Deep Learning on AWS

Guide

August 2019

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents AWS current product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. AWS responsibilities and liabilities to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

About this Guide

Today, deep learning is at the forefront of most machine learning implementations across a broad set of business verticals. Driven by the highly flexible nature of neural networks, the boundary of what is possible has been pushed to a point where neural networks outperform humans in a variety of tasks, such as classifying objects in images or mastering video games in a matter of hours. This guide outlines the end-to-end deep learning process implemented on Amazon Web Services (AWS). We discuss challenges in executing deep learning projects, highlight the latest and greatest technology and infrastructure offered by AWS, and provide architectural guidance and best practices along the way.

This paper is intended for deep learning research scientists, deep learning engineers, data scientists, data engineers, technical product managers, and engineering leaders.

Overview

The basic idea of deep learning has been around for decades. However, due to a recent surge in the digitization of information, organizations have amassed large amounts of data that are easily consumable by machine learning pipelines.

Even more, our generation is spending more time on mobile phones and computers connected on social media and that has led to more data. Even in medicine, an x-ray image is stored as a digital record instead of a physical film.

On one hand, the amount of data has exploded, but the performance of traditional machine learning algorithms such as logistic regression, decision trees, support vector machines, and others have plateaued even when fed with more data.

In a turn of events, the small neural network has improved in accuracy of application; the medium neural network has improved in accuracy of application; and the deep neural network continues to improve in accuracy when fed with more data. We have yet to reach the limits of accuracy we can get by introducing more layers and more data in a deep neural network.

Adding more layers to a neural network and providing more data helped improve the accuracy of deep learning applications. However, training the deep neural network was a hurdle because training requires access to powerful and often expensive compute infrastructure. Cloud computing solved this problem by offering on-demand GPUs in a cost effective and elastic manner, enabling large scale experimentation required to achieve the desired level of model accuracy.

Although there are other tools under the broader umbrella of machine learning, such as probabilistic graph models, planning algorithms, search algorithms, and knowledge graphs, which are steadily improving, deep learning has improved exponentially and continues to break new ground.

In this guide, we discuss the unique value proposition that Amazon Web Services (AWS) offers to support deep learning projects. You can leverage AWS innovation in the deep learning domain to improve the training time of deep learning jobs by using AWS optimized compute, storage, and network infrastructure. Deep learning jobs become more productive and agile from using AWS services and by offloading the undifferentiated heavy lifting involved in managing deep learning infrastructure and platform on AWS. AWS offers the deepest and broadest set of capabilities and flexibility that is required for the explorative nature of deep learning projects.

Throughout this guide, we use *deep learning engineers* and *deep learning scientists* to refer to users of AWS services for deep learning. Deep learning engineers and deep learning scientists implies a broader team working on a deep learning project with different titles.

Deep Learning Landscape

The following figure is a visual boundary of the deep learning landscape that we cover in this guide. See the following table for detailed descriptions of various parts of the diagram.

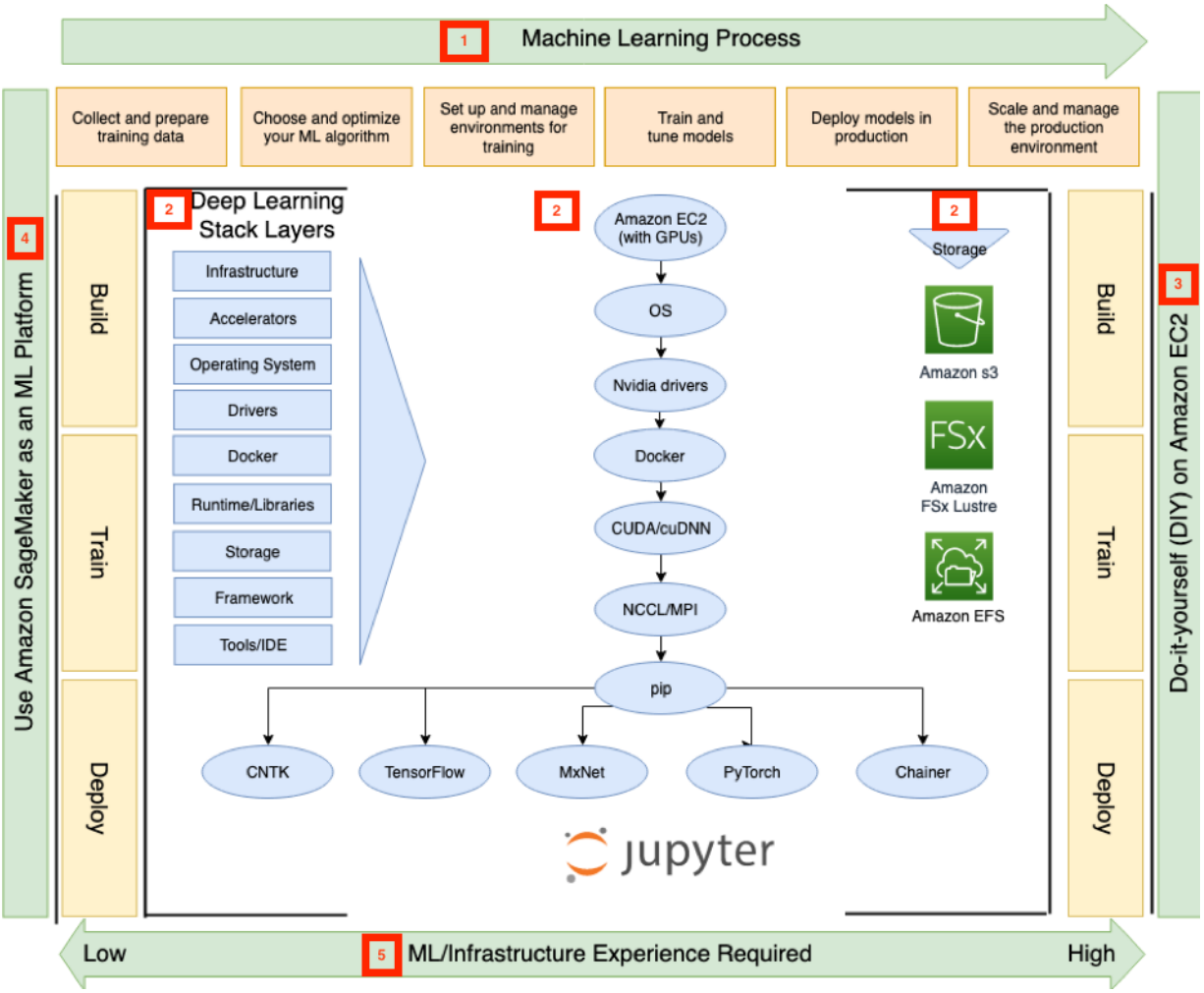

Figure 1: Deep learning landscape

Table 1: Deep learning landscape diagram descriptions

Label	Description
1	Six steps required to execute deep learning projects. The six steps involved are discussed in Deep Learning Process for Build, Train, and Deploy.
2	The different layers required to support a deep learning environment for build, train, and deploy tasks. The layers in the figure extend from infrastructure to tools required for deep learning projects.
3	The do-it-yourself (DIY) option where the customer is responsible for building and managing components and features required for deep learning using AWS compute, storage, and network technology building blocks.
4	Amazon SageMaker is a fully-managed service that covers the entire deep learning workflow to label and prepare your data, choose an algorithm, train the model, tune and optimize it for deployment, make predictions, and take action. Your models get to production faster with much less effort and lower cost.
5	A measure of infrastructure experience required to set up the deep learning environment in the context of ease-of-use and the shared responsibility model between customer and AWS. Fully managed is easy to use because AWS manages the major part of the stack. The do-it-yourself (DIY) option is more challenging because customers manage most of the stack

