Connecting to the AWS Training Environment

Instructors will provide students with credentials and IP addresses to connect to the AWS training environment. This is "pinned" in the course slack channel. Students will need an SSH client which is capable of establishing a SSH terminal session as well as port forwarding. Brief instructions are provided below for a couple SSH clients. Students should forward the local port to the following ports on the AWS side of the tunnel:

- port 8443 - HTTPS access to Grouper, phpMyAdmin, phpLdapAdmin, Shib IdP, Shib SP, rabbitmq

Note, you must not have anything listening on 8443 in your computer

OpenSSH

OpenSSH provides the command line **ssh** client found on most UNIX/Linux/Mac systems. This also works in windows powershell.

On Mac, open Finder Utilties Terminal

Copy and paste the SSH command column of the google sheet with passwords. e.g.

```
$ ssh -L 8443:localhost:8443 -l student    a.b.c.d
```

If you have Mac/Unix and want to use public key:

```
mkdir -p ~/.ssh
chmod 700 .ssh
ssh-keygen -o
```

Make a config file

```
vi ~/.ssh/config

Host gte
   HostName 1.2.3.4
   User student
   LocalForward 8443 localhost:8443
   LocalForward 8432 localhost:5432
   LocalForward 8389 localhost:389
   IdentityFile /Users/myusername/.ssh/id_rsa
   ServerAliveInterval 240
   ServerAliveCountMax 2
```

Save public key on server

```
mkdir .ssh
chmod 700 .ssh
cd .ssh
vi authorized_keys   (press i to edit)
<paste the public key from ~/.ssh/id_rsa>
ESC : w q
chmod 400 authorized_keys
```

Connect to server

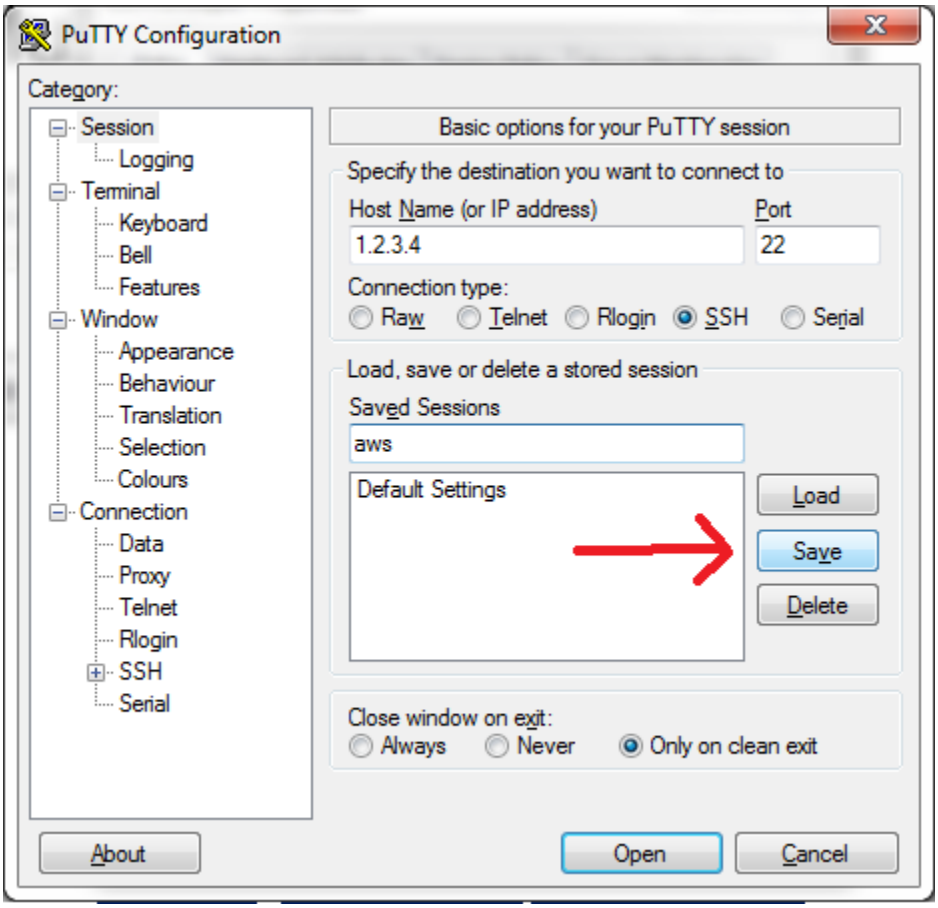
```
mchyzer@Chriss-MacBook-Pro-2 ~ % ssh gte
Last login: Wed Sep 28 06:10:06 2022 from pool-2-3-4-5.phlapa.fios.verizon.net

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[student@ip-1-2-3-4 ~]$
```

