RE:INFORCE

aws RE:INFORCE

FND316

Secure your Amazon SageMaker Jupyter Notebooks and Training Jobs

Vikrant Kahlir
AWS Solution Architect
Amazon Web Services

Agenda

What is Machine Learning?

How Amazon SageMaker fits into AWS AI/ML Stack?

How to secure Amazon SageMaker Pre-built Jupyter Notebook Instances?

How to secure Amazon SageMaker Training jobs?

What is Machine Learning?

Try to read the text below

“it deson’t mttaer in waht oredr the ltteers in a wrod aepapr, the olny iprmoatnt tihng is taht the frist and lsat ltteer are in the rghit pcale. The rset can be a toatl mses and you can sitll raed it wouthit pobelrm.

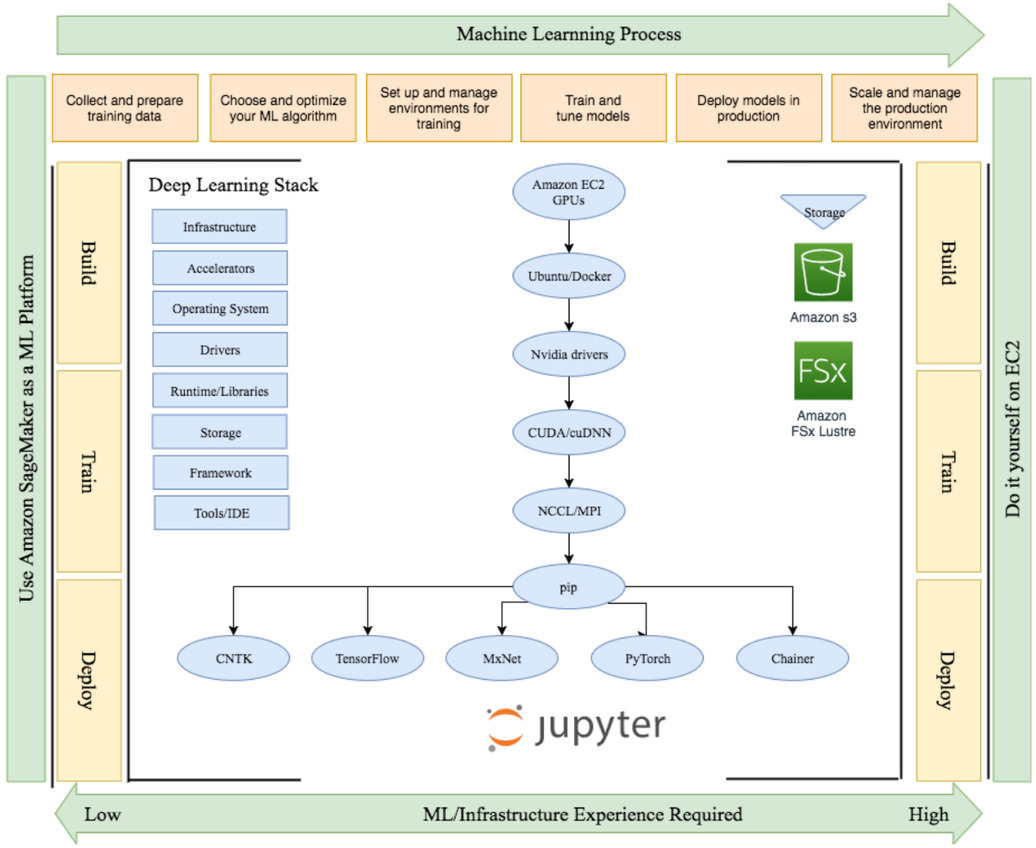
Machine learning empowers

system to recognize patterns that are generalized and not get caught up in specific details. This empowers systems to do things that are closer to the human cognition.

ML Process and ML Stack Overview

- Machine Learning model is a recipe that takes long time to cook, requires a lot of ingredients, a large container and a large storage.
- Machine Learning process is complex and the stack that it uses has many layers.

