBATCH --time=10:00
#SBATCH --mem=10
#SBATCH --partition=debug
#SBATCH --output=%x.o%j
echo "Hello World!"
sleep 120
```

Another script, complete with an explanation of the `SBATCH` directives, can be found in section **??**.

Note: Test scripts should contain the `sleep` *command to keep the job "running" for a longer time.*

13. Stop the slurm daemons:

    `systemd`: `sudo systemctl stop <daemon>`
    Manual start: `Ctrl-C`

14. We are using the default Prolog and Epilog scripts. Refer to the documentation if this changes.

15. Restart the node.

16. Start slurm and test the queue to confirm that it can run multiple jobs simultaneously.

17. Enable slurm.

    ```
    sudo systemctl enable slurmctld   # Control node(s)
    sudo systemctl enable slurmd   # Compute nodes
    ```

5.4 Configure the backup controller

If you have two controllers (primary and backup), both must have access to the slurm state save folder: `/var/spool/slurm/ctld`. Because of how our system is set up with NFS and to avoid a single point of failure, some `rsync` and `ssh` trickery is required to make both controllers share the state save information.

This particular setup is largely driven by permission-related considerations. Automated tasks cannot use `sudo`, as `sudo` is interactive. One way around this is to have `root` run the process, but `root` login is disabled on all machines for security reasons. The solution was to have `root` transfer between the slurm directory and the admin account, and the admin user transfer between servers. I tried getting the slurm user (the actual owner of the state folder) to transfer the data directly, but that didn't work.

5.4.1 Sharing StateSaveLocation

You need the `copy_state.sh` file from the MiniClusterTools repo to copy information locally between the slurm state folder and the admin folder. What it does:

1. Checks for the proper input parameters. There must be one or two options specified. The script is called as:

   `bash /path/to/copy_state.sh <direction> [sudo]`

2. Check that the value of `<direction>` is acceptable. The only accepted inputs for `<direction>` are `to_admin` and `to_root`, which transfer data to the admin account and to the proper slurm-owned state folder, respectively.

3. Controls whether the code runs with `sudo` privileges as required if the user calling the script is anyone other than `root`. Run with `sudo` privileges by assigning to a shell parameter a string of either `"sudo"` or `"with_sudo"`. Assigning *any* other value is equivalent to leaving this option empty.

4. Recursively copy (with `rsync`) and change file permissions/ownership as necessary, depending on the direction of transfer.

Now set up automatic Slurm state transfer.

1. Open `root`'s crontab on both machines with `sudo crontab -u root -e`.

   Add the following lines to copy to the other machine once an hour (for now, ultimately more frequently). (Slurm writes the state every 5 seconds.) Note: you must use the admin account for `rsync`. Running `rsync` from the root crontab with `sudo [-i] -u <admin> rsync` will be rejected by the remote servers.

   ```
   0    * * * * bash /home/<local-admin>/Code/MiniClusterTools/copy_state.sh to_admin
   15   * * * * bash /home/<local-admin>/Code/MiniClusterTools/copy_state.sh to_root
   ```

2. If `ssh` keys are already set up, skip to step 5. Otherwise, make ssh keys on each machine in the admin account. Modify the key name/location if desired, but *you must leave the passphrase empty.*

   ```
   ssh-keygen [-f ~/.ssh/<custom_name>]
   ```

3. Copy the keys to the admin account on the other controller, then test the key.

   ```
   ssh-copy-id <admin>@<remote>
   ssh -i ~/.ssh/<local_id_rsa> <admin>@<remote>
   ```

4. Test that `rsync` works over `ssh` in the admin account.

   ```
   rsync -a -e "ssh -i ~/.ssh/<local_id_rsa>" "<randomfile>" "<admin>@<remote>:~/"
   ```