Windows PuTTY

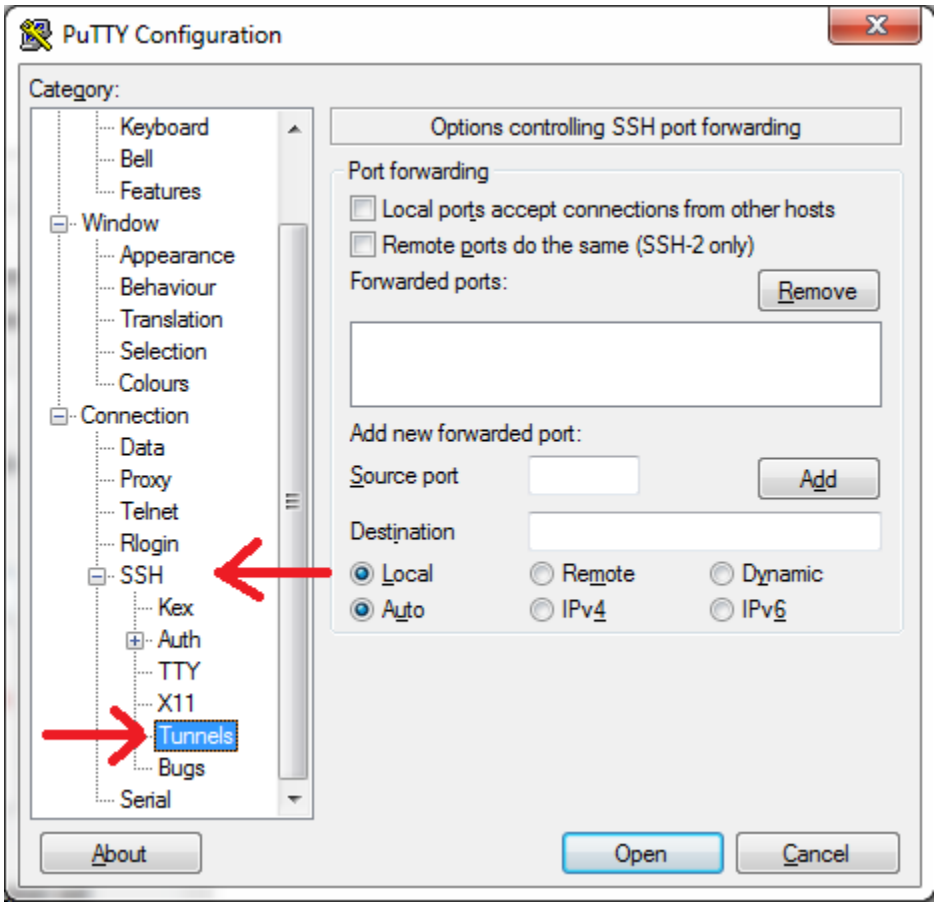
PuTTY is SSH client/terminal software frequently used on Windows operating systems, but also available on Linux systems. Configuration of connections and tunnels is configured using a GUI. See the screen captures below.

Download putty

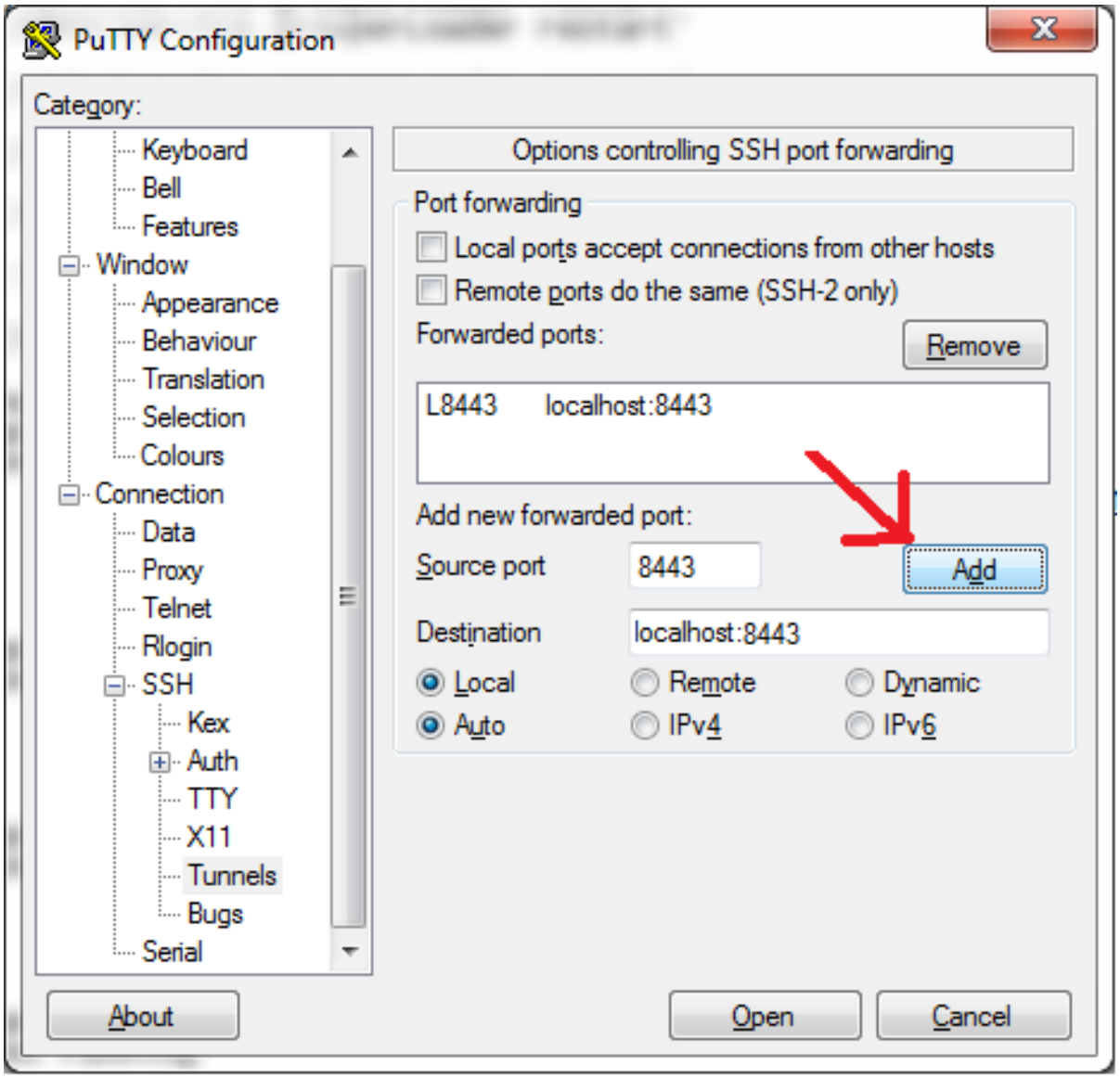
Start a session, to the IP address at AWS



