System Administration & Security

COMP 175 | Fall 2021 | University of the Pacific | Jeff Shafer

AWS: Getting Started

Lab 1 – AWS Virtual Machine Quick-Start

- Today's Goals
  - Deploy a virtual machine
    - Use Amazon Web Services (AWS) Elastic Compute Cloud (EC2) to obtain an instance on demand
  - Connect to it via Secure Shell (SSH)
  - Run a few basic commands at the terminal
  - Document your work w/screenshots
  - Shutdown the virtual machine
- **Opportunity to become familiar with tools and resolve any technical difficulties**

Intro to Amazon EC2

AMAZON EC2

amazon web services

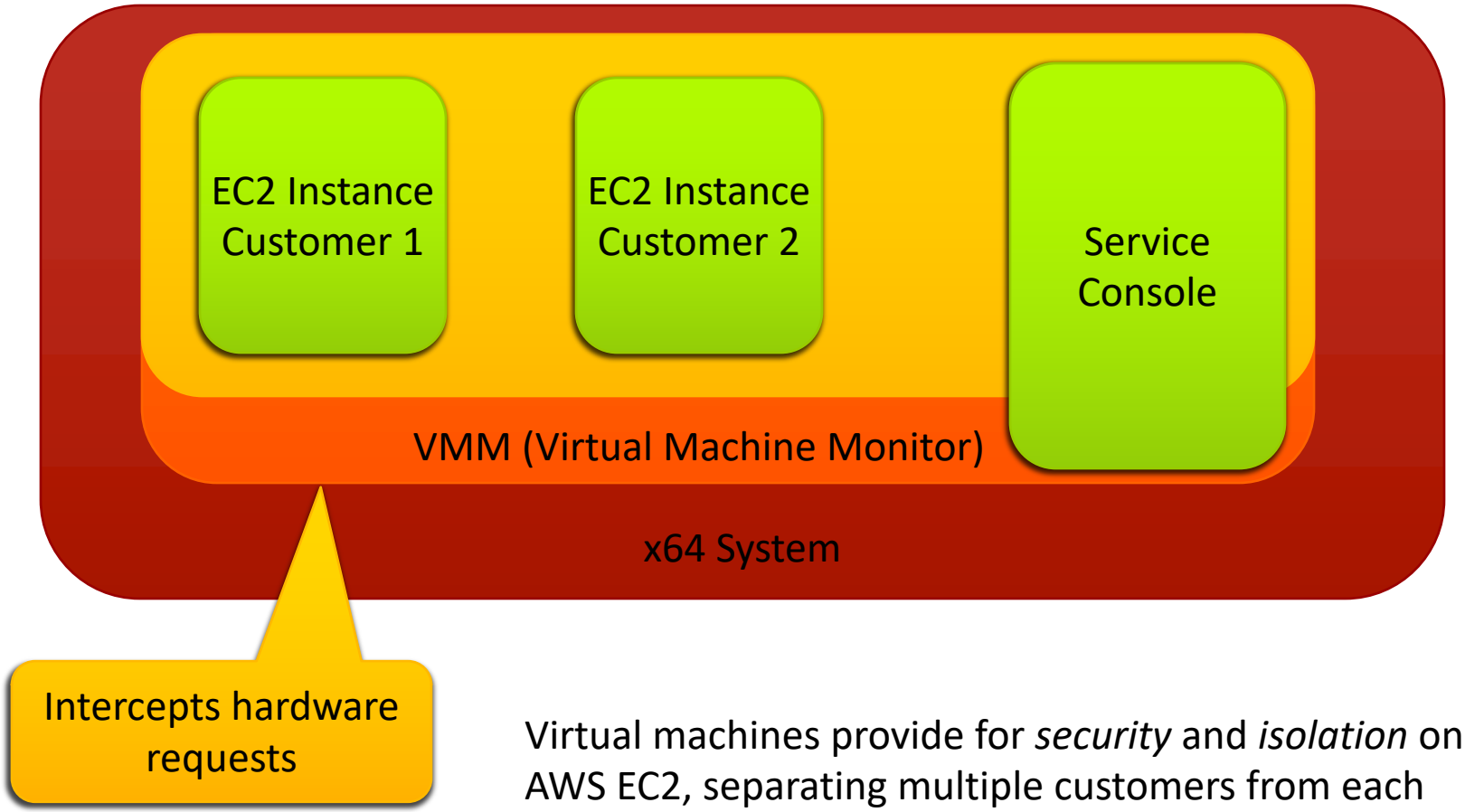
AWS.AMAZON.COM/EC2

https://www.youtube.com/watch?v=TsRBftzZsQo

Key Concepts for EC2

- Rent servers *on demand* and access them immediately
  - Small/Weak/Cheap?
  - Large/Powerful/Expensive?
  - **Many** options to choose from
- Pay per hour based on what you use
  - Pay for the compute usage
  - Pay for the storage usage
  - Pay for the network (outbound) usage
  - *Reserved instances* – Pay in advance, but cheaper
- Control via GUI or within a program (API access)
- Storage
  - Instance Storage
    - On the physical machine
    - *Ephemeral* – If you shut down the VM, this storage is gone!
  - Elastic Block Store (EBS)
    - Accessible over the network
    - Can *persist* after a VM is shut down (if configured)
- Virtual Private Cloud
  - Logically isolated network that you control