Think of Amazon SageMaker as Master Chef who knows how to simplify ML Process and can cook complex Machine Learning models and has access to latest and greatest Amazon EC2 compute instances, Deep Learning Docker containers and Amazon S3 for large storage.



Security of Amazon SageMaker Build and Train Infrastructure

Amazon SageMaker Jupyter Notebook

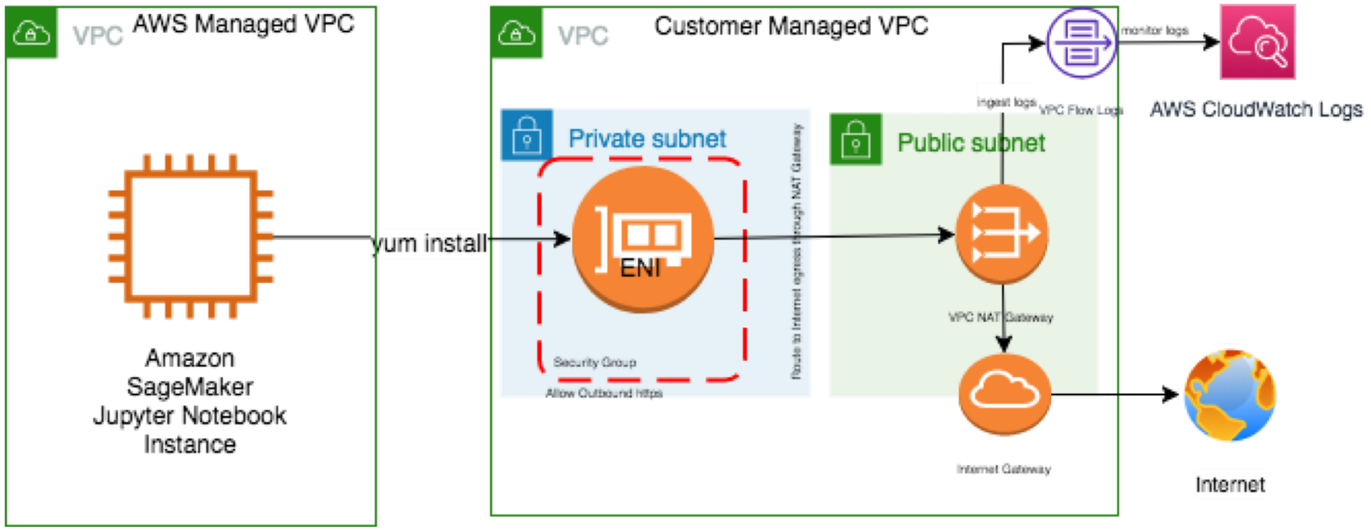
- Connect it to your VPC
- Apply Security Groups
- Disable Internet Access
- Disable Root Access
- Encrypt your EBS volume
- Use NAT Gateway for downloads
- Use AWS Backbone for secure access to data in Amazon S3

Amazon SageMaker Train

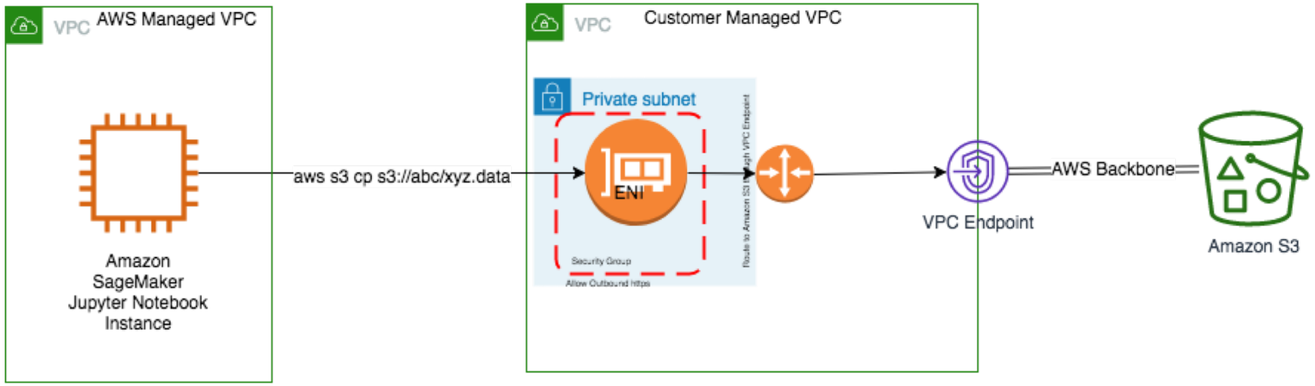
- Connect it to your VPC
- Apply Security Groups
- Encrypt connection between Instances