Click on SSH, tunnels



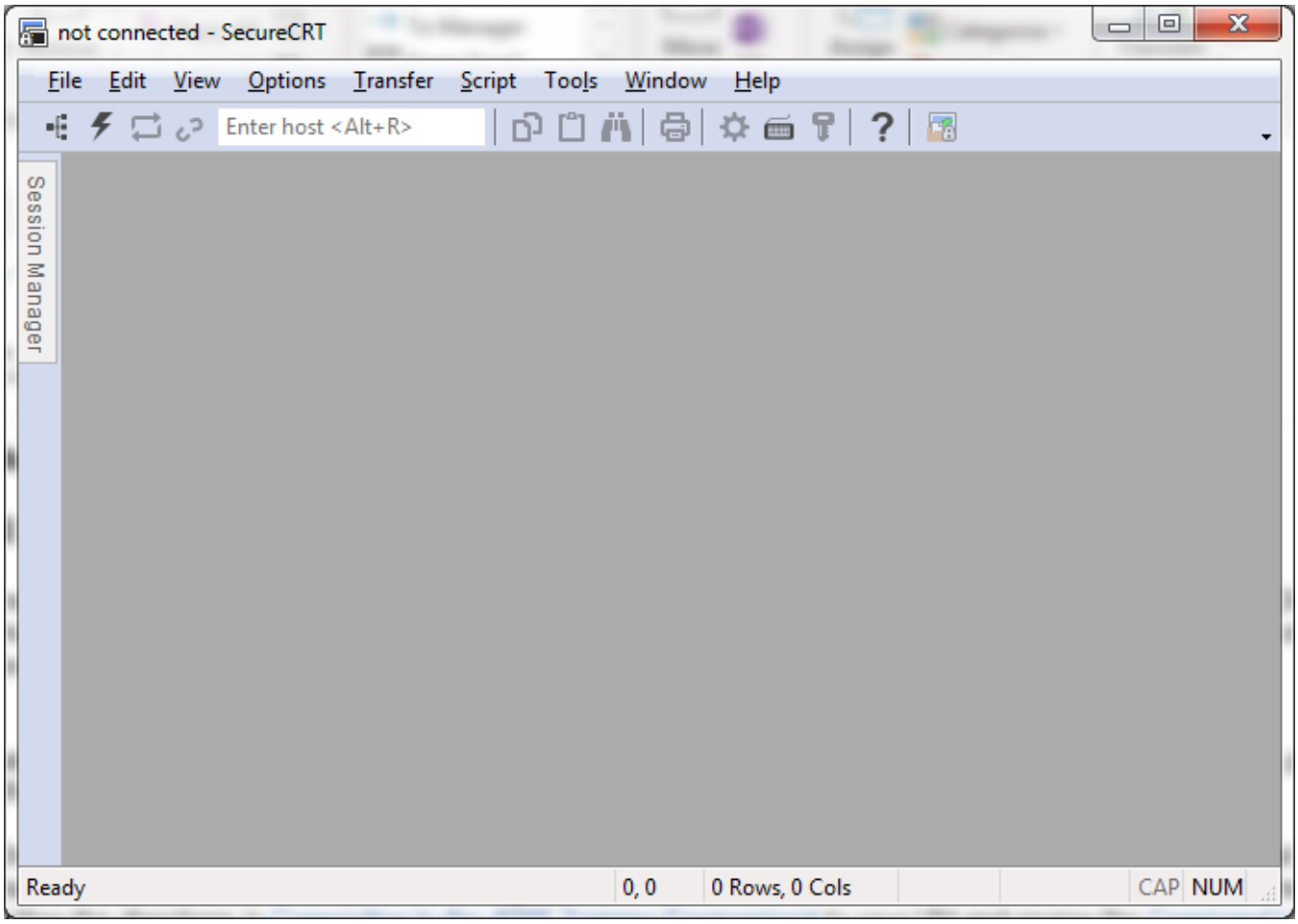
Add one for 8443, and 15672



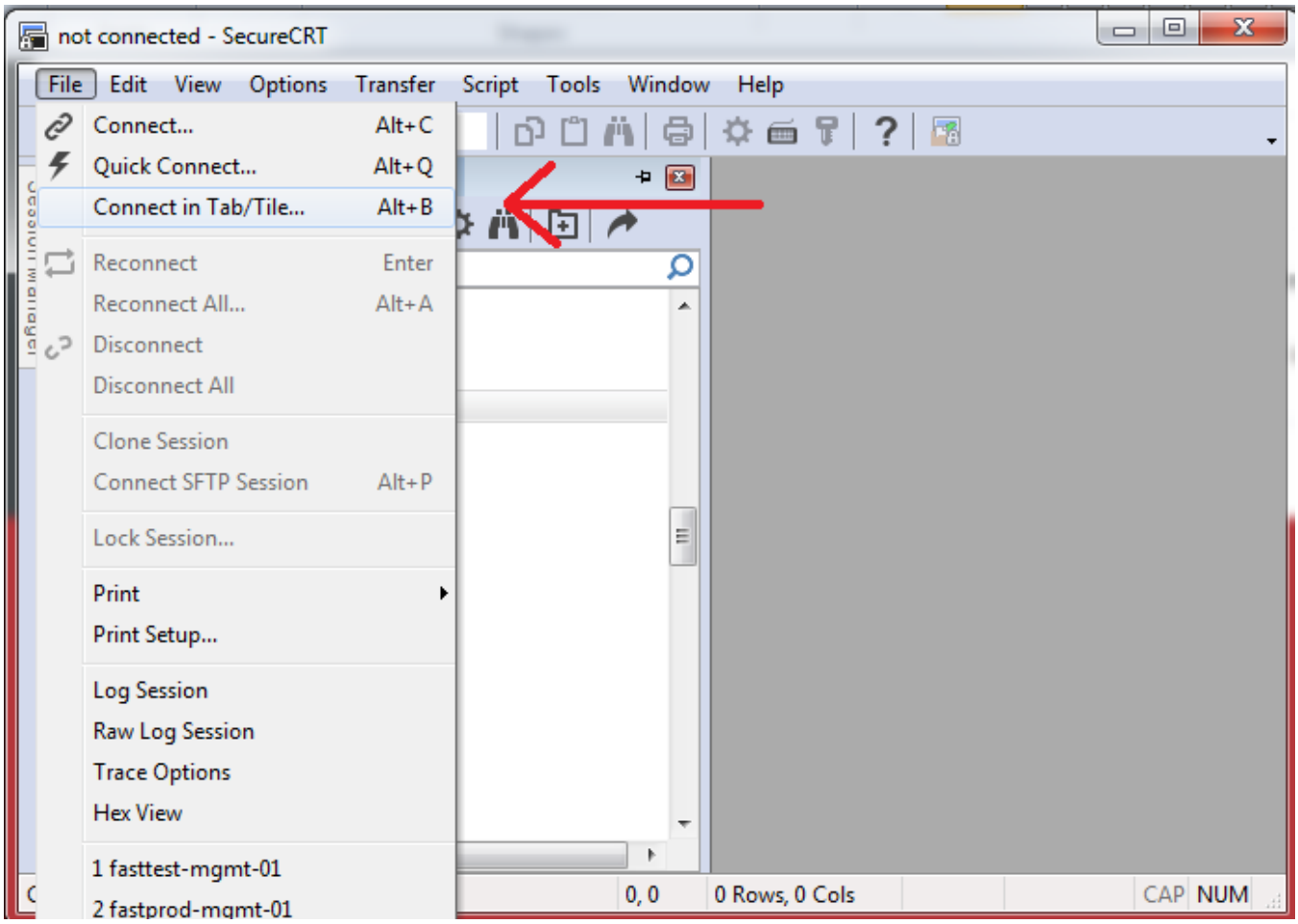
Windows SecureCRT

This is a windows program that might be on your computer from your work. It is not free. So if you dont have SecureCRT already, putty is preferred (above)