VMs - Security and Isolation



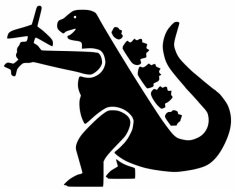
Virtual machines provide for *security* and *isolation* on AWS EC2, separating multiple customers from each other on the same hardware

AWS Regions (July 2021)

https://aws.amazon.com/about-aws/global-infrastructure/

AWS Infrastructure

- As-of July 2021
- **25 Regions**
  - Separate geographic area
  - Close to customers (lower latency, higher bandwidth)
  - Widely dispersed in case of disaster
  - Example: `us-east-1`



- **81 Availability Zones**
  - Multiple zones per region
  - Isolated *part* of a region (but yet closer, allowing applications to be distributed across availability zones faster/cheaper)
  - Example: `us-east-1`**b**

https://aws.amazon.com/about-aws/global-infrastructure/

$$$

We'll talk about billing (and monitoring $$/hour) in a future week, but for now…

Don't leave your VMs running when you're not using them!!

$100/student

For your course profile

Your account is **locked** when the limit is reached
(your files are **inaccessible**, all VMs shut down)

Learner Lab - Foundational Ser

https://awsacademy.instructure.com/courses/5013/modules/items/569201

ALLFv1-5013 > Modules > Learner Lab Foundation Services > Learner Lab - Foundational Services

Account
Dashboard
Courses
Calendar
Inbox
History
Help

Home
Modules
Discussions

AWS | Used $0 of $100 | 03:55 | ▶ Start Lab | ■ End Lab | AWS Details | Readme | Reset

ddd_v1_w_xkHh_643053@runweb25:~$

Launch AWS Management Console

Class Budget Spent (Must last entire semester)

Session Time Remaining

Close

Region: us-east-1
Lab ID: arn:aws:cloudformation:us-east-1:189852843776:stack/c37351a481098l910174t
f3f2-11eb-aaed-1242d233c5ef
Creation Time: 2021-08-02T17:37:02-0700

Start session at: 2021-08-02T17:37:03-0700
Remaining session time: 04:00:00(240 minutes)

Keep a close eye on how fast this is decreasing!

You are currently logged into Student View

Resetting the test student will clear all history for this student, allowing you to view the course as a brand new student.

Reset Student | Leave Student View

AWS Academy *Restrictions*

- Region: **ONLY** us-east-1 [N. Virginia] and us-west-2 (Oregon)
- Instance types: **ONLY**
  - nano, micro, small, medium, large
  - (Varying amounts of CPU and RAM)
- EC2 features
  - No spot instances
  - No reserved instances
  - No VPN Gateway
- No Marketplace (pre-built AMI images from 3rd parties)
  - Not supported (not even free ones) ☹

Secure Shell (SSH)

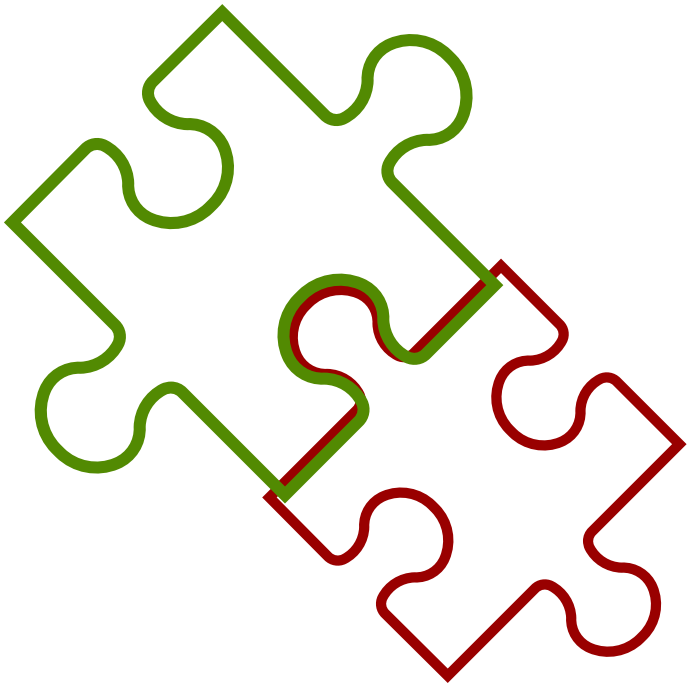
Secure Shell (SSH)