Security of Build Infrastructure

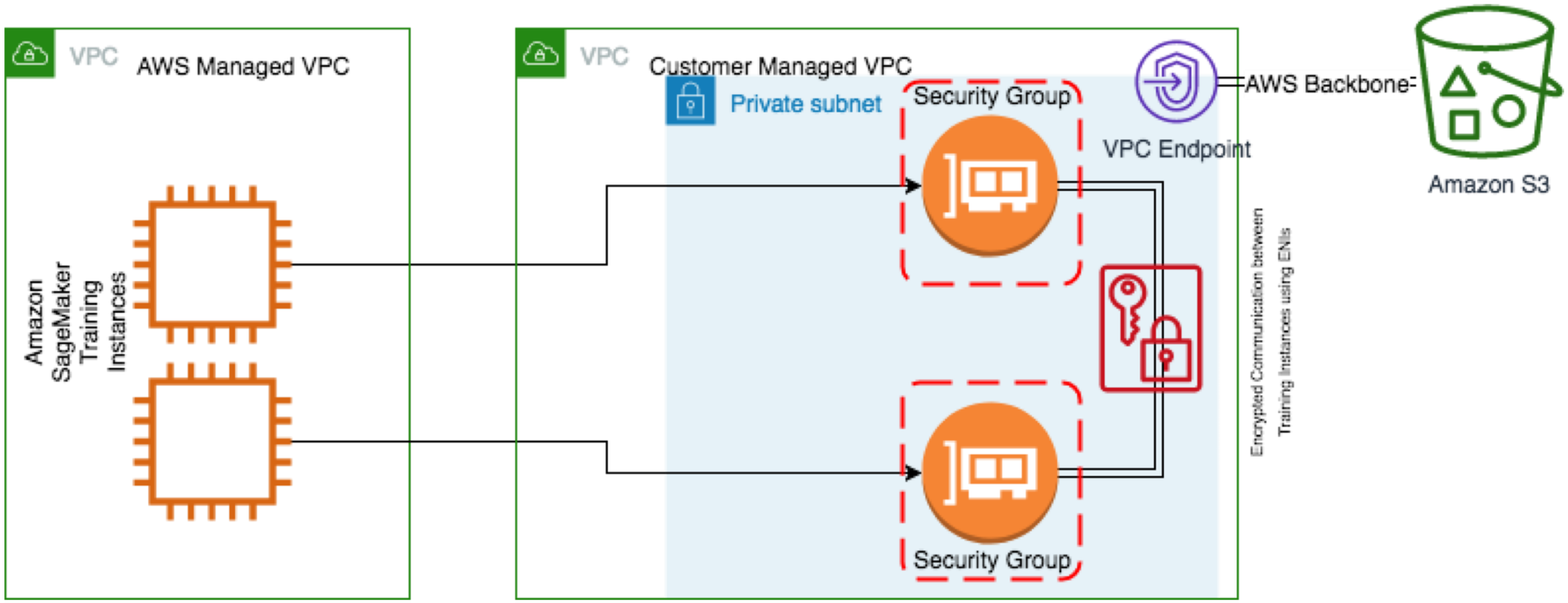
- Access to Internet



- Access to Amazon S3



Security of Train Infrastructure



Complete the workshop

http://bit.ly/2MTvXvv

Thank you!

Vikrant Kahlir
awsvik@amazon.com

aws RE:INFORCE

Please complete the session survey in the mobile app.

aws RE:INFORCE