5. Modify the admin crontab on each machine to copy to the remote machine once an hour.

   ```
   20 * * * *  rsync -au --fake-super -e "ssh -i ~/.ssh/<local_key>" \
          "/home/<local-admin>/slurm_state" "<admin>@<remoteIP>:/home/<admin>/"
   ```

6. There are a couple ways to confirm that it worked. Wait until after the cron job should have run, then do one of the following:

   - Check `/var/log/syslog`
   - Check the log mailed by `rsync`
   - Check the timestamps in the backup controller's slurm state folder

7. Each controller needs to copy the state files from the active controller *before* starting slurm. I've elected to have the local controller grab the files from the remote controller to ensure that it grabs the most recent state. (This may eventually get turned into a daemon that is required before `slurmctld` can start, but I'm going with the following for now.)

   NOTE: The following works beautifully on our cluster. When testing this code, either make sure the cluster is offline or test it on the backup controller! Otherwise you risk killing all jobs should a part of code not work properly.

   (a) Open the `~/.bashrc` file on the admin account on each controller.
   Append the following text:

   ```
   # Slurmctld start if daemon is not running
   if (! systemctl status slurmctld | grep "[Aa]ctive.*[Rr]unning" > /dev/null); then
       deltat=$(( $(date "+%s") - $(date "+%s" -r /var/spool/slurm/ctld/job_state) ))

       if (test $deltat -ge 30); then
           echo "Retrieving updated slurm state"
           rsync -au --fake-super -e "ssh -i ~/.ssh/id_rsa_<local>" \
                 "/home/<local>/slurm_state" "<remote>@<IP>:/home/<remote>/"
   ```

```
        echo "Copying files to proper directory"
        bash ~/Code/MiniClusterTools/copy_state.sh to_root with_sudo
    else
        echo "WARNING: Slurmctld not running for unknown reasons!"
    fi

    echo "Starting slurmctld..."
    sudo systemctl start slurmctld
fi
```

(b) Test this script on the backup controller. Stop `slurmctld`, then source `~/.bashrc`.

If you see `Starting slurmctld...` and no error messages, then the script works properly. Confirm that the daemon is running with `systemctl status slurmctld`.

(c) Disable `slurmctld`. Now the daemon will only start when the admin logs in for the first time, but the slurm state will always be up to date when the system resumes.

8. (Recommended) By default `cron` sends a message every time it does something, meaning that your inbox may get overrun if `cron` runs regularly. `cron` will not send mail if there is no output to send, so silencing a command's output is enough to stop getting that notification from `cron`.

   Some commands have a quiet option. For `rsync`, `-q` that suppresses non-error messages. If a command has a quiet option, this is the preferred way to suppress output.

   For commands *without* a quiet option, there are several ways to silence output. I recommend either redirecting `crond`'s mail output to the system log or using redirects (appending `>/dev/null 2>&1` to the offending line in your `crontab`) instead of completely disabling mail from `crond`. A more complete list of possibilities can be found here or here.

9. (Optional) Consider switching from `cron` to the `systemd` timers to run more frequently.

5.4.2 Set up backup controller takeover

You must set up the state transfer (section 5.4.1) before attempting this section.

You will need the `transfer_slurm_control.sh` file from the MiniClusterTools repo. What it does:

1. Uses `copy_state.sh` to transfer the state files to the admin account.
2. Copies files to the other controller using `rsync` and `ssh` keys.
3. Uses the remote machine's version of `copy_state.sh` to transfer the state files to the proper directory.
4. Issues the takeover command, `sudo scontrol takeover`.
5. Stops the local control daemon, `sudo systemctl stop slurmctld`.

Set up the state transfer and takeover command:

1. If `transfer_slurm_control.sh` isn't already an executable, make it executable:

   `sudo chmod +x transfer_slurm_state.sh`

2. (Optional) Open the admin's `.bash_aliases` (preferred) or `.bashrc` on both controllers and alias a command that transfers the slurm state immediately prior to issuing the takeover command, then source `.bashrc`.