- Provides an encrypted channel between two computers on a network
- Applications
  - **Remote command line**
  - Tunneling of arbitrary network traffic
  - TCP port forwarding
  - X11 display forwarding
  - File transfer
    - SSH File Transfer (SFTP)
    - Secure Copy (SCP)

SSH Authentication Methods

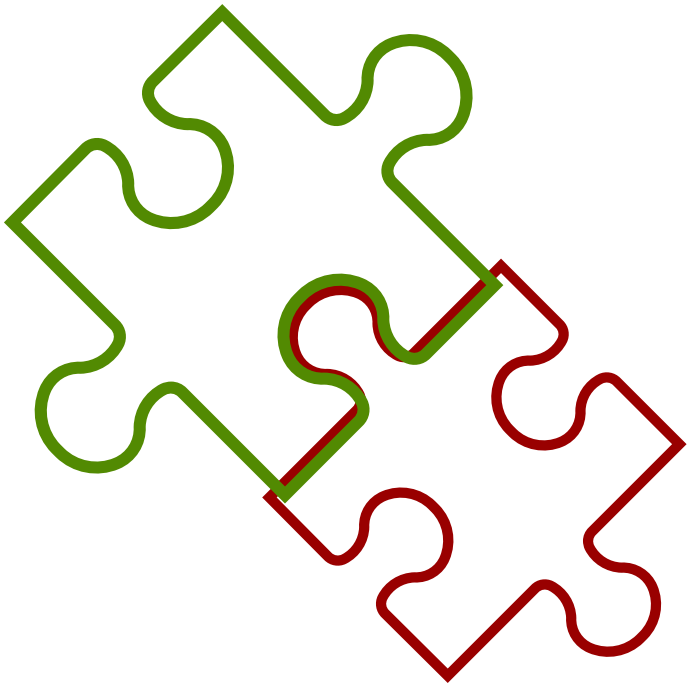
- Password
  - Username & Password
- **Public Key**
  - Username and Public Key / Private Key
  - Security advantages: Longer/random
  - *Amazon EC2 uses 2048-bit SSH-2 RSA keys*
- *Other options for single sign-on via GSSAPI (Generic Security Services Application Program Interface)*

SSH Public & Private Keys



- **Public Key**
  - Public! Safe to distribute widely
- **Private Key**
  - Private! *Only you should have this piece*
- With the ***public key***, I can **encrypt** a message that only the ***private key*** can **decrypt**