Note: Between the fully managed (4) and do-it-yourself (DIY) (3) options, there is a partially managed approach where you use a fully managed container service and a self-managed deep learning workflow service like Kubeflow. This partially managed approach is relevant for organizations that have decided to standardize their infrastructure on top of Kubernetes. For more details, see DIY Partially Managed Solution: Use Kubernetes with Kubeflow on AWS.

Using this Guide

This guide is organized into seven sections, as described below.

1. Deep Learning Process for Build, Train, and Deploy
2. Challenges with Deep Learning Projects
3. Highly Optimized AWS Technology Building Blocks for Deep Learning
4. Code, Data, and Model Versioning
5. Automation of Deep Learning Process for Retrain and Redeploy

6. Patterns for Deep Learning at Scale
7. AWS Guidance

If you are not familiar with the deep learning process and the deep learning stack, read this guide in its entirety, in sequence.

If you are familiar with AWS Deep Learning building blocks, deep learning challenges, and deep learning process, you can skip to sections 4, 5, 6, and 7.

Deep Learning Process for Build, Train, and Deploy

The following image shows the six steps of the deep learning process. In the following sections, we provide more information on each step of the deep learning process, explain challenges in terms of infrastructure performance, bottlenecks, scalability, reliability, and ease of use.

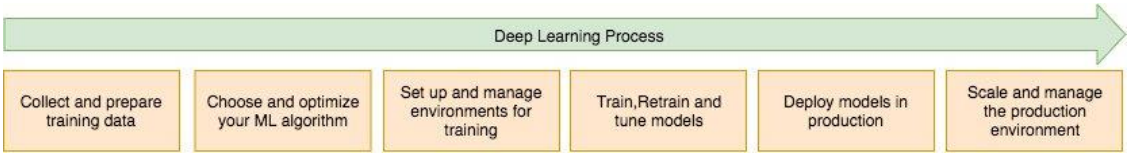

Figure 2: Six steps of deep learning process

Step 1. Collect Data

Deep learning is different from traditional machine learning with regard to data collection and preparation steps. Although feature engineering tends to be the bottleneck in traditional machine learning implementations, in deep learning (specifically in image recognition and natural language processing [NLP] use cases), features can be generated automatically by the neural network as it learns. The features are extracted by having each node layer in a deep network learn features by repeatedly attempting to reconstruct the input from which it draws its samples, allowing it to minimize the delta between the network's guesses and the probability distribution of the input data itself. However, when training from scratch, large amounts of training data are still necessary to develop a well-performing model, and this necessitates substantial amounts of labeled data. There may not be enough labeled data available upfront especially when dealing with new applications or new use cases for a deep learning implementation.

We will discuss ways to mitigate these unique challenges to deep learning in the Highly Optimized AWS Technology Building Blocks for Deep Learning section of this paper. As a first step, use the diagram below to assess your data collection process.

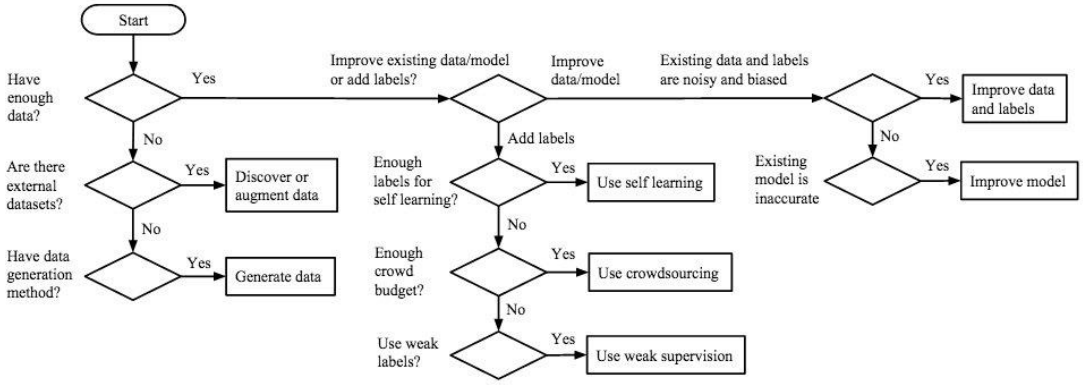

Figure 3: Data collection assessment[1]

Data Preprocessing

Data preprocessing comprises data cleaning, data integration, data transformation, and data reduction, with the intent to mitigate inaccurate, missing, noisy, and inconsistent data before starting the training process. AWS provides a variety of tools and services that you can use to perform the data preprocessing steps in addition to performing feature engineering: AWS Glue, Amazon EMR, AWS Lambda, Amazon SageMaker, AWS Batch, and AWS Marketplace. The use of these tools is described in detail in the Big Data Analytics Options on AWS whitepaper.

Most important, with the widespread availability of many open source deep learning frameworks, a broad variety of file formats have emerged to accommodate the individual frameworks. The choice of file format for your data ingestion process is an important step in the data preprocessing phase and greatly depends on the framework chosen to perform the deep learning implementation. Some of the standard formats include RecordIO, TFRecords, Hierarchical Data Format (HDF5), pth, N5, and light memory mapped database (LMDB).

Step 2. Choose and Optimize Your Algorithm

Within deep learning implementations, we differentiate between various network architectures and deep learning algorithms. Discussing every available network architecture and learning algorithm is outside the scope of this paper. For brevity, we briefly discuss three of the most commonly used network architectures and some popular learning algorithms used today.

Deep Learning Network Architecture

- Multilayer Perceptrons (MLPs) (Feedforward neural networks [FFNNs])
- Convolutional Neural Networks (CNNs)
- Recurrent Neural Networks (RNNs)

At a high level, we chose a network architecture based on the specific use case that we are trying to solve. The following table is a decision matrix mapping use cases to the individual network architectures.

Table 2: Mapping use cases to network architectures

MLPs (FFNNs)	CNNs	RNNs (LSTM)
Tabular Datasets	Image Data	Text Data
Classification Prediction Problems	Classification Prediction Problems	Speech Data
Regression Prediction Problems	Regression Prediction Problems	Classification Prediction Problems
		Regression Prediction Problems

Deep Learning Algorithms

Most deep learning models use gradient descent and backpropagation to optimize the neural network's parameters by taking partial derivatives of each parameter's contribution to the total change in error during the training process. Exploring optimization techniques concerning the training performance of deep learning algorithms is a topic of ongoing research and still evolving. Many new variants of the conventional gradient descent-based optimization algorithms such as momentum, AdaGrad (adaptive gradient algorithm), Adam (adaptive moment estimation), and Gadam (genetic-evolutionary Adam) have emerged to improve the learning performance of your deep learning network.