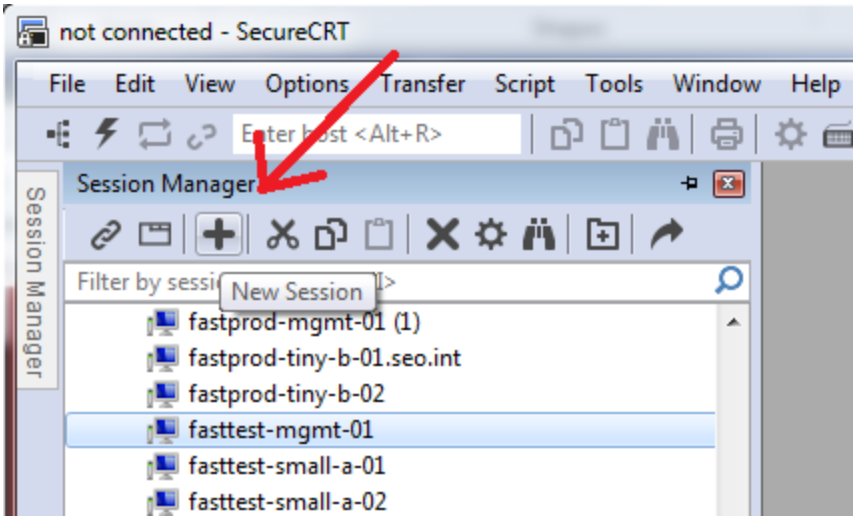
Open SecureCRT



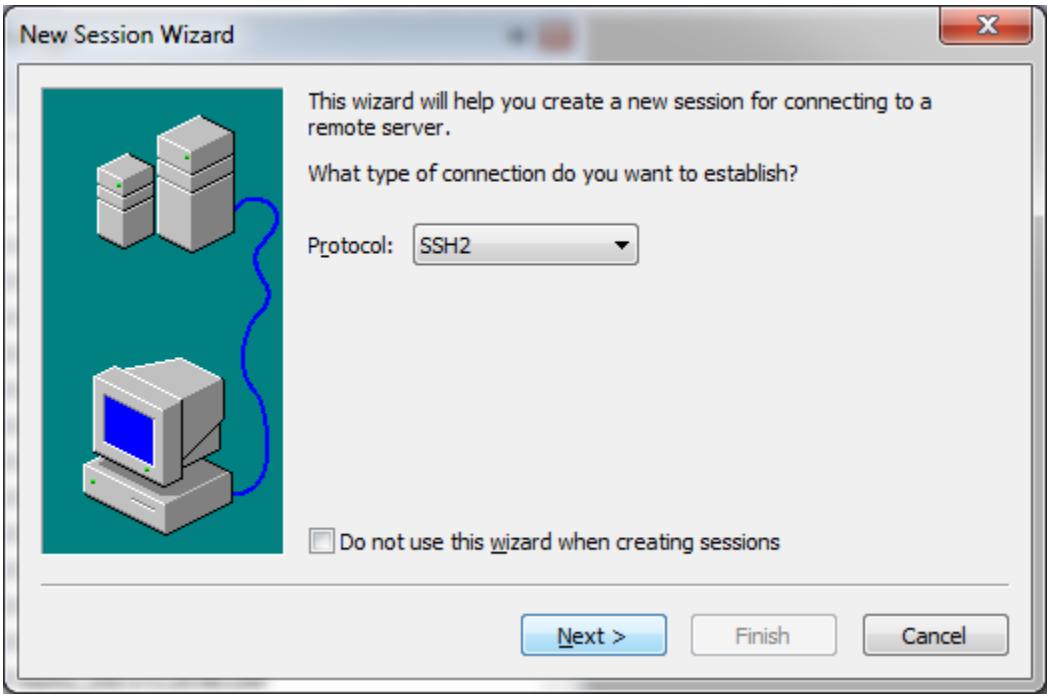
File Connect in Tab/Tile



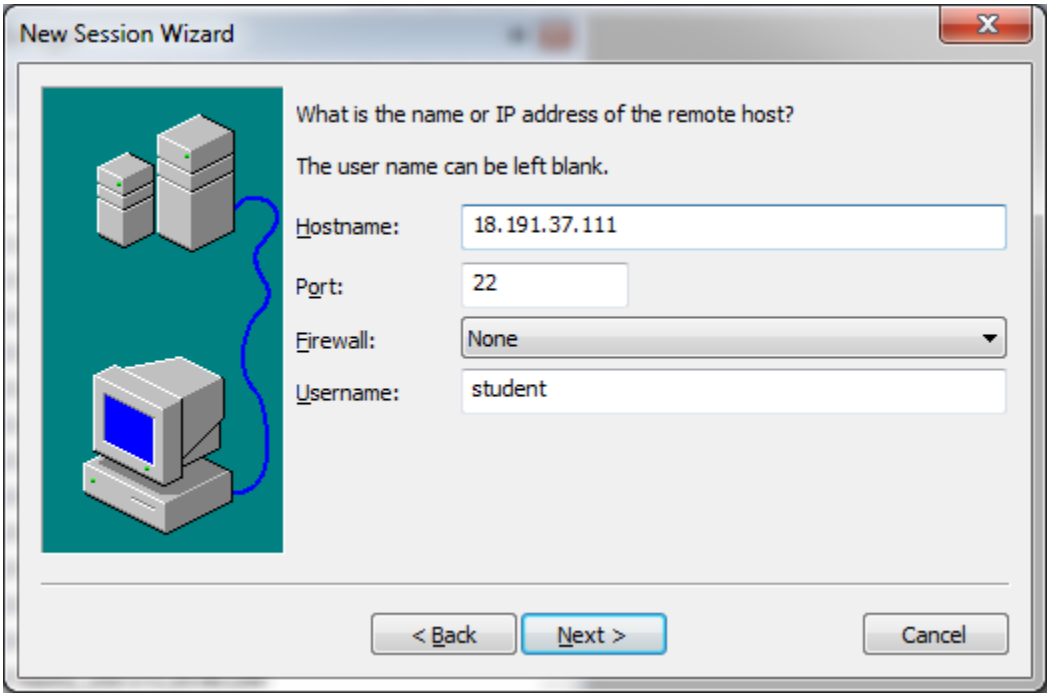
Click the plus sign to make a new session (if you havent connected before)