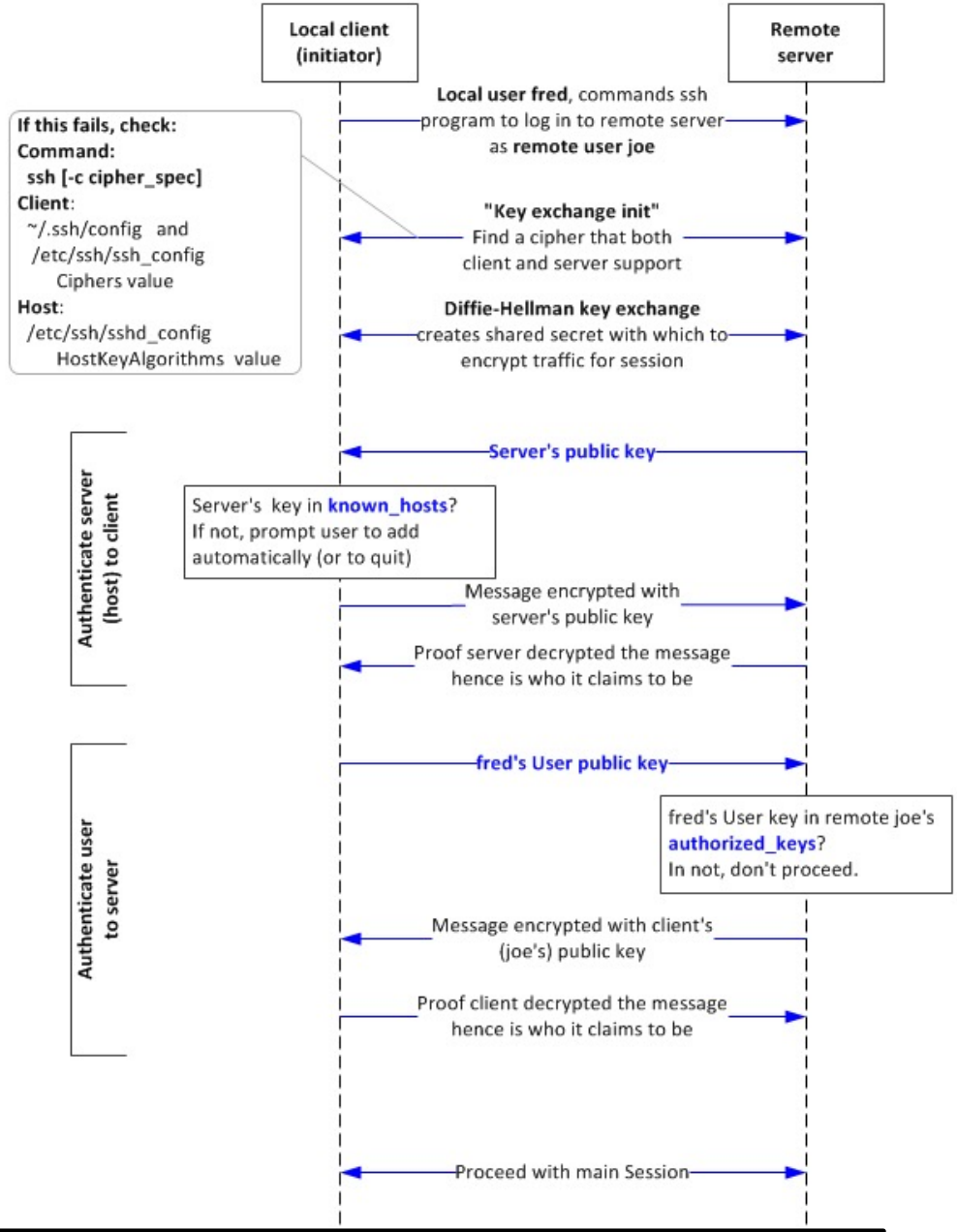
SSH Public & Private Keys



- AWS can generate a *keypair* (**public** & **private** key) for you
- **Private key** : You can download it once
  - AWS does not keep a copy
  - If lost, you cannot recover or recreate file – only solution is to abandon keypair and generate a new one
  - **Anyone who possesses your private key can logon to your EC2 instances**
- **Public key**: AWS keeps a copy and places it on every EC2 instance you start

