Access priviledges

Getting an account

For our SEECS collaborators, it's a 2 step process.

1. You have to be registered as a SLAC user. To do this go to https://oraweb4.slac.stanford.edu/apex/epnprod/f?p=134
   - The experiment is COMPUTING
   - You are NOT a SLAC employee, use your home institution as your employer.
   - Your work type is computing. SLAC will not be paying you. You will be using SLAC computing resources.
   - Your Activity Status is User (NOT Associate).
   - The experiment is Computing. Les Cottrell is your sponsor. Your SLAC group department is SCCS
   - You are probably at first not physically working at SLAC for any amount of time.
   - You are not a summer intern/rotation
   - Please be careful to use the recommended date format dd-mon-yyyy.
   - this will get you a SLAC ID. It may take a couple work days.
2. Once you have a SLAC ID then you will be able to apply for a SLAC computer account.For this you will need to go to http://www2.slac.stanford.edu/comp/slacwide/account/account.html Fill out these forms, sign them, and FAX to the attention of Les Cottrell at +1-650-926-3329, or scan and email to cottrell@slac.stanford.edu.
   - Unless you want to have emails in 2 boxes (SLAC and say SEECS or gmail), I would not request a SLAC email box unless you are at SLAC.
   - Just request a Unix and Windows account
   - Scan the form and email to cottrell@slac.stanford.edu. He will fill in the authorization section
3. Once you have an account you will need to know the userid and password. We will get these to you. You will need to change the password. This is done by ssh'ing to rhel6-64`.slac.stanford.edu` (a cluster of Linux interactive hosts) and issuing the `password` (not `passwd`) command. Please let us know when you have changed the password. The resetting of UNIX passwords will take up to 1 hour to take effect. The password must be >= 8 characters and include characters from three of the following sets: upper case, lower case, digits, and special characters. To ensure any email sent to your SLAC account goes to the right place, enter a `.forward` file (Google Unix .forward). We will be requesting the Unix group to enable you to logon to pinger but that will take some delay. You will probably need some privileges to access/write to various places. This will become more apparent as you get going. You may find Access priviledges of some use, however it is meant for iepm admins rather than iepm users.
4. Please refer to Use of SLAC Information Resource. More detailed policy and security information can be located here Under no circumstances should you attempt to log on to another user's account unless you have been given permission to use the account by your Group Leader or Account Czar. If you have questions then post to the maggie mailing list.
5. Kindly fill this form to get IEPM Wiki write access. The group name is "IEPM": https://jira.slac.stanford.edu/signup/

Hosts to Use

The following hosts are for general interactive use:

```
rhel6-64: is a cluster of interactive Linux hosts
```

See Network Test Hosts for special hosts used for network testing. This is also where pinger cron jobs are run from. For general cron jobs one uses suncron for Solaris and lnxcron for Linux.

Wiki Access

IEPM keeps a wiki based on confluence. It is accessible at https://confluence.slac.stanford.edu/display/IEPM/Home.

Most pages are world-readable, however, in order to edit pages you must subscribe for an account at https://jira.slac.stanford.edu/signup/. You should select the group `IEPM`. Once your request has been authorized, you will be sent your log in details for editing of the IEPM wiki pages.

Unix/NFS group iepm

File used to keep track of NFS network group privs. It use the ypgroup Unix databases

The groups below are Unix groups (not netgroup) which was made available over the network by NIS (formerly YP). Les can manage unix groups via the ypgroup command.

```
ypmatch <group_name> group
ypmatch <group_name> netgroup, e.g.
35cottrell@pinger:~>ypmatch u-network-management netgroup
(-,antony,)     (-,cal,)        (-,cottrell,)   (-,cxg,)        (-,jerrodw,)    (-,kmartell,)
```

or

```
ypgroup exam -group iepm
Group 'iepm':
GID:     2087
Comment:
Last modified at Aug  2 15:20:42 2006 by jonl
Owners:  cal
Members: akbar, cal, cottrell, cxg, fawad, hasan, iepm,
jerrodw, jiri, maheshkc, rich, ytl
```

To add someone to a group use (Les can execute this command):

```
ypgroup adduser -group iepm -user pinger
```

Please keep unix-admin & security notified when changes are needed, e.g. people changing function or moving etc.

#Note that people with privileges need to change their passwords at least every 9 months.