   `alias state_takeover='/<path>/<to>/MiniClusterTools/transfer_slurm_state.sh'`

5.5 Slurm mailing setup

You can use the slurm mailing function to notify users regardless of whether you have a fully-qualified domain name (FQDN), though the setup will differ. Both methods are given below for the sake of completeness.

Both methods require you to install a mail user agent. I chose `bsd-mailx` for MARVEL. If you do not have a FQDN, choose, choose "local only" and use the local machine's hostname as the mail server host when installing. (Also described in section **??**, though with about the same level of detail as here.)

5.5.1 Without a FQDN

If you do not have a FQDN, as is the case with MARVEL, you ***cannot send actual emails*** to users. The following setup works is a workaround to notify users hourly of job status without requiring a FQDN.

1. Add the following to `slurm.conf`, just above the "Resources" section. Keep `MailDomain` commented out or omit it entirely.

   ```
   # MAILING
   MailProg=/usr/bin/mail
   #MailDomain=
   ```

2. Propagate the updated `slurm.conf` file to the entire cluster, and reconfigure the slurm daemons for the changes to take effect.

3. Find a way to propagate messages to the users. In our case, we use `grab_slurm_mail.sh` (in the Mini-ClusterTools repo) for this purpose. It is designed so that the user can delete either `Slurm_mail.log` or its contents without harming operation of the script.

   (a) Stores the location of the slurm mailing information, `/var/spool/mail/slurm`.

   (b) Creates a list of all human users.

   (c) Makes sure every human user's home directory contains a file call `Slurm_mail.log`, owned by that user.

   (d) Retrieve the time and date while pretending to be the timezone immediately to the west of you. This allows you to grab all mail activity in the previous hour. The date must be formatted such that it matches the line in the mail message.

   ```
   hour=$(TZ=CST6CDT date +"%a, %_d %b %Y %_H")
   ```

   (e) Use `grep`, `cut`, and `tr` to grab line numbers for all messages in the past hour. This will include messages from both Slurm and other sources.

   (f) If there are any matches within the past hour, set the line numbers matching the sending information, the recipient, and the subject relative to the line number you got with `grep`.

   (g) Use `sed` to retrieve the subject line of the message. If the subject line contains "SLURM", extract the source and the recipient. Append the source, intended recipient, subject line, and a blank line to the recipient's copy of `Slurm_mail.log`.

4. Copy `grab_slurm_mail.sh` onto both controllers.

5. On the controllers, open `root`'s `crontab` and set `grab_slurm_mail.sh` to run at the top of the hour.

   ```
   0 * * * * bash /path/to/grab_slurm_mail.sh >/dev/null 2>&1
   ```

6. Transferring information from the controller's `Slurm_mail.log` file to an Oryx Pro is the individual user's responsibility. Refer to section **??** for information on setting this up.

5.5.2 With a FQDN

Setup is easier if you have a FQDN, then you ***can*** send emails. The following setup works is a workaround to notify users of job completion without requiring a FQDN.

1. Add the following to `slurm.conf`, just above the "Resources" section.

   ```
   # MAILING
   MailProg=/usr/bin/mail
   MailDomain=<your.fqdn.here>
   ```

2. Propagate the updated `slurm.conf` file to the entire cluster, and reconfigure the slurm daemons for the changes to take effect.

3. The user must enter their email when submitting the script if they want to be notified. Refer users to section **??**.

5.6 Database setup

SchedMD recommends a separate database server if possible. It may be on the same server as `slurmctld`, but this may impact performance. You should consider optimizing the database performance by mounting the MariaDB or MySQL database directory on a dedicated high-speed file system. Ideally this would be a PCIe SSD disk drive (e.g. Intel SSD P3700 series or Kingston E1000 series), but SSD SAS/SATA will also work. Drives must be qualified for high-volume random small read/write operations, and should be built with the Non-Volatile Memory Express (NVMe) storage interface standard for reliability and performance. A disk size of 200 GB or 400 GB should be sufficient. Consider installing 2 disk drives in a RAID-1 configuration.