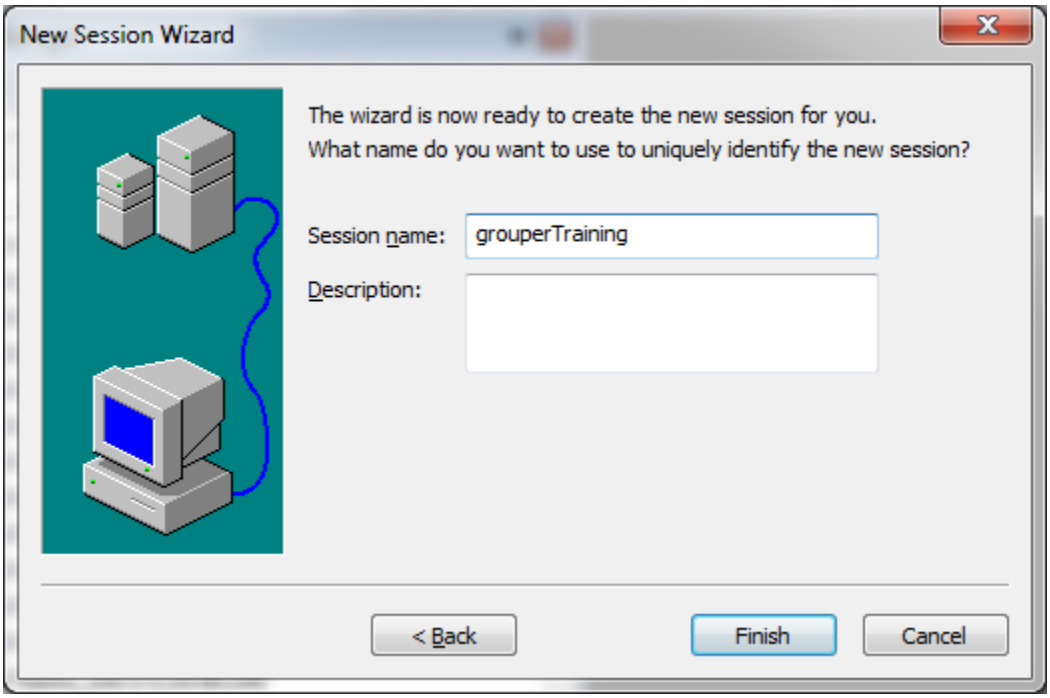
Protocol SSH2



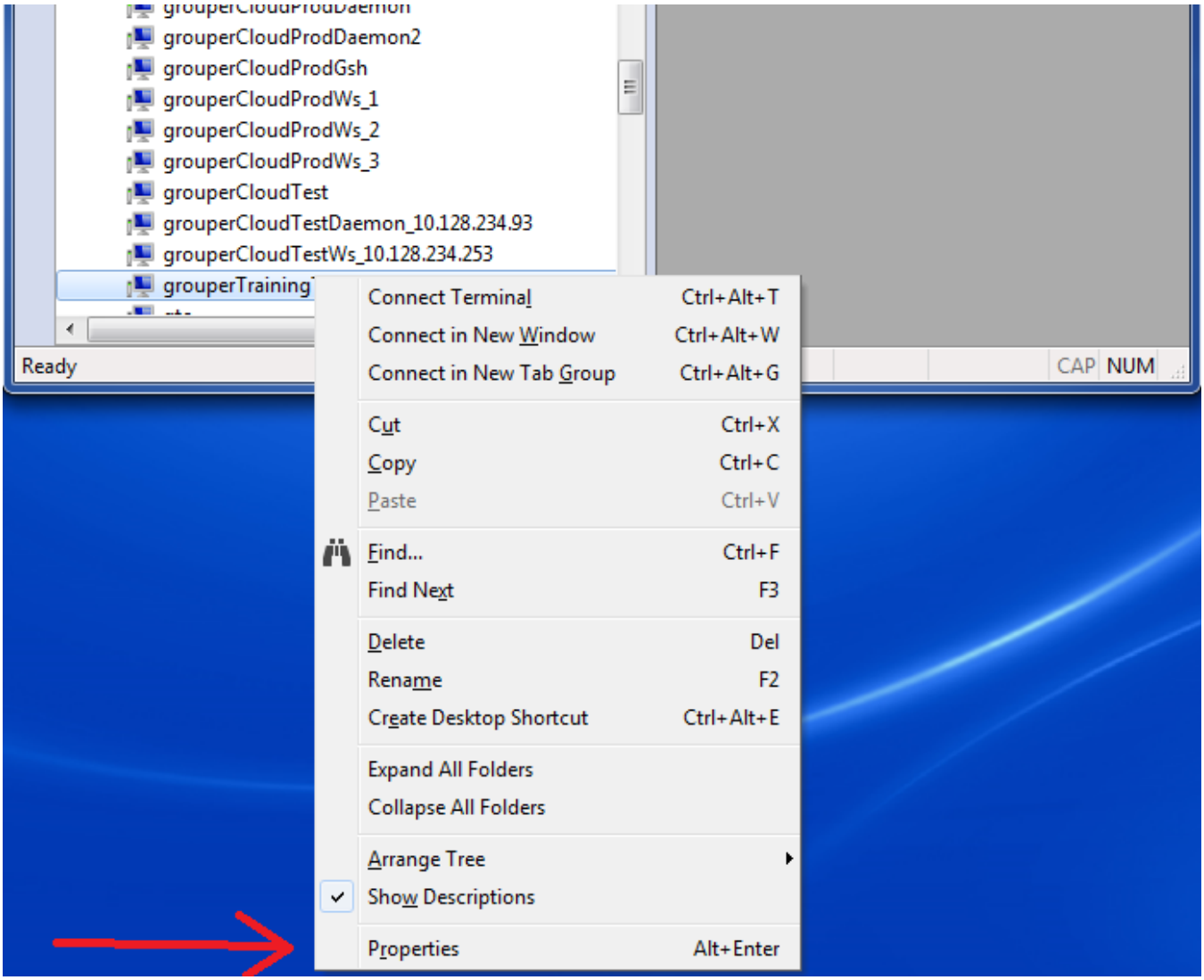
Enter the IP address and username from the google doc of passwords