Connecting to an AWS Instance

1) From the dashboard, select “EC2” to open the EC2 dashboard and select your instance.

2) In the “description” pane, below, copy either the Public DNS or “Public IP”.
   a) These addresses may change upon a power cycle, so we’d encourage the user of an Elastic IP, which is a static IP that may be reassigned to instances. On first setup, your server does not yet have a static (elastic) IP.
      i) If you have an elastic IP, the IP will be highlighted in blue.
      ii) You may also verify this by selecting **“Elastic IP’s”** to view existing IP’s.

3) In your putty or SSH console, connect to the Public DNS from step 1 using the PEM file you downloaded when you first set it up:
   a) **$ssh -i "path/to/your/key_file.pem" username@your-public-address**
      i) The default user is likely your OS name (ie. “ubuntu”). The “root” user will also work but will request you to switch to the default user.
      ii) The default user is a sudoer, so you’ll use “sudo” for most of these commands or you may switch user to root with **“su -”**
   b) We suggest storing this key on your local putty or console key repository (ie. your /.ssh keys or Putty Pageant).
      i) To do so, you may need to convert your PEM to PPK format. We suggest using PuttyGen.
      ii) To add your key to your repository, follow the software’s instructions. You can find a running pageant session in your system tray. Just right-click and select **“Add Key”** to import your key. If you have added a password to the key file, you’ll be prompted upon service initiation.
      iii) This will allow you to connect without explicitly identifying the key file **(ie. $ssh username@your-public-address)**
   c) If you have an additional key (ie. external user) that you would like to permit server access, without disclosing your PEM file, find the server’s key file and add it to the end: **~./ssh/authorized_keys**

4) To enable an elastic IP, select **“Elastic IP”** and click the **“Allocate New Address”** button.
   a) When prompted, select **“Yes, Allocate”** and **“Close”**
   b) Now select your newly created Elastic IP. You should see that it has no public DNS nor instance, identified, otherwise it is assigned elsewhere.
   c) Click **“Actions” > “Associate Address”**
   d) Select the **“Instance”** field to drop-down your instance list. Then select it or type-search the one you want. If you aren’t using tags/names, we advise you to; it will make this step easier.
   e) Once selected, click **“associate”**. If your IP is already assigned elsewhere, you’ll need to select **“reassociate”**. Then you’re done!

support@arcanestrategies.com
(541) 649-2508

Arcane Strategies
7 E. Congress St. #804
Savannah, GA 31401

1) To enable SFTP password authentication login, perform the following:
    a) **$sudo vi /etc/ssh/sshd_config**
    b) You may use vim or nano if you choose. To insert with vi, select “i”. To close and save, select “ctrl+[“ and “:wq” // if you have a conflict “:wq!” will force it through.
    c) Find “PasswordAuthentication” and change “no” to “yes”.

2) You should now be connected.
    a) If you are unable to connect, it could be due to firewall restrictions.
        i) To test this, try a “telnet” test against the SSH port (default is 22)
        ii) Check your EC2 security group to be sure that standard protocols (SSH, MySQL, HTTP) are opened to your local IP address/range.
        iii) The server also has its own firewall, IPTables, or UFW tables, which may require editing. Since you can’t access the server, try this pro tip:
            1) **Pro Tip:** If locked out due to firewall rules, you may edit them by mounting your root volume as a secondary volume on an available instance.
                a) Shut down your instance
                b) Detach the root (sda1) volume
                c) Attach the volume from step (b) to a new server that you have access to. Note the device name (ie. xvdf)
                d) Make a temp directory and mount the volume as a secondary partition.
                    i) **$sudo mount /dev/[device name] /[directory]**
                e) Now you can access the root filesystem including the firewall table files. Clean these up (enable SSH access)
                f) Now unmount and detach the volume (reverse step d)
                g) Reattach the volume as the primary drive/partition for your instance from step (a). Now you are safe to restart your instance and test access!