SSH

Table of Contents:

Projects:

- SSH Inbound Connections Reduction
  * SLAC IT Cyber Security Owns this project, for more information please see the link. (SLAC Active Directory Login is required)

Login Nodes

To SSH to your on-site desktop, we recommend you use jump.slac.stanford.edu for network access and then SSH onto your computer on-site.

For SLAC IT Storage Platform access, group creation and information please see the link.

Load-balanced Hostname	Pool Name	Operating System	Authentication	Non-Scientific File System
jump.slac.stanford.edu	jump	Rocky 9.x	Active Directory	Coming soon
rocky9.slac.stanford.edu	rocky9	Rocky 9.x	Active Directory	SLAC IT Storage Platform
ubuntu-lts.slac.stanford.edu	ubuntu-lts	Ubuntu LTS 22.04	Active Directory	Coming soon

X11 GUI Bastion Host

Load-balanced Hostname	Pool Name	Operating System	Authentication	Non-Scientific File System	Guides
nx4.slac.stanford.edu	nx4	RHEL 9.x	Active Directory	Coming soon	Modern NoMachine
fastx.slac.stanford.edu	fastx	RHEL 9.x	Active Directory	Coming soon	Modern FastX

The following scientific bastion host can be used for remote SSH access to SLAC:

Load-balanced Hostname	Pool Name	Operating System	Authentication	Scientific File System	Guides
s3dflogin.slac.stanford.edu	s3dflogin	RHEL 9.x	Heimdal "Unix"	WEKA	S3DF
s3dfnx.slac.stanford.edu	s3dfnx	RHEL 9.x	Heimdal "Unix"	WEKA	S3DF NoMachine

Restricted / Limited Login

The following systems require VPN access to use:

Load-balanced Hostname	Pool Name	Authentication	Scientific File System	Guides
rhel6-64.slac.stanford.edu	rhel6-64	Heimdal "Unix"	AFS & NFS	NA
cdlogin.slac.stanford.edu	cdlogin	Heimdal "Unix"	AFS & NFS	NA
centos7.slac.stanford.edu	centos7	Heimdal "Unix"	AFS & NFS	NA
nx.slac.stanford.edu	nx	Heimdal "Unix"	AFS & NFS	Legacy NoMachine
fastx3.slac.stanford.edu	fastx3	Heimdal "Unix"	AFS & NFS	Legacy FastX

Example usage:

```
ssh jump.slac.stanford.edu
```

You can add your username to the login command like this:

```
ssh rocky9.slac.stanford.edu -l username
```

(replace "username" with your actual SLAC username.

X11 GUI access

SSH is capable of forwarding X11 through the connection. This will be slow when you are connecting from a non-SLAC network. To display SLAC X11 / GUI applications to your remote desktop or laptop.
SLAC IT recommends NoMachine over FastX.

SLAC has NoMachine and FastX available. For more information on the programs, see:
For NoMachine, see NoMachine
For FastX, see FastX

Data Transfer Nodes (DTN)

SDF and S3DF can help with transferring data. For more information, see:
SDF https://sdf.slac.stanford.edu/public/doc/#/data-transfer
S3DF https://s3df.slac.stanford.edu/public/doc/#/data-transfer

SSH between a non-SLAC machine and a SLAC machine

You can ssh from offsite to rhel6-64, iris, or centos7. You will be prompted for your SLAC password. This method works fine.

If you want to use "passwordless" authentication, using ssh host keys will not be very useful since that will not provide you with an AFS token. If you have an AFS home directory on your SLAC linux computer, you will get logged in, but you will not have write access since you do not get an AFS token. Instead of ssh host keys, you can use Kerberos (GSSAPI) Authentication by doing the following:

1. Turn on GSSAPI options in your ~/.ssh/config file.

   ```
   # Specifies whether user authentication based on GSSAPI is allowed.
   GSSAPIAuthentication yes

   # Forward (delegate) credentials to the server.
   GSSAPIDelegateCredentials yes
   ```

2. On your non-SLAC machine:

   ```
   kinit --renew userid@SLAC.STANFORD.EDU || kinit --renewable userid@SLAC.STANFORD.EDU
   ```

   OR

   ```
   kinit -R userid@SLAC.STANFORD.EDU || kinit -r 7d userid@SLAC.STANFORD.EDU
   ```

   replace 'userid' with your SLAC username, and replace 'machine' with a slac machine (eg, centos7.slac.stanford.edu). Note: the version of 'kinit' on your machine may have different options, please see your local documentation (eg, 'man kinit' or 'kinit --help'

3. Then each time before you ssh (or at least once per day), renew your Kerberos ticket with this command (if the renew fails, then you will be prompted to enter your password to get a new Kerberos ticket). As long as your ticket remains renewable and hasn't expired, you can renew it for a longer period without having to enter your password again.

   ```
   kinit --renew userid@SLAC.STANFORD.EDU || kinit --renewable userid@SLAC.STANFORD.EDU
   ```

   OR

   ```
   kinit -R userid@SLAC.STANFORD.EDU || kinit -r 7d userid@SLAC.STANFORD.EDU
   ```

   Note: the version of 'kinit' on your machine may have different options, please see your local documentation (eg, 'man kinit' or 'kinit --help'

4. You can run the 'klist' command on your remote machine to view your Kerberos ticket:

   ```
   klist
   ```

   'klist -v' will show more details.

5. Now you can ssh to slac using Kerberos GSSAPI Authentication:

   ```
   ssh userid@machine.slac.stanford.edu
   ```

6. After you ssh to SLAC, you can run the 'tokens' command to verify you have an AFS token:

   ```
   tokens
   ```

7. After you ssh to SLAC, you can renew your afs token with this command

   ```
   kinit && aklog
   ```

If your ssh attempt to SLAC just hangs for a long time, or you are prompted for your password, that probably means your Kerberos ticket has expired. You can run 'klist' to verify that. You can run 'kdestroy' and then your ssh attempt won't hang (but you will be prompted to authenticate using a password).