1. If you followed the basic slurm install instructions in section 5.3, you should have downloaded the MiniClusterTools git repo. If not, do it now.

   ```
   git clone https://github.com/coyleej/MiniClusterTools.git
   ```

2. Run `slurmdb_initial_setup.sh`. It automates much of the setup:

   ```
   bash slurmdb_initial_setup.sh
   ```

   Here's what the script does, with some explanation:

   (a) Create the log file:
   ```
   touch /var/log/slurmdbd.log
   chown slurm:  /var/log/slurmdbd.log
   ```

   (b) Create the pid file:
   ```
   touch /var/run/slurm-llnl/slurmdbd.pid
   chown slurm:  /var/run/slurm-llnl/slurmdbd.pid
   ```

   (c) In `slurm.conf`, make the following changes:

   i. Uncomment:
   ```
   JobAcctGatherType=jobacct_gather/linux
   JobAcctGatherFrequency=30
   AccountingStorageType=accounting_storage/slurmdbd
   ```

   ii. Modify:
   ```
   AccountingStorageHost=<IP or domain name>
   AccountingStorageLoc=/var/lib/mysql
   AccountingStoragePass=/var/run/munge/munge.socket.2    # munge daemon port
   AccountingStoragePort=3306
   AccountingStorageUser=slurm
   ```

iii. Add:
```
AccountingStoreJobComment=YES
AccountingStorageEnforce=associations
AccountingStorageTRES=gres/gpu,gres/gpu:gtx1080ti    # by default billing, CPU, energy, and node are tracked
```

(d) Restart `slurmctld`, as required by some of these changes:
`systemctl restart slurmctld`

(e) Copy `slurmdbd.conf.example` to `slurmdbd.conf`.

(f) Open `slurmdbd.conf`

i. Change the following lines to the following:
```
DbdAddr=<controlIP>
DbdHost=<controlName>
PidFile=/var/run/slurm-llnl/slurmdbd.pid
```

ii. Modify the following:
```
StorageHost=magneto
StoragePort=3306    # the mysql default port
StoragePass=<password>    # slurm's password in MariaDB StorageLoc=slurm_acct_db
```

iii. Add the following:
```
PurgeEventAfter=12months
PurgeJobAfter=12months
PurgeResvAfter=2months
PurgeStepAfter=2months
PurgeSuspendAfter=1month
PurgeTXNAfter=12months
PurgeUsageAfter=12months
```

(g) Re-read the config files: `scontrol reconfigure`

(h) We need to enable remote access to mariadb. Open `/etc/mysql/my.cnf` (it's symlinked to `/etc/mysql/mariadb.cnf`), and append the following to the end of the file:
```
[mysqld]
skip-networking=0
skip-bind-address
```

(i) Start MariaDB: `systemctl start mariadb`

3. Verify the setup with

```
scontrol show config | grep AccountingStorageHost
```

4. Troubleshoot the MariaDB daemon if it didn't start automatically in the script. Follow whatever error messages it gives, then restart the node and try again.

```
sudo systemctl start mariadb
```

If there have been multiple failed connection attempts, you may need to use the following to unblock the host IP:

```
sudo mysqladmin flush-hosts
```

5. Set up MariaDB:

(a) `sudo mysql_secure_installation`

(b) Set up the MariaDB root user password: Y

(c) Create root password: [redacted]

(d) Remove the anonymous user: Y

(e) Restrict root user access to the local machine: Y

(f) Remove the test database: Y

(g) Reload privilege tables: Y

6. Log in to the MariaDB server as the root user and add a slurm user. (MariaDB doesn't actually require the capitalization, but I'm including it to match their documentation.