Files involved in SSH connection: in use

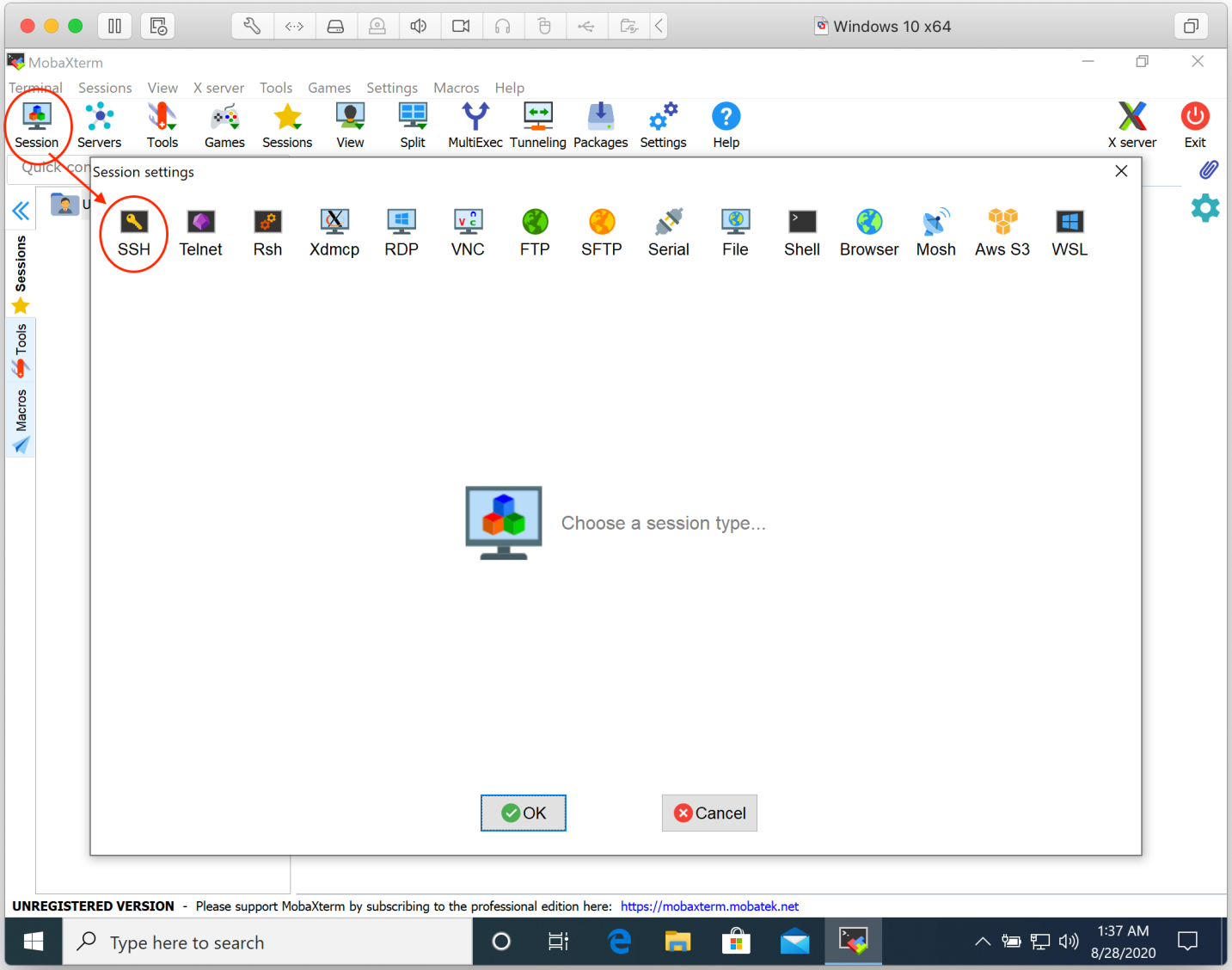
gwideman 2018-10-14

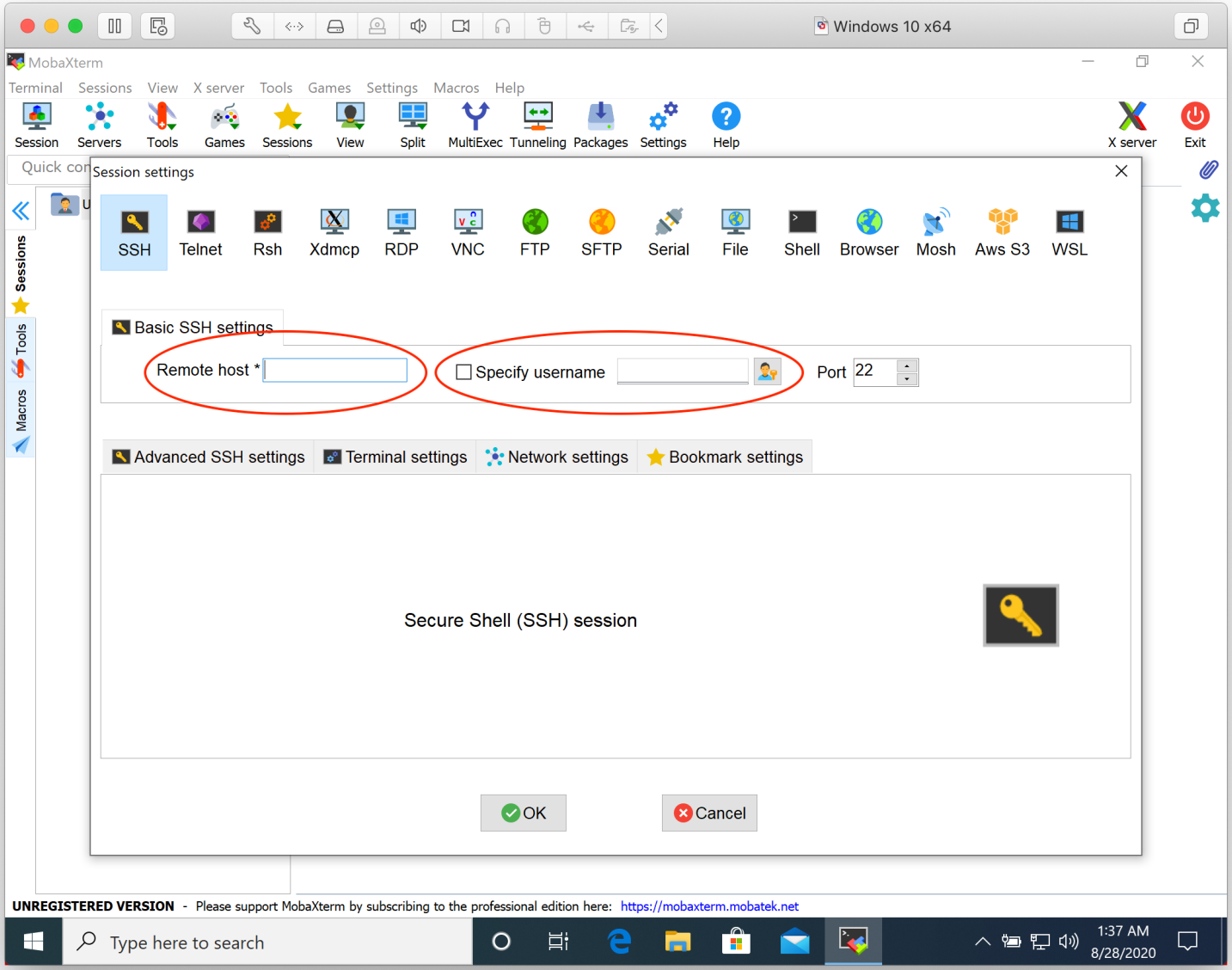


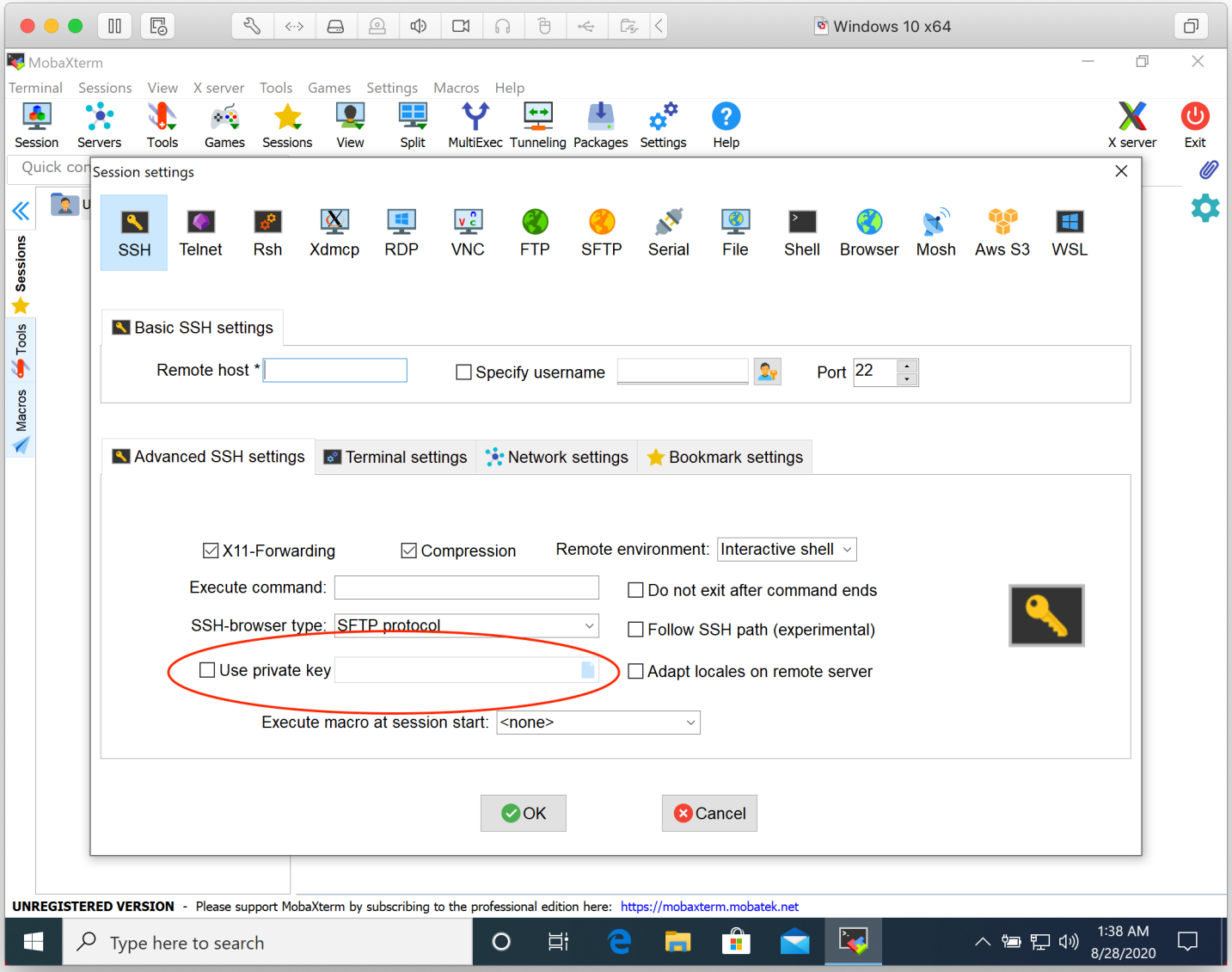
https://serverfault.com/questions/935666/ssh-authentication-sequence-and-key-files-explain

SSH Clients - Windows

- **PuTTY**
  - Free! **Classic!** Cross-Platform! Documented everywhere!
  - GUI hasn't been improved since 1999 release and is *super clunky*… ☹
  - https://www.chiark.greenend.org.uk/~sgtatham/putty/
- **OpenSSH** client, optional feature of **PowerShell**
- **MobaXterm**
  - Modern GUI (tabs, etc)
  - Built in X11 server for remote GUI applications
  - Numerous other features (GUI file transfer, …)
  - https://mobaxterm.mobatek.net/


Windows 10 x64
MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Session settings
SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL
Choose a session type...
OK
Cancel
Sessions
Tools
Macros
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
1:37 AM
8/28/2020


Windows 10 x64
MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Session settings
SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL
Basic SSH settings
Remote host *
Specify username
Port 22
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
Secure Shell (SSH) session
OK
Cancel
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
1:37 AM
8/28/2020

