Getting Started

Table of Contents

- Initial Steps
- Using LINUX
- SSH Access to login.seas
  - Access through the FAS VPN (using password authentication)
  - Access from anywhere in the world (using SSH public keys)
  - Trade-offs of each method
- Network Storage

Initial Steps

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://apply.seas.harvard.edu">http://apply.seas.harvard.edu</a></td>
<td>to request a SEAS account. Please include your course number if appropriate.</td>
</tr>
<tr>
<td><a href="https://password.seas.harvard.edu">https://password.seas.harvard.edu</a></td>
<td>to change your SEAS password. Email <a href="mailto:help@seas.harvard.edu">help@seas.harvard.edu</a> if you have forgotten your password and need it reset.</td>
</tr>
<tr>
<td><a href="https://vpn.harvard.edu">https://vpn.harvard.edu</a></td>
<td>password-based authentication to SEAS is only possible when you are on the VPN. Use your Harvard key and 2-step auth to connect to the VPN.</td>
</tr>
<tr>
<td>ssh://login.seas.harvard.edu</td>
<td>you must be on the VPN for username/password authentication, otherwise you must have ssh key based authentication setup. See details below if you don’t have ssh keys or if you haven’t used ssh before.</td>
</tr>
</tbody>
</table>
| scp ~/.ssh/id_rsa.pub
login.seas.harvard.edu:/ssh/authorized   | Copy your ssh public key to your .ssh directory on login.seas. This must be done over the VPN. Make sure the contents of your public key are in the .ssh/authorized_keys file. |
| http://code.seas.harvard.edu             | Git-based code repository (public and private). |

Little remains from what was a local HPC infrastructure, only the login system is still up, so most of this part of the wiki is gone reflecting such change.

Using LINUX

LINUX has quickly become the predominant OS used in HPC systems, and all clusters are LINUX based. Thus a very basic knowledge of LINUX is a prerequisite for any kind of computing.

Take a look at the following links for pointers:

- Introduction to LINUX
- LINUX command line tutorial
- LINUX Command reference
- Secure Shell (SSH) Tutorial
- "The Ultimate Linux Guide"

SSH Access to login.seas

In order to allow network access to systems, but to assure that this access does not entice hackers, we use SSH key based access to some local systems.

Password-based access is still available on the SEAS login server when connecting from the SEAS VPN

The SEAS login server is based on LINUX and provides interactive and secure file transfer capabilities for the SEAS community to home and group directories. The host is available as:

- login.seas.harvard.edu

Access is available in two ways:

1. Password authentication when connected from the FAS VPN.
2. By using SSH public keys

Access through the FAS VPN (using password authentication)

The only way to access the SEAS login server using password authentication is by connecting through the FAS VPN first; this provides two-factor authentication before using your SEAS password to login.

To begin, connect to the FAS VPN at

- http://vpn.harvard.edu

Enter your Harvard Key and duo token to login. You will need to install a small client on your machine, and to enter an administrator password in order to complete the initial setup.

For more details, see the page

- Using SEAS VPN.

Once connected to the VPN, you are ready to establish your password session to login.seas.harvard.edu from your SSH or SFTP client as usual.

Access from anywhere in the world (using SSH public keys)

To access using public keys, you will need to create an SSH public and private key pair for each client computer (i.e. laptop or desktop), and then add the public key to a file:

- /home/[username]/.ssh/authorized_keys

in your home directory.

For more details, see the page

- SSH Access to SEAS Hosts

Trade-offs of each method

In general, the VPN + password approach allows a user immediate access to their data, but requires the installation of the Cisco VPN client, and can be slower than direct access. In addition, a user needs a Harvard Key and 2 step auth token in order to use it, and must be a member of FAS.

The SSH-key based approach provides direct access to the login server from the internet, and doesn't incur the overhead of the VPN. However, installation and setup may be confusing to users not familiar with SSH keys, and may require intervention of SEAS computing staff in order to get setup.

In general, we consider VPN + password to be the initial way to connect for most users, but that most users should then setup SSH keys for continued access.

Network Storage

SEAS provides network storage to its members, that storage can come in different forms:

- Google Drive : provisioned with your g.harvard.edu email account
- One Drive : provisioned with your O365 email account
- Local network storage : located on the vfilers
- Storage for computing purposes : Hosted at FAS RC premises, for more information see the page : Connecting to your SEAS storage hosted in FAS RC