   (a) Open the database: `sudo mysql`

   (b) Create the database:

   ```
   MariaDB [(none)]> CREATE DATABASE slurm_acct_db;
   ```

   Confirm with:

   ```
   MariaDB [(none)]> SHOW DATABASES;
   ```

   (c) Create a slurm user and grant database access (replace '<pass>' with the value in `slurmdbd.conf`):

   ```
   GRANT ALL ON slurm_acct_db.* TO 'slurm'@'%' IDENTIFIED BY '<pass>' with grant option;
   ```

   Confirm with:

   ```
   MariaDB [(none)]> SELECT user, host, plugin FROM mysql.user;
   MariaDB [(none)]> SHOW GRANTS for slurm@localhost;
   ```

   (d) Review the current setting for MySQL's `innodb_buffer_pool_size` before running the slurmdbd for the first time.

   ```
   MariaDB [(none)]> SHOW VARIABLES LIKE innodb_buffer_pool_size;
   ```

   (e) Consider setting this value large enough to handle the size of the database. This helps when converting large tables over to the new database schema and when purging old records. Setting `innodb_lock_wait_timeout` and `innodb_log_file_size` to larger values than the default is also recommended. Note: The default buffer size is 128M.

   These variables can be changed in one of the following files (not sure which one, but I suspect it's the first one):

   ```
   /etc/mysql/conf.d/mysql.cnf
   /etc/mysql/mariadb.cnf
   /etc/mysql/mariadb.conf.d/*.cnf
   ```

   ```
   [mysqld]
   innodb_buffer_pool_size=256M
   innodb_log_file_size=256M
   innodb_lock_wait_timeout=1800
   ```

   To implement this change you must shut down the database and move/remove the log files:

   ```
   sudo systemctl stop mariadb
   sudo rm /var/lib/mysql/ib_logfile?
   sudo systemctl start mariadb
   ```

   Verify the new buffer setting using the following command in the MariaDB shell:

   ```
   MariaDB [(none)]> SHOW VARIABLES LIKE innodb_buffer_pool_size;
   ```

   This has been left as the default for now (obviously).

   (f) Exit MariaDB:

   ```
   MariaDB [(none)]> QUIT;
   ```

7. Start `slurmdbd`, acting on any issues that may appear:

   ```
   sudo systemctl start slurmdbd
   ```

   One issue I encountered was fixed by manually changing the owner of the database directory, and reinstall mariadb:

```
sudo chown mysql:  /var/lib/mysql
sudo apt install --reinstall mariadb-common mariadb-client mariadb-server
```

Try setting up the database again.

If it's still grumpy, install `mysql-server-5.7` with `apt`, then try setting up the database again.

8. Enable `mariadb` and `slurmdbd`.

9. For job accounting to work, the database and accounting tools must be configured as explained in the official documentation. Use `sacctmgr` to create and manage these records.

   Accounting records are maintained based on "associations" consisting of four elements: cluster, account, user names and an optional partition name. All accounting things are lower case. *You must define clusters before you add accounts and you must add accounts before you add users.*

   (a) Add the cluster to the database:
   `sacctmgr add cluster <clustername>`

   (b) Add accounts:
   `sacctmgr add account <account> [Cluster=<clustername>] [parent=<parent>] \`
   `Description="<description>" Organization=<organization>`
   Omitting `Cluster` will add the account to all clusters. `parent` is only required if the new account is a sub-account of another account.

   (c) Add users:
   `sacctmgr add user <username> [Account=<accounts>] [DefaultAccount=<account>]`
   `Account` can take a single account or a comma separated list. Not specifying `Account` will give the user access to all accounts on the cluster. `DefaultAccount` will set the default account for a user. At least one of the two options is required.

   (d) Commands to view accounting information:
   ```
   sacctmgr list cluster
   sacctmgr list configuration
   sacctmgr list stats
   ```

10. If other nodes than the `slurmdbd` node must be able to connect to the `slurmdbd` service, you must open the firewall to specific hosts. Please see the Slurm_configuration page under the firewall section.

11. Make the following changes in `slurmdbd.conf`:

    May want to set `PrivateData`

12. Currently have no need to set up WCkeys. (Workload characterization keys are an orthogonal way to do accounting against possibly unrelated accounts. This can be useful where users from different accounts are all working on the same project.)