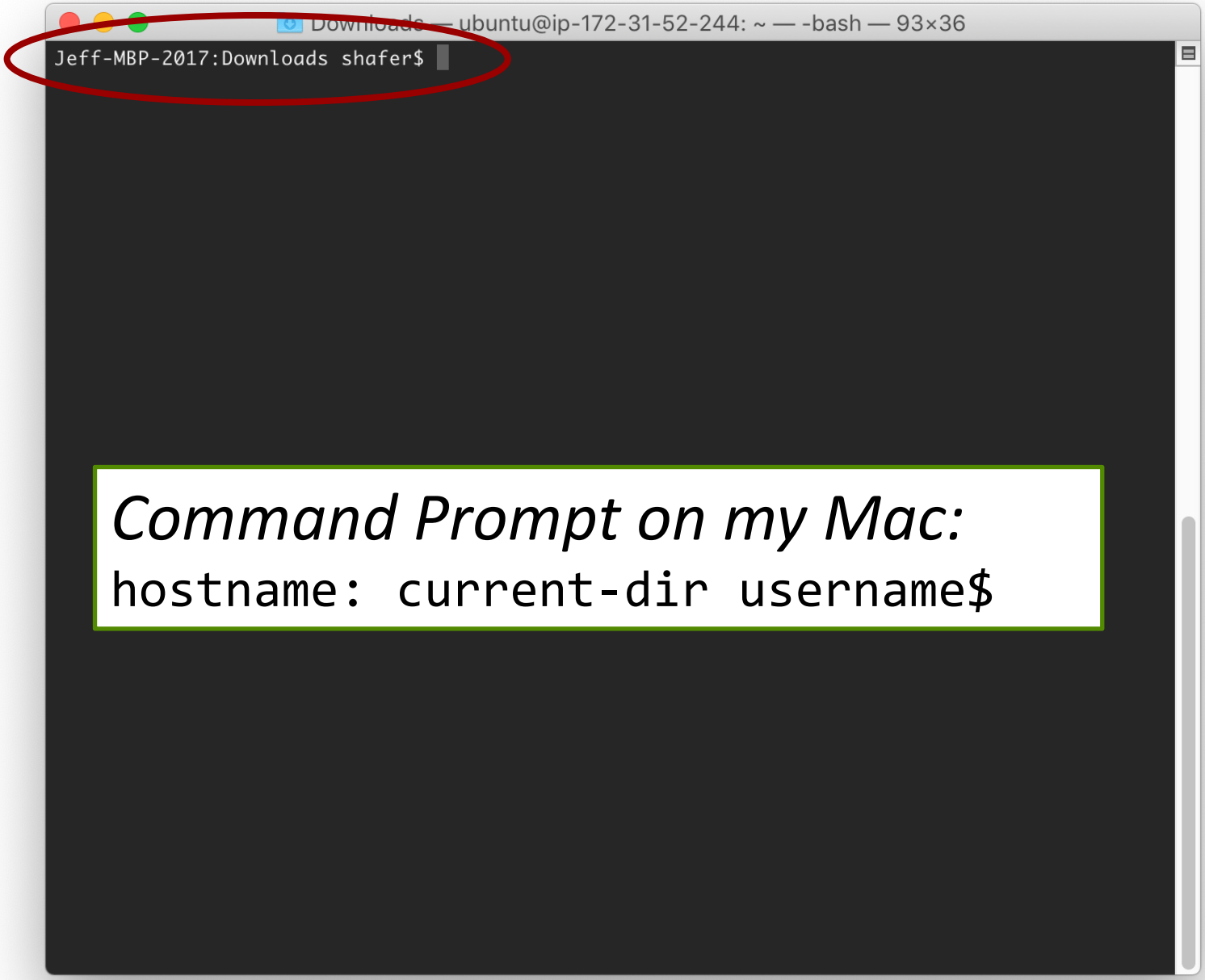

Windows 10 x64
MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Session settings
SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL
Basic SSH settings
Remote host *
Specify username
Port 22
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
X11-Forwarding
Compression
Remote environment: Interactive shell
Execute command:
Do not exit after command ends
SSH-browser type: SFTP protocol
Follow SSH path (experimental)
Use private key
Adapt locales on remote server
Execute macro at session start: <none>
OK
Cancel
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Type here to search
1:38 AM
8/28/2020

SSH Clients – Mac / Linux

- **Mac**
  - OpenSSH client (command-line)
  - *Bundled with OS*

- **Linux**
  - OpenSSH client (command-line)
  - *Bundled with OS*

https://www.openssh.com/



Command Prompt on my Mac:

`hostname: current-dir username$`

Downloads — ubuntu@ip-172-31-52-244: ~ — -bash — 93×36

```
Jeff-MBP-2017:Downloads shafer$ ssh cyberlab.pacific.edu -l ubuntu -i kp-cyberlab.pem
```