Step 3. Set up and Manage the Environment for Training

Designing and managing the deep learning environments for your training jobs can be challenging. Deep learning training jobs are different from traditional machine learning

implementations. Challenges arise based on the complexity of most neural networks, the high dimensionality of the dataset, and lastly the scale of the infrastructure needed to train large models with a lot of training data. To accommodate these challenges, you need elasticity and performance in your compute and storage infrastructure.

On AWS, you can choose to build your neural net from the ground up with the AWS Deep Learning Amazon Machine Image (AWS DL AMI) which comes preconfigured with TensorFlow, PyTorch, Apache MXNet, Chainer, Microsoft Cognitive Toolkit, Gluon, Horovod, and Keras, enabling you to quickly deploy and run any of these frameworks and tools at scale. Additionally, you can choose to use the preconfigured AWS Deep Learning Containers (AWS DL Containers) preinstalled with deep learning frameworks supporting TensorFlow and Apache MXNet and run them on Amazon Elastic Kubernetes Service (Amazon EKS), self-managed Kubernetes, Amazon Elastic Container Service (Amazon ECS), or directly on Amazon Elastic Compute Cloud (Amazon EC2). Lastly, you can take advantage of the AWS SDK for Python. This SDK provides open source APIs and containers to train and deploy models in Amazon SageMaker with several different machine learning and deep learning frameworks. We will discuss the most common solutions and patterns using these services in the second half of this paper.

Step 4. Train, Retrain, and Tune the Models

Training neural networks is different from traditional machine learning implementations because the model needs to learn the mapping function from the inputs to the outputs via function approximation in a nonconvex error space with many “good” solutions. Since we can’t directly compute the optimal set of weights via a closed form solution (as is the case with simple linear regression models), and we cannot get global convergence guarantees, training a neural network can be challenging and usually requires much more data and compute resources than other machine learning algorithms.

AWS provides a variety of tools and services to simplify the training process of your neural networks. Throughout this paper, we will discuss a variety of options that includes running your self-managed deep learning environment on Amazon EC2; running a deep learning environment on Amazon EKS or Amazon ECS; or using fully managed service Amazon SageMaker for deep learning. All these environment uses highly customized GPU powered hardware to reduce training time and training cost.

In addition to the model design discussed in Step 2. Choose and Optimize Your Algorithm, you also have the option of setting hyperparameters before starting the

training process. Searching for the optimal hyperparameters is an iterative process, and because of the high dimensionality and complexity of the search space in deep learning implementations, this endeavor can be labor and cost intensive. A variety of strategies have been developed to find the optimal hyperparameter settings via techniques such as grid search, random search, and Bayesian optimization.

Hyperparameter tuning is available as a turn key feature in Amazon SageMaker.

Step 5. Deploy Models in Production

Deploying a machine learning model into production often poses the most challenging part of an end-to-end machine learning pipeline. That is because deploying machine learning workloads differ from traditional software deployments.

First, we must consider the type of inference that the model provides: *batch inference* (offline) versus *real-time inference* (online). As the name implies, batch inference generates predictions asynchronously on a batch of observations. The batch jobs are generated on a recurring schedule (e.g., hourly, daily, weekly). These predictions are then stored in a data repository or a flat file and made available to end users. Real-time inference is the process of generating predictions in real time and synchronous upon request, most often on a single observation of data at runtime.

Second, we must consider how the model is retrained. For a model to predict accurately, the data that is provided to the model to make predictions on must have a distribution similar to the data on which the model was trained. However, in most machine learning deployments, data distributions are expected to drift over time, and because of that, deploying a model is not a one-time exercise but rather a continuous process. It is a good practice to monitor the incoming data continuously and retrain your model on newer data if you find that the data distribution has deviated significantly from the original training data distribution. Based on your use case, an automatic instead of an on-demand approach to retrain your model may be more appropriate. For example, if monitoring data to detect a change in the data distribution has a high overhead, then a simpler strategy such as training the model periodically may be more appropriate.

Third, implementing model version control and having a scaling infrastructure to meet demand is not specific to deep learning, but requires additional consideration. Version control is essential because it allows for traceability between the model and its training files in addition to allowing for verifiability, letting you tie the output generated by a model to a specific version of that model. Dynamically adjusting the amount of compute capacity for an inference endpoint in addition to having the capability to add fractions of

a GPU core to an inference endpoint allows you to meet the demands of your application without overprovisioning capacity.

Fourth, implementing tools to audit the performance of a model over time is the last step in implementing a model into production. The auditing solution must be able to accurately observe an objective evaluation metric over time, detect failure, and have a feedback loop in place should the model's accuracy deteriorate over time. Note that we do not cover auditing solutions in this guide.

Lastly, we will discuss the different model deployment and model and data version control approaches available to you on AWS in more detail in the next two sections – Code, Data and Model Versioning and Patterns for Deep Learning at Scale.

Step 6. Scale and Manage the Production Environment

Building and deploying effective machine learning systems is an iterative process, and the speed at which changes can be made to the system directly affects how your architecture scales, while also influencing the productivity of your team. Three of the most important considerations to achieve scale and manageability in your deep learning implementations are modularity, tiered offerings, and choosing from a multitude of frameworks. This decoupled and framework agnostic approach will provide your deep learning engineers and scientists with the tools that they want, while also catering to specific use cases and skillsets in your organization.

AWS provides a broad portfolio of services that cover all the common machine learning (ML) workflows while also providing you the flexibility to support the less common and custom use cases. Before discussing the breadth and depth of the AWS machine learning stack, let us look at the most common challenges encountered by machine learning practitioners today.

Challenges with Deep Learning Projects

Software Management

Deep learning projects are dependent on machine learning frameworks. Many deep learning frameworks are open source and supported by the community that is actively contributing to the framework code. The changes are frequent and sometimes breaking. In some cases, you need to customize the framework to meet your immediate needs for performance by writing custom operators.

Building, testing, and maintaining machine learning frameworks requires work. If the changes are breaking, you must make changes to your script as well. However, it is important to take advantage of the latest from the open source AI community and to support requirements of internal projects.

Performance Optimization

The full stack of deep learning has many layers. In order to extract maximum performance out of the stack, you must fine-tune every single layer of software that includes drivers, libraries, and dependencies. Poorly tuned layers in the software can increase the training time of the model and can lead to increased cost of training. Tuning the deep learning stack requires multiple iterations of testing and specialized skills. Most often tuning is required for both training and inference stacks. Different stacks may have different bottlenecks—network, CPU, or storage I/O—that must be resolved with tuning.