13. QOS includes multifactor job priority and job preemption. View with `sacctmgr`. By default everything is assigned normal. Can create something with higher priority.

14. Job completion logging is redundant if using the accounting infrastructure.

15. Don't set up PAM with the configuration we currently have! As long as users must submit from the node they want to run on, this is counterproductive!! For future use, see this guide.

16. Enable and start all daemons: `mariadb`, `slurmdbd`, `slurmctld`, `slurmd`

17. If you wish to customize `squeue` output, refer to section **??**

Chapter 6

Slurm Adminstration

6.1 Slurm admin commands

These are the most common admin-specific commands. Additionally, commands in section **??** can be run with `sudo` to affect *any* job. For details, refer to `man <command>`.

- Setup, rebooting, and shutdown commands

`scontrol takedown`	Orders switch to backup controller
`scontrol reboot [ASAP] [Nodelist]`	Reboots nodes, see documentation
`scontrol shutdown [slurmctld]`	Saves the current slurm state, then shuts down the daemons
`sacctmgr shutdown`	Shuts down the cluster
`slurmd -C`	Displays the physical configuration of a node when run on that specific node
`scontrol reconfigure`	Makes running daemons re-read configuration files

- Selected management and accounting commands

`sacct [options]`	Display accounting information for slurm jobs
`sacctmgr`	View and modify slurm account info
`sacctmgr add <entity> <specs>`	Add cluster, accounts, users; identical to `create`
`sacctmgr list <entity> [specs]`	Displays information about the specified entity
`sdiag`	Scheduling diagnostic tool
`smd`	Failure management suport tool
`sreport [options] [command]`	Generates reports of job usage and cluster utilization
`sstat`	Display various status information
`sview`	Graphical user interface to view and modify slurm

- Daemon commands: `slurmctld`, `slurmd`, and `slurmdbd` are the master/control, compute, and database daemons, respectively. They may need to be restarted if configuration files are modified (section 6.3).

`scontrol shutdown [slurmctld]`	Saves the current slurm state before stopping all slurm daemons (`slurmctld` option only shuts down the control daemons)
`systemctld enable <daemon>`	Enable to start on boot; does not start the daemon
`systemctld disable <daemon>`	Disable so that it will not start; does not stop the daemon
`systemctld start <daemon>`	Starts daemon manually, does not enable the daemon
`systemctld stop <daemon>`	Only use *if the cluster is fully idle* (you should default to `scontrol shutdown`): this stops daemon manually *without saving the current slurm state* and does not disable the daemon
`systemctld status <daemon>`	Reports status of daemon
`<daemon> -Dvvvv`	Manually starts the daemon; "D" runs in the foreground and "v" (can have 0 to 7 "v"s) indicates desired verbosity

6.2 Slurm node states

If the node is behaving properly, the node status should be `idle`, `mix`, or `alloc`, depending on the present usage. If this is not the case, see section **??**.

6.3 Adjusting configuration files

If you modify the configuration files (`slurm.conf`, `slurmdbd.conf`, `cgroup.conf`), the change must be distributed to all nodes before applying the changes. The `distribute_slurm_conf.sh` script in MiniClusterTools repository is one way to automate this process, as explained in section 3.1.

1. If you modify settings like Epilog, Prolog, SlurmctldLogFile, SlurmdLogFile, etc.), all you need to do is run `scontrol reconfigure` on the control node to force all slurm daemons to re-read the configuration files. The slurm controller (`slurmctld`) forwards the request to all other daemons (e.g. `slurmd`). Running jobs will continue execution.

2. Slurm daemons *must be restarted* if any of these parameters are changed: AccountingStorageEnforce, AuthType, BackupAddr, BackupController, ControlAddr, ControlMach, PluginDir, StateSaveLocation, SlurmctldPort, SlurmdPort.