next to your name (note, this is not your IP address



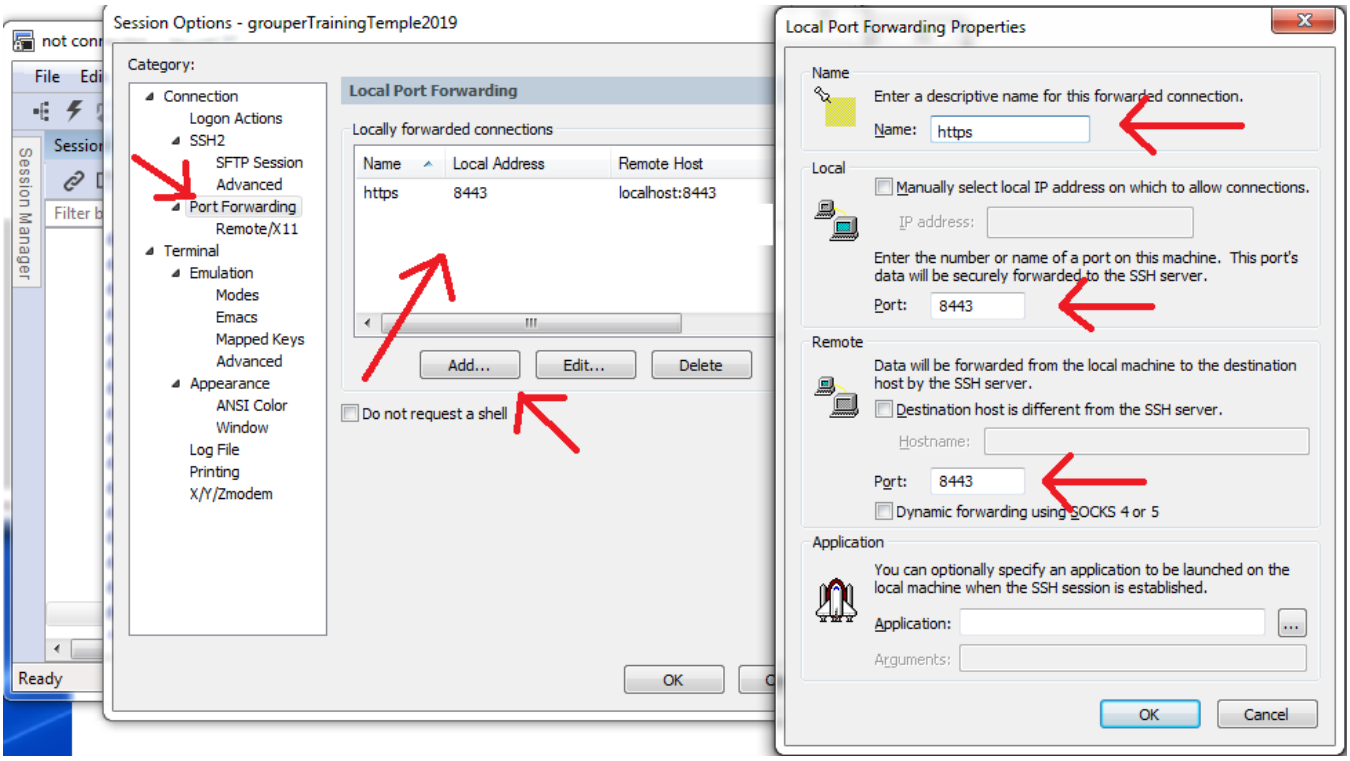
Enter a name for the connection so you can find it later



