Working Remotely on the School of Meteorology Linux Lab

Patrick T. Marsh
patrick.marsh@ou.edu

Ryan M. May
rmay@ou.edu

Mark J. Laufersweiler
laufers@ou.edu

Last Modified
23 August 2012

Contents

Chapter 1

Introduction

In Meteology we make extensive use of computers, in particular the Linux operating system. If you are like most students, you probably do not want to drive to the School of Meteorology (SoM) Linux Lab every time you want, or need, to access data available on the SoM network. To be able to access the SoM computers remotely is not hard, but it also is not trivial. This guide is written to help you achieve this goal.

For security purposes you cannot connect directly to computers located inside the National Weather Center. Instead, you will actually be connecting to a bastion host, which is a computer that has the ability to receive connections from outside the NWC and then allow a user to connect to a different computer located on the NWC network. To do this, we will be making use a network protocol called *Secure Shell*, or SSH, for short. This protocol allows a user from one computer to access and work remotely on another computer via a terminal. Depending on your operating system, there are different terminals available to you.

It is only fair to warn users that the methods of remotely accessing the SoM computing network discussed in this document rely on resources that are maintained outside the SoM control. In particular, both the Aventail client and the Bastian host are maintained by OUIT via the National Weather Center (NWC) Network Operations Center (NOC).

Chapter 2

Connecting to the SoM Network

2.1 Connecting via Bastian Host

BEFORE YOU ATTEMPT TO DO THIS, YOU MUST FIRST SUBMIT YOUR 4X4 TO MARK LAUFERSWEILER VIA `http://som.ou.edu/computing/forms/bastion/`. Please note that when you try to access this website it will ask you for your username and password. These are your **OU-SoM username and password**, (i.e., the ones you would use to log in to either the Linux or Mac lab computers).

2.1.1 Connecting from Your Computer to the Bastian Host

As mentioned in the Introduction, we cannot connect directly to the computing network used by the SoM. Instead we must first connect to a bastian host and then from there we can log on to the SoM network. For our purposes the bastian host we will be using is named "STARBUCK".

2.1.1.1 Windows

Those using a Windows operating system will need to download a SSH client[1]

The configuration of Windows SSH software is different for each program and thus will not be convered in this section. Instead you can check Appendix B for specific information regarding each piece of software. The general information that you will need to know to setup each program is the hostname of the computer you wish to connect.

- ⋆ Hostname: **starbuck.nwc.ou.edu**

Using this information, please refer to the specific instructions in Appendix B on how to configure and execute your specific program.

2.1.1.2 OSX and Linux

For those using an Apple computer or any of the various Linux distributions, the instructions to log on to STARBUCK are fairly straight forward; you simply need to do the following from an SSH terminal[2]:

ssh your-OU-4x4-here@starbuck.nwc.ou.edu

If this is your first time connecting to STARBUCK you will be asked if you will accept the authentication. This is normal, so go ahead and accept it. If you do not, you will be unable to complete the log on to STARBUCK and will be unable to then remotely log on to the Linux Lab computers. After accepting the authentication, you will then be asked for your password. **This is your OU4x4 password!**, not your SoM Computing password.

[1] If you are unsure what SSH terminals are available for the Windows operating system, please see Appendix A.1.
[2] If you are unsure what SSH terminals are available for the OSX operating system, please see Appendix A.2.

2.1.2 Connecting from the Bastian Host to the SoM Network

Once you have typed in your password you will be connected to STARBUCK. From here you will then be able to log on to the SoM network. To do this we will need to once again use SSH, but this time we will use our SoM computing information.

SoM Linux Lab computers have the following naming convention:

somclass##.som.nor.ou.edu **(where ## is a number from 01-24**[3]**)**

Remember, we are connecting to a SoM computer so we need to use our SoM computing account information. From STARBUCK, type:

ssh your-SoM-Username-here@somclass##.som.nor.ou.edu

Again, if this is your first time to connect to this particularl machine you will be asked to accept authentication. After doing so, you will be asked for your password. Once again, **this is your SoM Computing Account password!**

You are now connected to the SoM Linux Lab (in particular, the computer number ## — which you chose). Please remember to use considerate computing techniques!