Collaborative Development

In most cases, it's a team of deep learning engineers and deep learning scientists that would collaborate on a deep learning project. The team must conform to certain standards to collaborate and provide feedback on each other's work. As the project moves from proof of concept to production, it is important to track that the model's performance over time for consistency. Consistency is required between the dataset and hardware versions and software configuration of different stacks used during the training by different practitioners. Consistency is also required between the training and the inference stack. The stack and the results from the stack should be reproducible.

Infrastructure Management

In order to prove the value of the model, it should be trained with the appropriate hyperparameters and on a large dataset. The search for the most optimal hyperparameters requires multiple jobs to be run concurrently on a large dataset. This exercise requires working with job schedulers, orchestrators, and monitoring tools, which creates dependency on IT assets managed by centralized IT teams. Even after the first version of the model is fully developed, the DevOps team must support the infrastructure required to retrain the model on fresh data, and to monitor and support the endpoint used to deploy the model.

Scalability

Both deep learning training and inference workloads have spiky characteristics. There may be a specific time period during the project where you may have to scale specific experiments to hundreds and thousands of instances. This is true for inference and when seasonal spike in inference is expected during special events during the year. Planning and forecasting the high-performance compute required to support experiments and seasonal bursts for training and inference is difficult to plan.

AWS services optimized for deep learning solves above challenges faced by deep learning engineers and deep learning scientists. Let us take a closer look at the individual buildings blocks.

Highly Optimized AWS Technology Building Blocks for Deep Learning

The following figure outlines the composition of the individual deep learning layers on AWS.

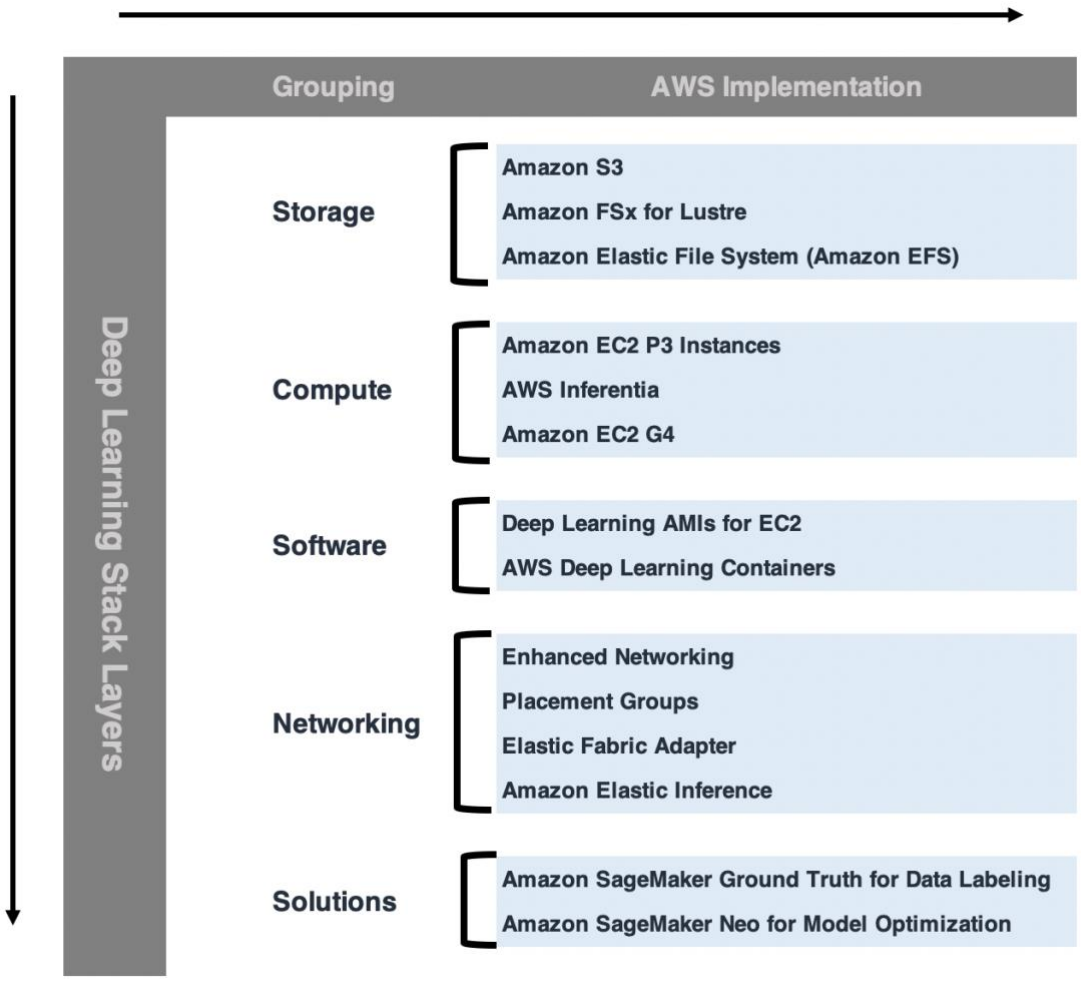

Figure 4: Building blocks for deep learning

Storage

Amazon Simple Storage Service (Amazon S3)

Data acquisition and making that data available for exploration and consumption across the enterprise for different deep learning projects is an important strategic initiative. It

involves tasks such as ingesting the data, performing extract, transform, load (ETL), visualizing data, and wrangling data to develop high-quality training dataset for training deep learning models.

Amazon Simple Storage Service (Amazon S3) can be used as central storage layer to store and democratize data for deep learning. Your applications can easily achieve thousands of transactions per second by using Amazon S3 as the storage tier for deep learning training jobs. Amazon S3 automatically scales to high request rates.

Make sure to consider the throughput between Amazon EC2 and Amazon S3 during ingestion and reading of objects from Amazon S3. You can achieve higher performance using multiple Amazon EC2 instances in a distributed manner.

Amazon SageMaker uses Amazon S3 as a storage tier for data used in training jobs and batch inference, and for storing trained models. Amazon SageMaker supports both batch and pipe mode to read data from Amazon S3 in the local Amazon Elastic Block Store (Amazon EBS) volume of Amazon SageMaker training instances.

DIY customers who want to manage their own compute clusters on Amazon EC2 can use Amazon S3 as the storage layer or they can use Amazon FSx for Lustre hydrated from Amazon S3 with lazy loading to build a data caching layer for deep learning jobs. Both of the options are available for a DIY setup. You must make a tradeoff between price and performance.

Amazon FSx for Lustre

Amazon FSx for Lustre is built on open-source Lustre. Lustre is an open-source highly scalable, highly distributed, and highly parallel file system that can be used as a deep learning data caching layer for distributed training.

The high-performance capabilities and open licensing make Lustre a popular choice for deep learning workloads. Lustre file systems are scalable and can be used with multiple compute clusters with tens of thousands of client notes, PBs of data, and TB per second of aggregate I/O throughput.

If you are training a deep neural network, Lustre provides you with the capability to get the source data fast with low latency. But, setting up a Lustre cluster can be challenging.

