Preparation for the Hands on Labs

Creating an SSH Keypair

OSX / Linux: Create a keypair

```
aws ec2 create-key-pair --key-name aws-nick --query 'KeyMaterial' \
  --output text > ~/.ssh/aws-nick.pem
```

- Use any --key-name you want, I like to prefix mine with aws- and match the IAM user
- Feel free to save the key into a different location if you do not want it in your ~/.ssh directory

OSX / Linux: Set the proper permissions on the keypair

```
chmod 400 ~/.ssh/aws-nick.pem
```

Windows: Download PowerShell

https://www.microsoft.com/en-us/download/details.aspx?id=42554

Windows PowerShell: Create a keypair

```
aws ec2 create-key-pair --key-name aws-nick --query 'KeyMaterial' ^
  --output text | out-file -encoding ascii -filepath aws-nick.pem
```

- We need to set the encoding type to ASCII because UTF-8 fails on some SSH clients

Windows: Planning to use Putty to SSH into your container instance?

- Install the full Putty suite
- Start PuTTYgen
- Under Type of key to generate, choose SSH-2 RSA
- Choose load and ensure "All Files" is selected from the file type drop down
- Select the PEM file you created before and choose open
- Choose ok to close the dialog box
- Choose save private key and ignore the warning about a passphrase
- Specify the same name for the key that you created before

Verify the keypair has been created

```
aws ec2 describe-key-pairs --key-name aws-nick
```

(Optionally) Delete the keypair

```
aws ec2 delete-key-pair --key-name aws-nick
```

- Do not delete the keypair now unless you're experimenting on your own
- You should also delete the aws-nick.pem file locally if you decide to delete the keypair