2.2 Connecting via VPN (Aventail Client)

For those of you who do not wish to use the Bastian host, you might be able to use the Virtual Private Network (VPN). However, be warned that the Aventail will most likely not work for most of you due to permission issues outside the SoM's control. The idea behind a VPN is that once activated it makes your computer think that it is virtually connected to a different network. For our purposes this means that we can "trick" our computer to believing it is on the SoM network. This would allow us to directly connect to a SoM computer without having to first connect to Starbuck.

The VPN client used for SoM is called Aventail. To download the Aventail client go to `http://som.ou.edu/computing/downloads/downloads.html` and download the client that corresponds to your operating system and then go ahead and install it.

To launch the program, double click on the icon. For Windows uses, the Aventail client will be found in the Start Menu. For OSX users, it will be found in the Applications directory.

The first time you launch the program you will see a screen that says "Configuration:" with an empty drop down menus to the right of "Configuration". To conifgure the Aventail client, click on the drop down menu and choose "Create/Edit Configuration". A new window should open. When the window first pops up the form on the right of the window should be grayed out. To be able to fill out the form, click on the "+" on the lower left of the window to create a new VPN configuration. After doing this the form on the

[3] Yes! The leading 0 is important for numbers less than 10!

right of the window should change to allow you to enter information.

The configuration name should be something that will allow you to remember that this is to log you on to the SoM Computer Accounts. I suggest something like "SoM Connect", however anythign will suffice. However, the host name and login group must be as listed below.

- ⋆ Configuration Name: **SoM Connect**
- ⋆ Host Name: **apollo.nwc.ou.edu**

After supplying the information above, click on the "Change" button. This should populate the Login Group with "OU Tenants", and then after a few seconds, create a "Username" and "Passowrd" option in the Authentication section. (Please note that you may get a pop up window asking you to accept a security certificate. This is normal. Go ahead and accept.). To fill out the Authentication section use the following:

- ⋆ Username: **Your OU4x4**
- ⋆ Password: **OU4x4 Password**

After filling out this portion of the form, click on the "Validate" button. If your information is correct a pop up message should appear saying that you were "Successfully Authenticated". If your information is incorrect or you do not have a Bastian Host account (yes, you need that for this to work), you will see a pop up message with the message "Authentication Failure". At this point, please double check your information. If it is correct, please contact `laufers@ou.edu` for further assistance.

If everything is correct and validated, please click "Save" and then "Close". At this point you should return to the main Aventail window. Please select the Configuration drop down menu and select the confuration settings you just made. Fill in the Username and Password (**remembering this is your OU4x4 information!**) and click connect. When the Aventail window disappears, you are now connected to the SoM network, or more precisely, the OU network.

At this point, the directions to log on to a SoM computer are identical to the directions for Bastian host users to connect to the Bastian host, except instead of connecting to STARBUCK using your OU4x4, you connect to the SoM Linux Lab and use your SoM computing account. Specifically, you will be connecting to a machine that has a name of the form:

somclass##.som.nor.ou.edu **(where ## is a number from 01-24**[4]**)**

For more information on how to set up a SSH connection on various operating systems, please refer to the operating system specific information provided in section 2.1.1.

LASTLY, A NOTE OF CAUTION FOR THOSE USING AVENTAIL TO CONNECT TO THE SOM. When you use a VPN, like Aventail, your computer is "tricked" into believing that it is on a different network. In this case, your computer believes it is connected to the private SoM network. This means that whatever you do that requires the Internet is being routed through the university servers. **WHEN CONNECTED TO AVENTAIL I STRONGLY ENCOURAGE YOU NOT TO DO ANYTHING THAT**

[4] Yes! The leading 0 is important for numbers less than 10!

YOU WOULD NOT WANT SOMEONE ELSE TO KNOW ABOUT. THIS INCLUDES WHAT WEBSITES YOU VISIT. Because your computer's network devices (ethernet port, wireless, etc) have a unique identifier associated with it (called a MAC address), it is possible that if you are doing something illegal, it can be found out and traced back to you. (Remember, if you've connected your device to the OU Wireless networks, you were required to register your computer to your OU4x4!)

Chapter 3

File Transfer

3.1 File Transfer with Bastian Host

TODO...

3.1.1 SSH Tunnels

TODO...