3. Slurm daemons *must be restarted* if nodes are added to or removed from the cluster.

`ControlMachine` and `ControlAddr` are defunct in newer versions; use `SlurmctldHost` instead.

6.3.1 Adding/removing nodes

When adding/removing nodes, do the following:

1. Stop `slurmctld`

2. Add/remove nodes in `slurm.conf`

3. Restart `slurmd` on all nodes

4. Start `slurmctld`

It is also possible to add nodes to `slurm.conf` with `state=FUTURE`. The nodes will not be seen by slurm commands in this state. Make them available by changing their state in the `slurm.conf` file and update the node state using `scontrol` rather than restarting the `slurmctld` daemon.

6.4 Slurm plugins

Do not change the default Slurm plugin location in `slurm.conf`!
Default: `/usr/lib/x86_64-linux-gnu/slurm-wlm`

6.5 Reboot and shutdown nodes

6.5.1 Slurm downtime behavior

Be mindful of your configured SlurmdTimeout and SlurmctldTimeout values. If the Slurm daemons are down for longer than the specified timeout (currently 5 minutes), nodes will be marked DOWN and their jobs killed. Either increase the timeout values during an upgrade or ensure that the compute node slurmd are not down for longer than SlurmdTimeout.

6.5.2 Reboot

Nodes may need to be rebooted after firmware or kernel upgrades. Use the `RebootProgram` in `slurm.conf` to reboot nodes as they become idle. Be mindful of slurm downtime behavior (section 6.5.1).

Controller reboot

Because of how MARVEL is set up, you *must* complete the setup in section 5.4.2 first or you risk killing all jobs. (Note: On other systems the switch to the backup controller may be automatic and the following will not apply.) On MARVEL, the reboot procedure depends on which controller being rebooted:

- Primary controller:
  1. *Make sure that* `slurmctld` *is running on the* ***backup*** *controller!*
  2. Transfer the state to the proper location on the backup controller, then stop `slurmctld` on the primary controller. This process is automated in the `slurm_transfer_control.sh` script. (See section 5.4.2 for setup instructions and an explanation of the script.)

     If you are in the MiniClusterTools directory, you can call it with

     `./transfer_slurm_control.sh`

     From other locations, you will need to specify the path

     `/<path>/<to>/transfer_slurm_control.sh`

     or use your aliased command.
  3. Follow the compute node reboot procedure or the slurm shutdown procedure.
  4. The admin user must log into the primary controller to fetch the current slurm state from the backup controller and start `slurmctld`. (In our system, this is done with the admin user's `.bashrc` file.)
- Backup controller:
  1. *Make sure that* `slurmctld` *is running on the* ***primary*** *controller!*
  2. Follow the compute node reboot procedure or the slurm shutdown procedure.
  3. The admin user must log into the backup controller to start `slurmctld`. (`slurmctld` is disabled, and the start command is located in the admin user's `.bashrc` file.)

Compute node reboot

Issue the appropriate command for your version of Slurm (you'll need `sudo`):

```
scontrol reboot [ASAP] [NodeList]                                              # 17.11.2
scontrol reboot [ASAP] [nextstate=<RESUME|DOWN>] [reason=<reason>] [NodeList]  # newer
```

Explanation: `ASAP` prevents initiation of new jobs. Otherwise the system waits until it is idle to reboot and job scheduling is still allowed. The node state will be DRAIN (17.11.2) or REBOOT (newer) until rebooted or the reboot is cancelled.

If you are rebooting 17.11.2 or older, you may need to manually resume the node with `scontrol` post-reboot. Newer versions of slurm include `nextstate`, which specifies the state of the node after reboot, and `reason`, which shows users the reason the node is unavailable.

To cancel a reboot, use one of the following

```
scontrol update NodeName=<nodename> State=RESUME   # slurm 17.11.2
scontrol cancel_reboot <nodelist>                  # newer versions, e.g. 18.08
```

6.5.3 Shutdown

Be mindful of slurm downtime behavior (section 6.5.1).