Amazon FSx for Lustre simplifies the complexity of setting up and managing the Lustre File System and provides an experience that allows you to create a file system in minutes, mount it on any number of clients, and start accessing it right away. Amazon

FSx for Lustre is a fully managed service, so there's nothing to maintain and nothing to administer. You can build standalone file systems for ephemeral use, or you can seamlessly join them to an S3 bucket and then access the contents of the bucket as if it were a Lustre file system. Amazon FSx for Lustre is designed for workloads that require high levels of throughput, IOPS, and consistent low-latencies.

One unique feature of Amazon FSx for Lustre is its deep integration with Amazon S3 that allows lazy loading of data into the actual file system. If a customer doesn't know which object to load from the S3 bucket, the Amazon FSx for Lustre loads only the metadata comprised of names, dates, sizes, and so forth for the objects themselves, but it does not load the actual file data until it is required. By default, Amazon S3 objects are only loaded into the file system when first accessed by your applications. If your applications access objects that haven't yet been loaded into your file system, Amazon FSx for Lustre automatically loads the corresponding objects from Amazon S3.

Amazon Elastic File System (Amazon EFS)

When selecting a storage solution, there is a tradeoff between data locality and a centrally managed storage solution. Amazon EFS is well-suited to support a broad spectrum of use cases—from highly parallelized, scale-out workloads that require the highest possible throughput to single-threaded, latency-sensitive workloads. However, when running batch processing on central locations, Amazon EFS is likely the most suitable storage solution. Amazon EFS enables you to provide easy access to your large machine learning datasets or shared code, right from your notebook environment, without the need to provision storage or worry about managing the network file system yourself.

Amazon EFS scales automatically as more data is ingested. Data is stored redundantly across multiple Availability Zones and the performance scales up to 10+ GB per second of throughput as your data grows. Amazon EFS can be simultaneously mounted on thousands of Amazon EC2 instances from multiple Availability Zones.

As shown in the diagram below, up to thousands of Amazon EC2 instances from multiple Availability Zones can connect concurrently to a file system. It can also be mounted on multiple Amazon SageMaker Jupyter Notebooks. This feature allows Amazon EFS to be used for data and code sharing, enabling collaboration among deep learning engineers and deep learning scientists. You can also use Amazon EFS as a caching layer for training datasets in distributed training jobs.

The following figure shows how you can add an Amazon EFS endpoint to all ephemeral compute nodes to mount a centrally accessible storage solution. Most importantly, this

endpoint can grow on-demand to petabytes without disrupting applications, growing and shrinking automatically, as you add and remove files.

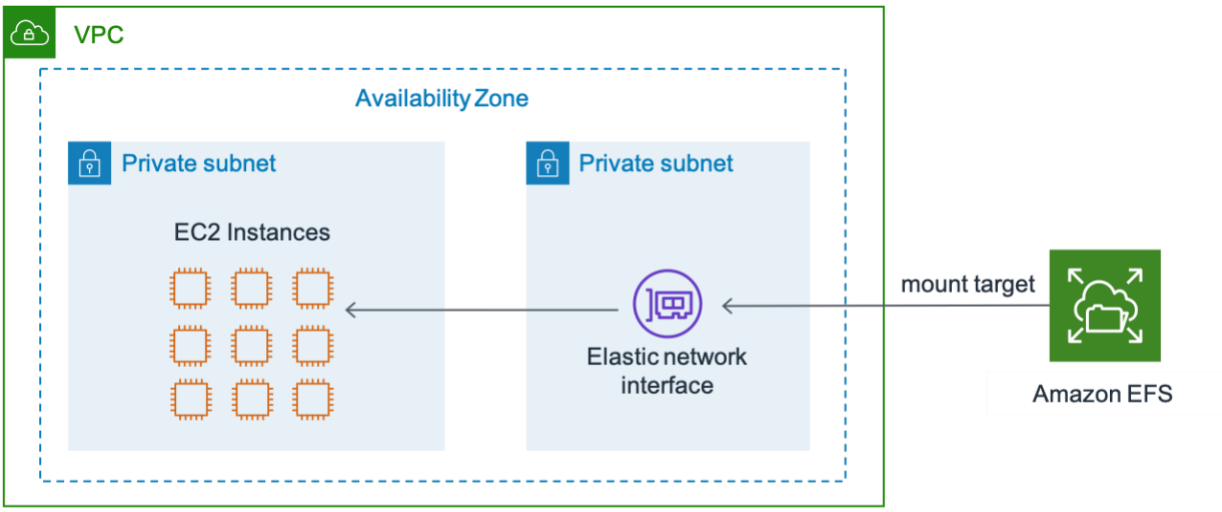

Figure 5: Multiple EC2 instances connected to a file system

Compute

Amazon EC2 P3 Instances

The computationally intensive part of the neural network is made up of many matrix and vector operations. We can make this process faster by doing all of the operations at the same time instead of doing operations one after the other. This is why GPUs, which are better at handling multiple simple calculations in parallel are used instead of CPUs for training neural networks.

Adding more layers to a neural network (up to a specific limit) and training on more and more data has been proven to improve the performance of deep learning models. GPU has thousands of simple cores and can run thousands of concurrent threads. GPUs have improved the training time required for training a complex neural network. The access and availability of high performance and cost-effective GPU infrastructure is the primary requirement for a project using neural network architecture to build complex models. The GPU-based Amazon EC2 P3 instances offer the best price/performance compared to other GPU alternatives in the cloud today.

Amazon EC2 P3 instances, the next generation of EC2 compute-optimized GPU instances, are powered by up to eight of the latest-generation NVIDIA Tesla V100 GPUs and are ideal for deep learning applications.

Amazon EC2 P3 instances provide a powerful platform for deep learning by leveraging 64 vCPUs using the custom Intel Xeon E5 processors, 488 GB of RAM, and up to 25 Gbps of aggregate network bandwidth leveraging Elastic Network Adapter (ENA) technology. We will discuss ENA is detail in the later sections.

GPUs are faster than CPUs and can saturate the network and CPUs during the training job. The size of network pipe and number of vCPUs on a training instance can become a bottleneck and may limit you from achieving higher utilization of GPUs.

Amazon EC2 P3dn.24xlarge GPU instances, the latest addition to the P3 instance family, have up to 4x the network bandwidth of P3.16xlarge instances and are purpose-built to address the aforementioned limitation.

The above enhancements to Amazon EC2 P3 instances not only optimize performance on a single instance but also reduce the time to train deep learning models. This is accomplished by scaling out the individual jobs across several instances that leverage up to 100 Gbps of network throughput between training instances.

AWS is the first cloud provider to deliver 100 Gbps of networking throughput, which helps remove data transfer bottlenecks and optimizes the utilization of GPUs to provide maximum instance performance. The doubling of GPU memory from 16 GB to 32 GB per GPU provides the flexibility to train more advanced and larger machine learning models as well as process larger batches of data, such as 4k images for image classification and object detection systems.

For a comparison of P3 instance configurations and pricing information, see Amazon EC2 P3 Instance Product Details.