Connect to remote server:

```
ssh <hostname> -l <username> -i <private key>
```

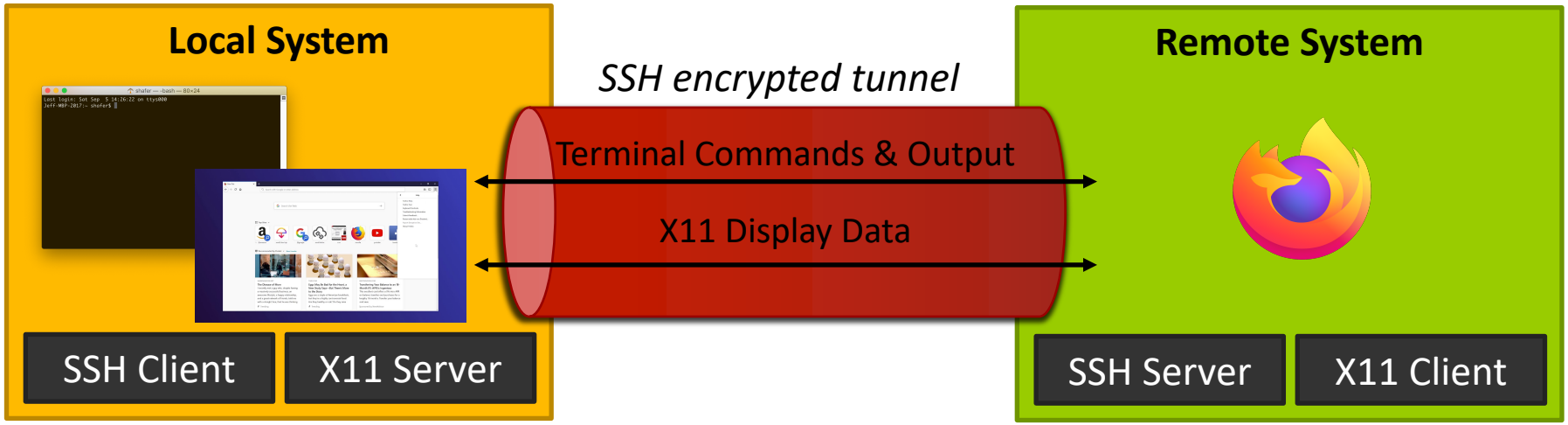
Downloads — ubuntu@ip-172-31-52-244: ~ — ssh cyberlab.pacific.edu -l ubuntu -i kp-cyberlab...

```
Jeff-MBP-2017:Downloads shafer$ ssh cyberlab.pacific.edu -l ubuntu -i kp-cyberlab.pem
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.3.0-1030-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Sep  5 21:27:39 UTC 2020

  System load:  0.0                Processes:           106
  Usage of /:   25.6% of 29.02GB   Users logged in:     0
  Memory usage: 73%                IP address for ens5: 172.31.52.244
  Swap usage:   0%

 * Kubernetes 1.19 is out! Get it in one command with:

     sudo snap install microk8s --channel=1.19 --classic

   https://microk8s.io/ has docs and details.

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.


*** System restart required ***
Last login: Sat Sep  5 21:27:04 2020 from 108.207.255.214
ubuntu@ip-172-31-52-244:~$
```

Welcome message from remote server

Command Prompt on Remote Server:
`username@hostname:current-dir$`

X11 Forwarding




```
local$ ssh -X user@remote
remote$ firefox &
```

X11 Forwarding
The *application* runs on the remote system, but the display data is sent to the local system

Secure Copy (scp)

Single File:
Copy `file.txt` from the current directory **to** the remote server `host.com` (login in as `user`), and save it in `/remote/dir/`:

```
$ scp file.txt user@host.com:/remote/dir/
```

Directory:
Copy the contents of `/local/dir` **to** the remote server `hostname.com` (login in as `user`), and save it in `/remote/dir/`:

```
$ scp -r /local/dir user@host.com:/remote/dir/
```

Secure Copy (scp)

Single File:
Copy `/remote/dir/file.txt` **from** the remote server `host.com` (login in as `user`), and save it in `/local/dir/`:

```
$ scp user@host.com:/remote/dir/file.txt /local/dir
```

Directory:
Copy the contents of `/remote/dir` **from** the remote server `host.com` (login in as `user`), and save it in `/local/dir/`:

```
$ scp -r user@host.com:/remote/dir/ /local/dir/
```

Lab 1 – AWS Virtual Machine Quick-Start

- Today's Goals
  - Deploy a virtual machine
    - Use Amazon Web Services (AWS) Elastic Compute Cloud (EC2) to obtain an instance on demand
  - Connect to it via Secure Shell (SSH)
  - Run a few basic commands at the terminal
  - Document your work w/screenshots
  - Shutdown the virtual machine
- Opportunity to become familiar with tools and resolve any technical difficulties

Wrap-Up

- Questions?
- Concerns?

- **Today**
  1. **Lab 1** - Configure and Launch a basic Linux Virtual Machine at AWS
- **Next Week**
  - **Lab 2** – VPC, Security Groups, and More VMs
  - **Lab 3** – Billing