Netgroup

To see which hosts use a netgroup

Access to hosts is controlled by netgroup. ~~Only unix-admin can add users to a netgroup (e.g. u-iepm) or change what hosts that the netgroup can access.~~

grep the files at /afs/slac.stanford.edu/g/scs/systems/system.info/<machine>/taylor.opts.expanded looking for the group, e.g.

```
136cottrell@pinger:~$grep u-iepm /afs/slac/g/scs/systems/system.info/*i*/taylor.opts.expanded
/afs/slac/g/scs/systems/system.info/pinger/taylor.opts.expanded:limit_login=u-iepm
```

N.b. replacing *i* with * will probably result in /bin/grep: Argument list too long. Also note that as of 9/19/2013 the hosts whose access is controlled by u-iepm are: pinger

To see who is in a netgroup use the command*

```
netgroup <group_name>, e.g.
36cottrell@pinger:~>netgroup u-network-management
u-network-management
   (-,antony,)
   (-,cottrell,)
     (-,gcx,)
       (-,reuber,)
       (-,ytl,)


or
136cottrell@pinger:~$/usr/local/bin/netgroup_adm examine -group u-iepm
notes
# Users authorized to login to all the restricted-login machines
# involved in the IEPM project. Note that cottrell is in
# u-network-management, which is part of u-scs-staff.
hosts
 []
users
 ["arash", "iepm", "pinger", "ytl", "saqibali", "cottrell"]
owners
 ["kalim"]
netgroups
 []
exit
.
pid 19732 exit 0
```

The u-iepm group is the one to enable users to logon to the special iepm hosts (in particular pinger.slac.stanford.edu). It can be updated by u-scs-staff that includes u-bsd-admin, u-network-management, u-security-team, u-tech-coordinators, u-unix-role-accts, u-unix-staff. The command to add someone is netgroup_adm adduser -user cottrell -group u-iepm

NFS file access

NFS file systems such as /nfs/slac/g/net/pinger are exported to netgroup from netfs02, so it is available on all machines in that group. To see the full list of machines that can access these files, you can type:

```
119cottrell@pinger:~>netgroup slac > ! /tmp/junk
```

and edit the file (/tmp/junk). The amd mountpoints are transient....they timeout when not in use. So sometimes it will work to cd to /nfs/slac/g and you will see an entry for net/pinger, but if it has timed out you may not, even on pinger (unless something runs there that keeps it constantly available). Once the mountpoint has timed out you will have to cd to the full amd mount path which in this case is /nfs/slac/g/net/pinger to get amd to remount the space. AS a rule it is always a good idea to use the full path to the nfs space, especially in scripts.

Unix/AFS groups

Group Name	Purpose	afs path	contact(s)
g-scs	SVN access	/afs/slac/g/scs/net/netmon/repo/svn	Cottrell
g-www:admin-www-iepm	www-iepm/pinger web site	/afs/slac/g/www/www-iepm	Cottrell
iepm:iepm	Code	/afs/slac/g/scs/net/iepm-bw[/bin]	Cottrell

To see the names of groups and privileges on a particular directory, issue the command

```
fs la <directory>, e.g.
fs la .
```

or

```
fs la /afs/slac/g/scs/net/pinger

jerrodw@pinger $ fs la /afs/slac/g/scs/net/pinger/
Access list for /afs/slac/g/scs/net/pinger/ is
Normal rights:
  maint-pkg-netmon rlidwk
  g-scs rlidwka
  system:slac rl
  system:administrators rlidwka
  system:authuser rl
```

To view members of a particular group listed from 'fs la', issue the command:

```
pts mem <group_name>, e.g.

jerrodw@pinger $ pts mem maint-pkg-netmon
Members of maint-pkg-netmon (id: \-4786) are:
  <list of user_id's belonging to this group>
```

To add users to a particular group (only if you have privileges of course), issue the command

```
pts adduser \-group <group_name> \-user <user_id>
```

Escrow

Escrow is the shared password safe used to keep common credentials in a secure way. The main use is to enable you to find out the password to the pinger account. This is needed for setting up cron jobs under the pinger account.

To add a new user to the escrow "clique" or group for IEPM:

1. The new user should create a new key for him/herself with the PGP key generation command: How to Get PGP Key

   ```
   pgp -kg
   ```

   When prompted, use a key strength of 1024 bits and use the suggested key name format `Firstname Lastname <username@slac.stanford.edu>`.
2. The new user should export his/her PGP key for use with escrow:

   ```
   escrow setupuser
   ```

   This will export the user's public PGP key into a separate file which can then be imported into escrow.
3. An existing escrow user should add the user's key to the clique's keyring:

   ```
   escrow adduser -c iepm ~*<newuser>*/.escrow/publickey
   ```

   e.g. `escrow adduser -c iepm ~jaredg/.escrow/publickey` The program will repeatedly prompt for confirmation that the key is trusted. It will also prompt you for the existing user's PGP passphrase.
4. Note 4 MUST come after 3. An existing escrow user should add the user's key to the iepmacct list of secrets:

   ```
   escrow adduser -c iepm iepmacct *<username>*
   ```

   e.g. `escrow adduser -c iepm iepmacct jaredg` The program will prompt for the existing user's PGP passphrase.
5. Add user to the AFS group cottrell:iepm

   ```
   pts adduser -user kalim -group cottrell:iepm
   ```

To add a new user to "netdev" (Networking escrow clique):

Follow steps 1 and 2 above.