AWS Inferentia

Making predictions using a trained machine learning model–a process called inference–can drive as much as 90% of the compute costs of the application. Inference is where the value of ML is delivered. This is where speech is recognized, text is translated, object recognition in video occurs, manufacturing defects are found, and cars are driven.

Amazon Elastic Inference solves these problems by allowing you to attach just the right amount of GPU-powered inference acceleration to any Amazon EC2 or Amazon SageMaker instance type with no code changes. With Amazon Elastic Inference, you can now choose the instance type that is best suited to the overall CPU and memory needs of your application, and then separately configure the amount of inference

acceleration that you need to use resources efficiently and to reduce the cost of running inference.

However, some inference workloads require an entire GPU or have low latency requirements. Solving this challenge at low cost requires a specialized and a dedicated inference chip.

AWS Inferentia is a machine learning inference chip designed to deliver high performance at low cost. AWS Inferentia hardware and software meet wide spectrum of inference use cases and state of art neural networks.

AWS Inferentia supports the TensorFlow, Apache MXNet, and PyTorch deep learning frameworks, as well as models that use the ONNX format.

Each AWS Inferentia chip provides hundreds of TOPS (tera operations per second) of inference throughput to allow complex models to make fast predictions. For even more performance, multiple AWS Inferentia chips can be used together to drive thousands of TOPS of throughput. AWS Inferentia will be available for use with Amazon SageMaker, Amazon EC2, and Amazon Elastic Inference. To be notified about AWS Inferentia availability, you can sign up here

Amazon EC2 G4

We are advancing into an age where every customer interaction will be powered by AI in the backend. To meet and exceed your customer demands, you need a compute platform that allows you to cost effectively scale your AI-based products and services.

The NVIDIA® Tesla® T4 GPU is the world's most advanced inference accelerator. Powered by NVIDIA Turing™ Tensor Cores, T4 brings revolutionary multi-precision inference performance to accelerate the diverse applications of modern AI. T4 is optimized for scale-out servers and is purpose-built to deliver state-of-the-art inference in real time.

Responsiveness is key to user engagement for services such as conversational AI, recommender systems, and visual search. As models increase in accuracy and complexity, delivering the right answer right now requires exponentially larger compute capability. Tesla T4 delivers up to 40X times better low-latency throughput, so more requests can be served in real time.

The new Amazon EC2 G4 instances packages T4-based GPUs to provide AWS customers with a versatile platform to cost-efficiently deploy a wide range of AI services. Through AWS Marketplace, customers will be able to pair the G4 instances with NVIDIA

GPU acceleration software, including NVIDIA CUDA-X AI libraries to accelerate deep learning inference.

With new T4-based G4 instances, you can make your machine learning inference easy and cost-effective.

Amazon EC2 G4 is available in preview.

Software

AWS Deep Learning AMIs

Even for experienced machine learning practitioners, getting started with deep learning can be time consuming and cumbersome.

To expedite your development and model training, the AWS Deep Learning AMIs include the latest NVIDIA GPU-acceleration through pre-configured CUDA and cuDNN drivers, as well as the Intel Math Kernel Library (MKL), in addition to installing popular Python packages and the Anaconda Platform.

The AWS Deep Learning AMIs provide machine learning practitioners and researchers with the infrastructure and tools to accelerate deep learning in the cloud, at any scale. You can quickly launch Amazon EC2 instances pre-installed with popular deep learning frameworks and interfaces such as TensorFlow, PyTorch, Apache MXNet, Chainer, Gluon, Horovod, and Keras to train sophisticated, custom AI models, experiment with new algorithms.

Deep Learning AMIs are available in two different versions—Conda AMIs and Base AMIs.

For developers who want pre-installed pip packages of deep learning frameworks in separate virtual environments, the Conda-based AMI is available in Ubuntu, Amazon Linux, and Windows 2016 versions. The environments on the AMI operate as mutually isolated, self-contained sandboxes. The AMI also provides a visual interface that plugs into your Jupyter notebooks so you can switch in and out of environments, launch a notebook in an environment of your choice, and even reconfigure your environment—all with a single click, right from your Jupyter notebook browser.

For developers who want a clean slate to set up private deep learning engine repositories or custom builds of deep learning engines, the Base AMI is available in Ubuntu and Amazon Linux versions. The Base AMI comes pre-installed with the foundational building blocks for deep learning. The Base AMI includes NVIDIA CUDA

libraries, GPU drivers, and system libraries to speed up and scale machine learning on Amazon EC2 instances. The Base AMI comes with the CUDA 9 environment installed by default. However, you can also switch to a CUDA 8 environment using simple one-line commands.

AWS Deep Learning Containers

AWS provides a broad choice of compute to accelerate deep learning training and inference. Customers can choose to use fully managed services using Amazon SageMaker or decide to use a do-it-yourself (DIY) approach by using Deep Learning AMIs.

DIY is a popular option among researchers and applied machine learning practitioners working at the framework level.

In the last few years, using Docker containers have become popular because this approach allows deploying custom ML environments that run consistently in multiple environments. Building and testing the Docker container is difficult and error-prone. It takes days to build a Docker container due to software dependencies and version compatibility issues. Further, it requires specialized skills to optimize the Docker container image to scale and distribute machine learning jobs across a cluster of instances. The process is repeated as a new version of software or driver becomes available.

With AWS Deep Learning Containers (AWS DL Containers), AWS has extended the DIY offering for advanced ML practitioners and provided the Docker container images for deep learning that are preconfigured with frameworks such as TensorFlow and Apache MXNet. AWS takes care of the undifferentiated heavy lifting that is involved in building and optimizing Docker containers for deep learning. AWS DL Containers are tightly integrated with Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS). You can deploy AWS DL Containers on Amazon ECS and Amazon EKS in a single click and use it to scale and accelerate your machine learning jobs on multiple frameworks. Amazon ECS and Amazon EKS handle all the container orchestration required to deploy and scale the AWS DL Containers on clusters of virtual machines. Today, AWS DL Containers are available for TensorFlow and Apace MXNet.

The container images are available for both CPUs and GPUs, for Python 2.7 and 3.6, with Horovod support for distributed training on TensorFlow for Inference and Training.

AWS DL Containers are available in AWS Marketplace or from within the Amazon ECS console.

AWS DL Containers version 2.0 for TensorFlow Docker images have been tested with Amazon SageMaker, Amazon EC2, Amazon ECS, and Amazon EKS. One Docker image can be used across multiple platforms on AWS.

Networking

Enhanced Networking

Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. Most of the instance types that are used in deep learning support an Elastic Network Adapter (ENA) for enhanced networking.

The ENA was designed to work well with modern processors, such as those found on C5, M5, P3, and X1 instances. Because these processors feature a large number of virtual CPUs (128 for X1), efficient use of shared resources like the network adapter is important. While delivering high throughput and great packet per second (PPS) performance, ENA minimizes the load on the host processor in several ways and also does a better job of distributing the packet processing workload across multiple vCPUs. Here are some of the features that enable this improved performance:

- **Checksum Generation** – ENA handles IPv4 header checksum generation and TCP/UDP partial checksum generation in hardware.
- **Multi-Queue Device Interface** – ENA uses multiple transmit and receive queues to reduce internal overhead and to improve scalability. The presence of multiple queues simplifies and accelerates the process of mapping incoming and outgoing packets to a particular vCPU.
- **Receive-Side Steering** – ENA can direct incoming packets to the proper vCPU for processing. This technique reduces bottlenecks and increases cache efficacy.