If you want to shut down the primary or backup controller without killing simulations, see 6.5.2 to transfer control to the other machine before shutting anything down.

Shut down the slurm daemons with `scontrol shutdown [slurmctld]`. If the `slurmctld` option is used, only the control daemons will be shutdown. The benefit of `scontrol` over `systemctl` is that the former will save the current slurm state before shutting down the daemons.

Shut down the cluster with `sacctmgr shutdown`.

6.6 Backup and restore database

In order to backup the entire database to a different location (for disaster recovery or migration), the following files must be backed up. (source) Make a database mysqldump using this script /root/mysqlbackup (insert the correct root database password for PWD).

```
#!/bin/sh
# MySQL Backup Script for All Databases
HOST=localhost
BACKUPFILE=/root/mysql_dump
USER=root
PWD='**********'
DUMP_ARGS="--opt --flush-logs --quote-names"
DATABASES="--all-databases"
/usr/bin/mysqldump --host=$HOST --user=$USER --password=$PWD $DUMP_ARGS \
     --result-file=$BACKUPFILE $DATABASES
```

Write permission to $BACKUPFILE is required.

Make regular database dumps, for example by a crontab job: `30 7 * * * /root/mysqlbackup`

Restore of a database backup: The database contents must be loaded from the backup. To restore a MySQL database see for example How do I restore a MySQL .dump file?. As user root input the above created backup file:

```
mysql -u root -p < /root/mysql_dump
```

6.7 Upgrading slurm

Almost every new major release of Slurm (e.g. 16.05.x to 17.02.x) involves changes to the state files with new data structures, new options, etc. Slurm permits upgrades between any two versions whose major release numbers differ by two or less (e.g. 16.05.x or 17.02.x to 17.11.x) without loss of jobs or other state information. State information from older versions will not be recognized and will be discarded, resulting in loss of all running and pending jobs. State files are not recognized when downgrading and will be discarded. Create backup copies of state files before proceeding to later recover the jobs.

`slurmdbd` must be the same or higher major release as `slurmctld`. When changing the version to a higher release number (e.g. from 16.05.x to 17.02.x) *always* upgrade `slurmdbd` first. Database table changes may be required for the upgrade. If the database contains a large number of entries, `slurmdbd` may require an hour or two to update the database and will be unresponsive during this time.

`slurmctld` must be upgraded before or at the same time as `slurmd` on the compute nodes. It is recommended to update all daemons at the same time.

The `libslurm.so` version is increased every major release. Packages with slurm integration (e.g. MPI libraries) should be recompiled. Sometimes symlinking old `.so` name(s) to the new one(s) may work, but this is not guaranteed.

If you built your own version of Slurm plugins, they will likely need modification to support a new version of Slurm. It is common for plugins to add new functions and function arguments during major updates. See the RELEASE_NOTES file for details.

The recommended upgrade order is as follows:

1. Shutdown the slurmdbd daemon
2. Dump the Slurm database using `mysqldump` in case of possible failure
3. Increase `innodb_buffer_size` in `my.cnf` to 128M
4. Upgrade the slurmdbd daemon
5. Restart the slurmdbd daemon
6. Increase SlurmdTimeout and SlurmctldTimeout values and `scontrol reconfigure` to take effect
7. Shutdown the slurmctld daemon(s)
8. Shutdown the slurmd daemons on the compute nodes
9. Copy the contents of the configured StateSaveLocation directory in case of possible failure
10. Upgrade the slurmctld and slurmd daemons
11. Restart the slurmd daemons on the compute nodes
12. Restart the slurmctld daemon(s)
13. Validate proper operation
14. Restore original SlurmdTimeout and SlurmctldTimeout, and then `scontrol reconfigure`
15. Destroy backup copies of database and/or state files

Note: It is possible to update the slurmd daemons on a node-by-node basis after the slurmctld daemon(s) are upgraded, but make sure their down time is below the SlurmdTimeout value.