Step 3:

```
escrow adduser -c netdev ~*<newuser>*/.escrow/publickey
```

Step 4:

```
escrow adduser -c netdev <escrow file name> *<username>*
```

VPN access

See How to Connect to SLAC VPN

Note you will need to request VPN Usage access.

Network Test hosts

Please note that we would like to see network testing, especially WAN testing, done primarily and by convention from machines set aside for that purpose (e.g. iepm-bw, iepm-resp, pinger), the list of network machines is kept at http://www-iepm.slac.stanford.edu/about/nodes.html

To find out who can logon to a specified host look at the /etc/passwd file on that host, look towards the end for things like
+@u-iepm
and use the netgroup u-iepm command to see who is in the group.
To find out what hosts u-iepm can logon to use:

```
#65cottrell@pinger:/afs/slac/g/scs/systems/system.info>grep u-iepm \*/passwd
#pinger/passwd:+@u-iepm
#iepm-bw/passwd:+@u-iepm
#iepm-resp/passwd:+@u-iepm
#nettest5/passwd:+@u-iepm
#iepm-raptor1/passwd:+@u-iepm
#iepm-raptor2/passwd:+@u-iepm
#...
```

To logon to account iepm

Account iepm (typically on iepm-bw.slac.stanford.edu) is used to work on the iepm-bw project. Password logon to this account is to first order blocked. To access this account one has to have one's ssh public keys installed in ~iepm/.ssh/.public/authorized_keys. The first thing for the new person wishing to run unnder the account iepm is to create her/his ssh key pairs. To create the ssh key pairs use the commands:

```
ssh-keygen -t dsassh-keygen -t rsassh-keygen -t rsa1
```

It will also ask you for a pass phrase, just enter a carriage return. If it asks where to save the keys just take the default (carriage return). Another used can verify that the public keys are created as follows:

```
3cottrell@pinger:~>more ~tanzeel/.ssh/.public/identity.pub
    1024 35 146653454394770889044623166877077310614501899921965775234647207308036879
    637504138520090805397371267524126010888568377079972314298180262346201379642851 89
    909161392172472524655546358680808635955984996774105333214917621630270070694918 91
    434058737855187038839682593448694292089719275997227366904221127090067358673 57 ta
    nzeel@iepm-bw
```

Someone who can already logon to account iepm will then need to copy the new person's (in the example above tanzeel) public keys into ~iepm/.ssh/.public/authorized_keys:

```
2iepm@iepm-bw:~>cat ~tanzeel/.ssh/identity.pub >> ~/.ssh/authorized_keys
3iepm@iepm-bw:~>cat ~tanzeel/.ssh/id_dsa.pub >> ~/.ssh/authorized_keys
4iepm@iepm-bw:~>cat ~tanzeel/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
5iepm@iepm-bw:~>cat ~tanzeel/.ssh/id_dsa.pub >> ~/.ssh/authorized_keys2
```

One can then check that the new person's public ssh keys are available in the iepm account as follows:

```
9iepm@iepm-bw:~>tail -3 ~/.ssh/authorized_keys
    1024 35 146653454394770889044623166877077310614501899921965775234647207308036879637504138520
    090805397371267524126010888568377079972314298180262346201379642851899091613921724725246555 46
    358680808635955984996774105333214917621630270070694918914340587378551870388396825934486942 92
    089719275997227366904221127090067358673 57 tanzeel@iepm-bw
    ssh-dss AAAAB3NzaC1kc3MAAACBAIEC24o7qaGXu7BhvDEyVLfbtNCyHDqsW5N7urvW2DLKam7MMyZmnAqpQh1X7j8L
    U+DAy6eX50ToychvrwDA8pmA45Hbf61dnoSc/yfd1sM8fC1x0faWvglf/PNT5EfQzwPKEEzIeTieNRL9OTNr4ZS7WjXJ
    +i+bvc/a6bq+6Rj1AAAAFQCWTL/9FG3xCJ3nKwRg/g5cduZ9BwAAAIA8N63JWBa+xr2I4ylDaaONQNfVP9ODNMvtSBSj
    OlEK7YD4oDd/ZZPLEdW+mcHGTbEgwBB15acl+4PdpGBy5HCGsA7xXJPEPGnjNHRcsfRCdAuyQiaUKfJLfPPvdAAlKxO+
    DGJCItlsE8hyf+vbDJGxoa4nOqm2aQ6XneXhWhJuwAAAAIAXJMhOKrGAYBn72q+IbwM2c33bXLDnTTlGo7WKlzeBpLas
    jnt79E10TZEX6h0WDYuK0Ymdjy8XEoaStpF/bH+TxXclLNCAhjeWVf/FJI1neDhvhfrLHV3rOVEgH+d9Wka7Q+e2RPYY
    8WJOx/eh7vW21LwqmnfLK/h0lyxJ3/EX9w== tanzeel@iepm-bw
    ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA4uzuhQTykqyFHpEayNxTz0HC951ynsxxT2ltHXzjdTbudozvtXEnCYGe
    hXVoog4wS2yhwXskRZj8mKyoa/ZtPOd2fXZgQs+zJB5SrDN7jf2aWt5A1a2VynVAFPor4Vu/Yh79dAkj3zN3ojcoelqt
    wFheKhmPRh1cxNIpNyPmelE= tanzeel@iepm-bw
```

