ssh Authentication Forwarding (xbio)

Access xbio and cluster nodes

Explanation

ssh uses paired private and public keys for access control. You keep your private key, called id_rsa by default, and never share it. You distribute your public key, typically id_rsa.pub, to people such as HPC admins who need to give you access to ssh servers. Because your private key functions like a password, it should always be encrypted, and never put into an unsafe environment, such as an email attachment or a shared server. Specifically your private key should not be on xbio.mskcc.org, which is under constant attack from the Internet.

The obvious problem this raises is: How can you authenticate from your Mac at home to lilac or jun, when your Mac can’t talk directly to lilac or jun through the MSKCC firewalls? The answer is ssh authentication forwarding.

These instructions are for Macs. OpenSSH works the same on Linux and Windows, but they don’t have the Apple Keychain, which stores decryption passwords for private keys. PuTTY on Windows includes the Pageant ssh agent instead. The HPC admins don’t support Windows or Linux clients. If you’re not using a Mac you’ll probably need to start ssh-agent manually and load your private key, probably once per login session. The Mac handles this mostly invisibly behind the scenes.

Procedure

Watch a screencast of the steps.

Let’s start by loading your private key’s passphrase into the Apple Keychain, making it available for authentication:

On your Mac, execute:

```
ssh-add -K ~/.ssh/id_rsa
```

This tells OpenSSH to load your private key and decrypt it in memory. If you haven’t already saved your passphrase to the Apple Keychain, macOS will prompt for the passphrase used to encrypt your private key when you created it. Once it has your passphrase, macOS will automatically decrypt and load your private key as needed.

Next confirm your private key is available:

```
ssh-add -L
```

This should show a long public key, which typically starts with ssh-rsa. If it doesn’t show a key, your ssh-agent doesn’t have your private key, and Agent Forwarding will not work.

Assuming your private key is now loaded, you can log into xbio with authentication forwarding active:

```
ssh -p2222 -A pepper@xbio.mskcc.org
```

If your HPC username is different than on your Mac, you need to specify it on the ssh command line.

If this is your first time logging into xbio, or a new Mac, you’ll need to accept the xbio host fingerprint.

Once you’re logged into xbio, confirm your private key is available there as well:

```
ssh-add -L
```
Again, you need to see your public key in the output. If you don't, xbio doesn't have access to your key through ssh-agent back on your Mac, and you cannot ssh into lilac or juno.

```
ssh lilac ssh juno
```

Notes

The error "Permission denied (publickey)." means you tried to connect to an ssh server which requires public key authentication (such as an MSKCC HPC system), but your ssh program doesn't have an authorized private key available. This is typically because your ssh-agent isn't working (doesn't have your private key) or the server doesn't trust your public key.

Assuming your key is available, at this point you should be able to use either ssh lilac or ssh juno from xbio to log into whichever cluster you have access to. If you see your key available on xbio but you cannot log in, there may be a problem with your ~/.ssh/authorized_keys file (missing your public key or incorrect permissions) on the server.

For assistance, you can email hpc-request@cbio.mskcc.org. If you do this, please execute the following commands and include the complete transcript in your email. See below for the details we need to investigate.

Note that on campus xbio has a different name and ssh port (playa.mskcc.org, port 22/tcp). But on campus (or via VPN) you don't need to use xbio -- you can ssh directly into lilac or juno.

The authentication forwarding procedure is very similar to ssh through juno or lilac into a juno or lilac compute node, although lilac nodes only allow ssh access from users currently running jobs on the node.

Warning: If your home directory, .ssh directory, or ~/.ssh/authorized_keys file is group or world writable, ssh considers it insecure and will not let you authenticate. You'll need an admin to fix permissions.

IdentityFile and IdentitiesOnly prevent use of ssh-agent.

Troubleshooting

On your Mac, execute:

```
* ssh-add -K ~/.ssh/id_rsa
* ls -L .ssh
* ls ~/.ssh/id_rsa.pub
* cat ~/.ssh/id_rsa.pub
* cat ~/.ssh/config
* ssh -p2222 -A xbio.mskcc.org
```

Then on xbio, execute:

```
* ssh-add -L
* ssh -v lilac
```

Email your whole session to: hpc-request@cbio.mskcc.org.