All of these features are designed to keep as much of the workload off of the processor as possible and to create a short, efficient path between the network packets and the vCPU that is generating or processing them.

Placement Groups

A placement group is an AWS solution to reduce latency between Amazon EC2 instances. It is a mechanism to group instances running in the same Availability Zone to be placed as close as possible to reduce latency and improve throughput.

Elastic Fabric Adapter

Elastic Fabric Adapter (EFA) is a network interface for Amazon EC2 instances that enables customers to run high performance computing (HPC) applications requiring high levels of inter-instance communications, like deep learning at scale on AWS. It uses a custom-built operating system bypass technique to enhance the performance of inter-instance communications, which is critical to scaling HPC applications. With EFA, HPC applications using popular HPC technologies like Message Passing Interface (MPI) can scale to thousands of CPU cores. EFA supports open standard libfabric APIs, so applications that use a supported MPI library can be migrated to AWS with little or no modification. EFA is available as an optional EC2 networking feature that you can enable on C5n.18xl and P3dn.24xl instances at no additional cost.

You can use Open MPI 3.1.3 (or later) or NCCL (2.3.8 or later) plus the OFI driver for NCCL.

The instances can use EFA to communicate within a VPC subnet, and the security group must have ingress and egress rules that allow all traffic within the security group to flow. Each instance can have a single EFA, which can be attached when an instance is started or while it is stopped.

Amazon Elastic Inference

Amazon Elastic Inference allows you to attach low-cost GPU-powered acceleration to Amazon EC2 and Amazon SageMaker instances to reduce the cost of running deep learning inference by up to 75%. Currently, Amazon Elastic Inference supports TensorFlow, Apache MXNet, and ONNX models, with more frameworks coming soon. To use any other deep learning framework, export your model by using ONNX, and then import your model into MXNet. You can then use your model with Amazon Elastic Inference as an MXNet model.

Amazon Elastic Inference is designed to be used with AWS enhanced versions of TensorFlow serving or Apache MXNet. These enhanced versions of the frameworks are automatically built into containers when you use the Amazon SageMaker Python SDK, or you can download them as binary files and import them into your own Docker containers.

Typically, you don't need to create a custom container unless your model is complex and requires extensions to a framework that the Amazon SageMaker pre-built containers do not support.

Amazon Elastic Inference accelerators are network-attached devices that work along with Amazon EC2 instances in your endpoint to accelerate your inference calls. When your model is deployed as an endpoint, ML frameworks use a combination of the Amazon EC2 instance and accelerator resources to execute inference calls.

To use Amazon Elastic Inference in a hosted endpoint, you can use any of the following, depending on your needs.

- Amazon SageMaker Python SDK TensorFlow - if you want to use TensorFlow and you don't need to build a custom container.
- Amazon SageMaker Python SDK MXNet - if you want to use MXNet and you don't need to build a custom container.
- The Amazon SageMaker SDK for Python (Boto 3) - if you need to build a custom container.

Typically, you don't need to create a custom container unless your model is complex and requires extensions to a framework that the Amazon SageMaker pre-built containers do not support.

The following Amazon Elastic Inference accelerator types are available. You can configure your endpoints or notebook instances with any Amazon Elastic Inference accelerator type.

Table 3: Elastic Inference accelerator types[2]

Accelerator Type	F32 Throughput (TFLOPS)	F16 Throughput (TFLOPS)	Memory (GB)
ml.eia1.medium	1	8	1
ml.eia1.large	2	16	2
ml.eia1.xlarge	4	32	4

Consider the following factors when choosing an accelerator type for a hosted model:

- Models, input tensors and batch sizes influence the amount of accelerator memory you need. Start with an accelerator type that provides at least as much memory as the file size of your trained model.
- Demands on CPU compute resources, GPU-based acceleration, and CPU memory vary significantly between different kinds of deep learning models. The latency and throughput requirements of the application also determine the amount of compute and acceleration you need. Thoroughly test different configurations of instance types and Amazon Elastic Inference accelerator sizes to make sure you choose the configuration that best fits the performance needs of your application.

Solutions

Amazon SageMaker Ground Truth for Data Labeling

Relative to other forms of machine learning, supervised learning continues to dominate the machine learning space. Feeding more data into the model training cycle continues to improve machine learning model performance. However, building a training dataset with accurate labels is a challenging and cost prohibitive task.

Amazon SageMaker Ground Truth helps in the first step of the machine learning process when data is collected and labeled. Amazon SageMaker Ground Truth combines automated data labeling techniques based on active learning with crowdsourced data labeling processes using Mechanical Turk. You can use active learning to identify attributes that must be learned and then use crowdsourced workforce to perform the labeling. Active learning is a methodology that can sometimes significantly reduce the amount of labeled data required to train a model. It does this by prioritizing the labeling work for the experts.

Active learning model looks at unlabeled data and calculates answers ranked by confidence. Next, the model compares its least confident scores against the labeled data. Last, the model tweaks itself so that if it sees the same data again, it is be more likely to calculate the correct answer.

Besides active learning capability and access to Mechanical Turk workforce, Amazon SageMaker Ground Truth helps you with label management and workflow management. Optionally, you also set up private and hybrid workforces for the labeling task.

Amazon SageMaker Neo for Model Optimization

Once you have a trained model, you may want to deploy it in the cloud, at the edge, or on mobile devices. The request for inference has to travel through the client HTTP stack, over the network, through the web server and application server stack to finally make it to the inference endpoint. Considering the latency introduced by all of the above layers, there is a small fraction of time left to compute the inference and serve it back to the client before it starts impacting the user experience. Therefore, it is always desirable to get maximum performance out of the inference endpoint.

Improving the performance of an inference endpoint is a complex problem. First, the computation graph of the model is a compute-intensive task. Second, optimizing machine learning models for inference requires tuning for specific hardware and software configuration on which the model is deployed. For optimal performance, you must know the hardware architecture, instruction set, memory access patterns, and input data shapes, among other factors.

In the case of traditional software, compilers and profilers handle the tuning. In the case of deep learning model deployment, it becomes a manual trial and error process.

Amazon SageMaker Neo can help you eliminate time and effort required to tune the model for specific software and hardware configuration by automatically optimizing TensorFlow, Apache MXNet, PyTorch, ONNX, and XGBoost models for deployment on ARM, Intel, and NVIDIA processors. This list of supported deep learning frameworks, model formats, and chipsets will continue to grow in the future.