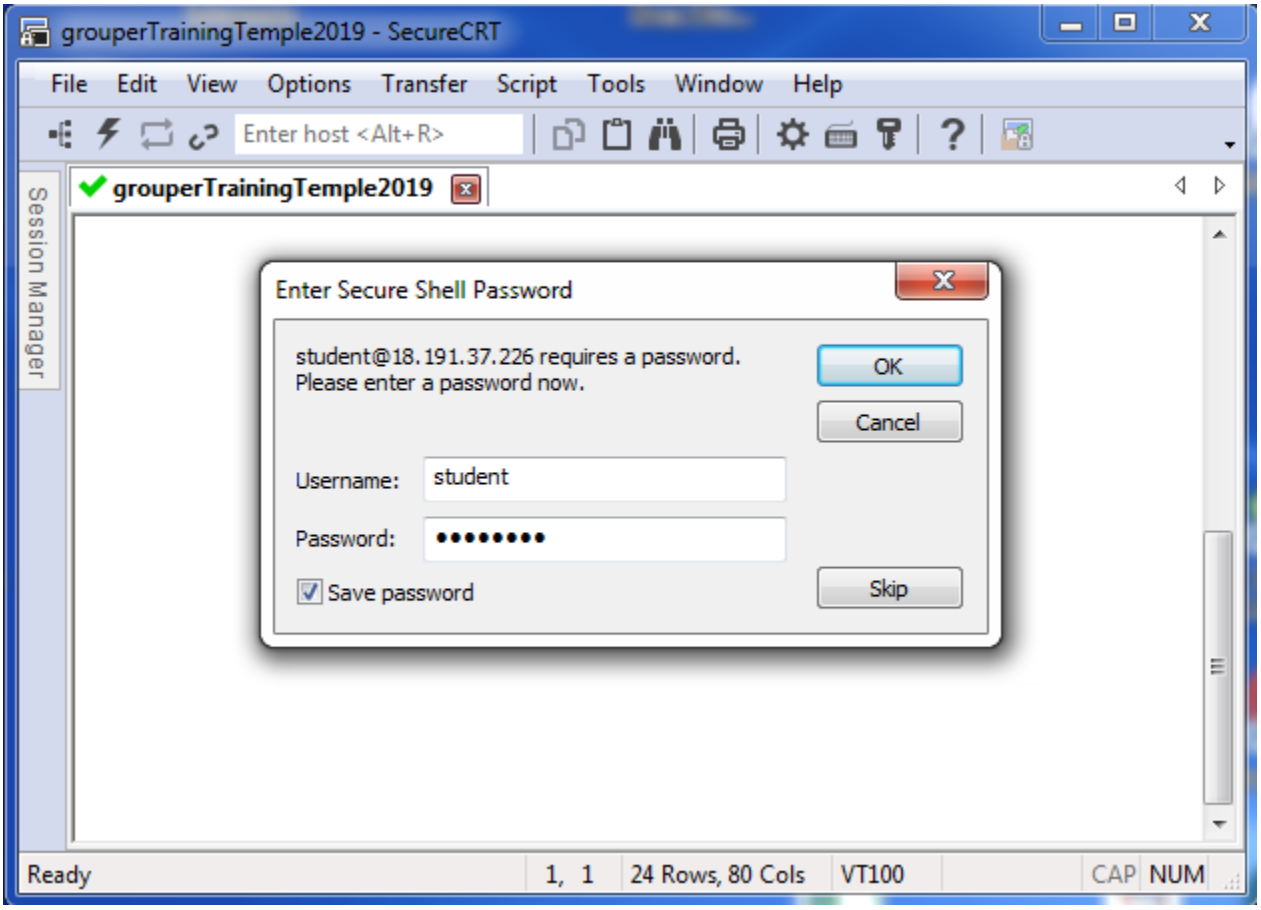
Right click and go to properties on that connection



Add port forwarding for the browser (8443) and rabbitmq (15672)



Connect, save password (from google doc of passwords)



Troubleshooting

If you are having issues with the ssh session timing out after a short period of inactivity, try adding this to your ssh command line:

```
-o TCPKeepAlive=yes -o ServerAliveCountMax=20 -o ServerAliveInterval=15
```