and the new user should be able to logon to the iepm account using:

```
~tanzeel@iepm-bw.slac.stanford.edu>ssh -v iepm@iepm-bw.slac.stanford.edu if that does not work then try:
    ~tanzeel@iepm-bw.slac.stanford.edu>ssh -v -1 iepm@iepm-bw.slac.stanford.edu
and
    ~tanzeel@iepm-bw.slac.stanford.edu>ssh -v -2 iepm@iepm-bw.slac.stanford.edu
```

Sudo Access

The sudoers file can be found at:

```
/afs/slac/package/taylor/prod/base/sudoers
```

The following lines are in the sudoers file:

```
# NB: The following two aliases define collections of commands for use
# by members of the IEPM group on all machines and on the network
# trouble-shooting machine, pharlap, respectively.  In this context,
# "IEPM group" is not necessarily the same as the NIS group named
# "iepm"; changes to the commands in the two aliases, or to the users
# who should be authorized to use the commands, still need the usual
# approvals.

# Commands authorized for members of the IEPM group on all machines:
Cmnd_Alias IEPM_ALL     = NIKHEF_PING,PATHCHAR,PCHAR,PIPECHAR

# Commands authorized for members of the IEPM group on pharlap:
# The addition of PIPECHAR to this list of commands is granted for
# six months only and should be revisted May 28, 2002.
Cmnd_Alias IEPM_PHARLAP = SNOOP,TCPDUMP,NDD,PIPECHAR,KILL
#the following enables net-eng people to execute the command on
#all non-retricted, taylored systems.
Cmnd_Alias NET_ENG      = NDD_GET,TCPDUMP,ETHTOOL
```

The people in the sudoers file with privileges assigned by these two Cmnd_Alias-es are: `cal, cottrell, cxg`.

```
iepm group: cottrell, warrenm, cal, dougc, cxg, grosso
Pathchar        All        sudo /afs/slac/g/scs/bin/pathchar
Pchar                All        sudo /afs/slac/package/netperf/bin/@sys/pchar
Pipechar        All        sudo /afs/slac.stanford.edu/package/netperf/bin/@sys/pipechar
NIKHEF ping        All        sudo /afs/slac/package/nikhef/@sys/ping
#Snoop and tcpdump are big security exposures, so please be careful with their use.
#Probably a good idea to notify security (email just before you start) if you are
#going to use snoop and/or tcpdump
Snoop           Pharlap        sudo snoop
Tcpdump               Pharlap        sudo /afs/slac/package/netperf/bin/@sys/tcpdump

u-network-management: warrenm, cottrell, kmartell, cal, cxg, grosso, janewei, gtb
ssh               All

maint-pkg-nikhef: cxg, warrenm, dougc
```

The following have /usr/sbin/ndd -set privs and sudo kill (via cmd macro IEPM_PHARLAP) on pharlap (7/19/01):

cal, cottrell, cxg

Account iepm has sudo kill with no password on pharlap (12/14/01)

cottrell also has ndd -set for evagore (11/21/01)

iepm has pipechar with no password on pharlap and antonia (11/28/01)

Mailing lists

The main mailing list is iepm-group. To get added to this list contact Les Cottrell. To see who is in the group etc. go to majordomo

The following mailing lists exists that may of interest to IEPM users:

Mailing List	Description
iepm-group	group messages
iepmbw-dev	iepmbw development mailing list
iepmbw-alerts	alerts from iepmbw monitoring systems
iepm-diag	diagnostics from monitoring systems
pinger-dev	development mailing list for pinger based activity

The pinger account has a .forward file to which trscrontab errors are sent.