3.2 File Transfer with VPN (such as Aventail)

TODO...

Appendices

Appendix A

Aquiring SSH Software

As mentioned in the beginning of this guide, how you utilize the SSH protocol depends on your operating system. In particular, there are different terminals available on different operating systems. This appendix is dedicated to ensuring that you have the correct tools for your particular system.

A.1 Windows

On the Windows Operating System we will be making use of one of two programs: **SSH Secure Shell Client**or **PuTTy**.

A.1.1 SSH Secure Shell Client

If you chose to use SSH Secure Shell, it can be downloaded from the SoM Computing Website at (`http://som.ou.edu/computing/downloads/files/`). To install, download the files, click on the SSH Secure Shell Client v.3.2.5 link and double click the resulting download. After installing the program you should see two icons on your desktop: the "SSH Secture Shell Client" and the "SSH Secure File Transfer Client".

A.1.2 PuTTy

If you choose to use PuTTy, you can download it here: `http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html`. You will want to choose the download option that contains all applications; it should be a zip file. To run PuTTy, you will need to unzip the downloaded file, open the resulting folder, and double click PUTTY.EXE.

A.2 OSX

A.2.1 Terminal

Apple users have a terminal application that ships with the OSX operating system. The terminal application is creatively called “Terminal” To access the default terminal one can either type “Terminal” into spotlight or one can:

1. Open up Finder
2. Click on the Applications Folder
3. Open the Utilities Folder
4. Click on Terminal.app

A.2.2 iTerm2

For users who find the default OSX Terminal application a bit lacking an alternative terminal application is available for free from `http://www.iterm2.com`. To install iTerm2:

1. Go to `http://www.iterm2.com/`
2. Click on the large download button on the bottom of the screen
3. From the downloads page select `iTerm2_v1_0_0.zip`
4. On the next page, once again select `iTerm2_v1_0_0.zip`
5. Unzip the package that was just downloaded
6. Move iTerm.app contained in the newly unzipped folder to your Applications folder. (If you do not know where this is located, please check the directions listed in section **??**.)
7. Double click iTerm2.app to start iTerm2

Appendix B

Windows Configuration

B.1 Standard SSH Setup Configuration

This section will detail how to configure the specific SSH client listed in the header.

B.1.1 SSH Secure Shell Client 32

To configure the SSH Secure Shell Client, use the following steps:

1. Double click the icon labeled "SSH Secure Shell Client" to launch the program.
2. Click on the "Profiles" button in the top middle.
3. In the resulting menu, click on the "Edit Profiles" option.
4. This should take you to a new screen. On the new screen, in the "Hostname" box, please enter the correct hostname. You may need to refer back to earlier portions of this document to determine the correct hostname.
5. Enter your username for accessing the machine listed in the hostname.
6. Click OK
7. You should now be back at the main screen. Once again, click on "Profiles".
8. Click on "Add Profile"
9. Enter a name by which to remember these connection options.

Now, anytime you wish to connect to this connection, all you need to do is choose this configuration name from the "Profiles" menu.

B.1.2 PuTTy

To configure PuTTy, use the following steps:

1. Double click on "PUTTY.EXE" to launch the program.
2. In the resulting screen, enter your hostname in the hostname space. You may need to refer back to earlier portions of this document to determine the correct hostname.
3. In the "Saved Sessions" blank (middle of the screen), please give a name to remember this connection configuration. Then click "SAVE".
4. Next click on the "Open" button in the bottom right.

Now, anytime you wish to connect to this connection, all you need to do is choose this configuration name from the "Profiles" menu. However, it will ask you for your logon name everytime you try to connect. To have PuTTy remember your login name:

1. Restart PuTTy
2. Click on the name of the saved session to which you want to add a username
3. Click "Load"
4. On the far left, (in the hierarchy), click on "Data". It will be toward to bottom of the list.
5. In the new screen on the right, enter the username into the "Auto-login username" box.
6. Click "Session" from the hierarchy on the left.
7. Click "Save"

Now you have saved a username with this configuration and should no longer be prompted for your username.

B.2 SSH Tunnel Configuration

TODO...

B.2.1 SSH Secure Shell Client 32

TODO...

B.2.2 PuTTy

TODO...