Amazon SageMaker Neo consists of a compiler and a runtime. First, Amazon SageMaker Neo APIs read models and parse it into a standard format. It converts the framework-specific functions and operations into a framework-agnostic intermediate representation. Next, it performs a series of optimization on the model graph. Then, it generates binary code for the optimized operations. Amazon SageMaker Neo also provides a lean runtime for each target platform and source framework that is used to load and execute the compiled model. Last, Amazon SageMaker Neo is also available as open source code as the Neo-AI project under the Apache Software License, enabling you to customize the software for different devices and applications.

Code, Data, and Model Versioning

Version Code with Git

The training, preprocessing, and inference scripts are the smallest components of the overall deep learning stack. In addition to the above scripts, you can also script your deep learning pipeline for model retraining and model deployment using services such as AWS Step Functions. Together, all the above scripts can be version controlled using any Git-based repository or using AWS CodeCommit, a fully managed source control service that hosts secure Git-based repositories.

Version Data in Amazon S3

In deep learning, the copy of the data that was used to retrain a model is important to explain and troubleshoot the bias and the drift in the model. You can use Amazon S3 to version your training data. Create a new Amazon S3 object or new version of Amazon S3 object for every new or updated training dataset. You can use the naming convention of the Amazon S3 object or use object tags to track training dataset versions. Optionally, you can push dataset S3 object location and data metadata in an Amazon DynamoDB table and index the table to make it searchable for data discovery.

Version Model in Amazon S3

Training a model is costly and time consuming. It is important to persist the model to compare the performance and accuracy of new variants of the model. You can assume trained model as a special data file that can be persisted in Amazon S3 as a data file with version control enabled. Amazon S3 allows you to tag and version data files of any type.

Automation of Deep Learning Process for Retrain and Redeploy

After you demonstrate a functional prototype, it is time to put the model in production and create an endpoint for serving prediction using the trained model. During the prototyping, all the steps to build, train, and deploy are performed manually in the Jupyter notebook. However, deployment in production requires precision, consistency, and reliability. Manual interventions in the production pipeline often lead to human errors that can lead to downtime. You can address human errors by automating all the

steps involved in retraining and redeployment. Discussed below are the solutions and services that can be used to automate your deep learning production pipeline on AWS.

AWS Step Functions for Amazon SageMaker

AWS Step Functions allows you to orchestrate multiple steps in the ML workflow to allow for seamless model deployment in the production. AWS Step Functions translates your workflow into a state machine diagram that is easy to understand, easy to explain to others, and easy to change. You can monitor each step of execution as it happens.

Today, Amazon SageMaker supports two different patterns for service integration:

- Call an Amazon SageMaker instance and let AWS Step Functions progress to the next state immediately after it receives an HTTP response.
- Call an Amazon SageMaker instance and have AWS Step Functions wait for a job to complete.

Apache Airflow for Amazon SageMaker

Apache Airflow is an open source alternative platform that enables you to programmatically author, schedule, and monitor workflows. Using Apache Airflow, you can build a workflow for Amazon SageMaker training, hyperparameter tuning, batch transform and endpoint deployment. You can use any Amazon SageMaker deep learning framework or Amazon SageMaker algorithms to perform these operations in Airflow.

You can build a Amazon SageMaker workflow using Airflow SageMaker operators or using Airflow Python Operator.

You can also use Turbine, an open-source AWS CloudFormation template, to create an Airflow resource stack on AWS.

Kubeflow Pipelines on Kubernetes

If you are a DIY customer not using Amazon SageMaker and are leveraging your current investment in Kubernetes on AWS, you can use Kubeflow Pipelines. Kubeflow Pipelines is a platform for building and deploying portable, scalable machine learning (ML) workflows based on Docker containers. A *pipeline* is a description of an ML workflow, including all of the components in the workflow and how they combine in the form of a graph. This is popular tool that is used by practitioners using Kubernetes for build, train, and deploy. It has native integrations with Kubernetes.

There are also AWS pipeline components for Kubeflow that integrate with Amazon SageMaker and other AWS services used for data cleaning and transformation, such as Amazon EMR and Amazon Athena. This approach is for customers who want a unified control plane (unifying their microservices architecture with their AI/ML service releases) but also want to leverage different AWS services, such as Amazon EKS, Amazon FSx for Lustre, and Amazon SageMaker that are best fit for job and can help with the undifferentiated heavy lifting.

Patterns for Deep Learning at Scale

In this section, we describe different solutions and patterns that you can use to scale out deep learning adoption in your organization. The options include fully managed, DIY using AWS services, or a hybrid approach. You can also extend these options using other AWS services to build a custom environment.

Options for Deep Learning on AWS

In this section, we discuss both fully managed and DIY platform as a solution approaches for deep learning on AWS. AWS offers multiple options that cover the full spectrum of solutions for deep learning depending on different levels of shared responsibility between AWS and the customer, as shown in the following figure.

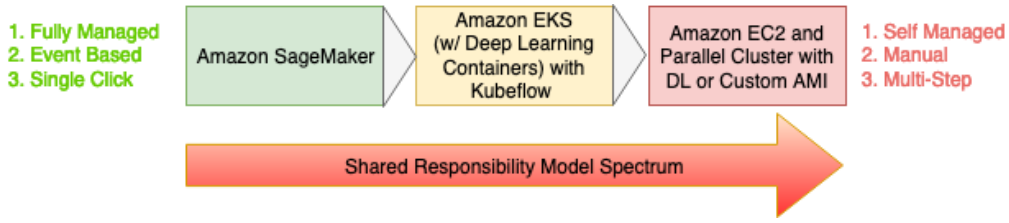

Figure 6: Deep learning solutions on Shared Responsibility Model spectrum

The left side of the spectrum is Amazon SageMaker, fully managed service for deep learning, event-based, and provides a single-click build, train, deploy experience. On the right side of spectrum is a fully customized deep learning solution that is self-managed, manual and involves multiple steps to build, train, and deploy. In between these options is a partially managed solution where you can simplify infrastructure management by using managed services, such as Amazon EKS and you can deploy self-managed Kubeflow for deep learning workflow.

To provide more information on the differences between self-managed and custom DIY solutions, let's walk through operational and steps involved in one-time setup of deep learning environment.

For a DIY setup, you must manage the following operational issues to keep the deep learning environment available for deep learning engineers and scientists:

- Driver installation
- Update coordination
- Network breakdowns
- Unscheduled reboots
- Power outages
- Equipment failure
- Response issues
- Disk space shortage
- Cable problems
- Server not reachable via VPN
- Unsecured physical perimeter of server

In the case of AWS managed services, such as Amazon SageMaker, the chances of operational issues are minimized because all of the AWS managed services are fault-tolerant and highly available by design.

For example, in a custom DIY setup, where you build a deep learning environment from scratch on Amazon EC2, you must perform the following tasks to run distributed training using TensorFlow and Horovod to generate value. These tasks include one-time software installation and ongoing job scheduling tasks.

1. SSH, Login to Head Node
2. Install MPI
3. Install Anaconda, Python 3
4. Create a Virtual Environment
5. Install Intel Optimized TensorFlow with MKL
6. Install Horovod for Distributed Training

7. Create SLURM Job Script (SLURM is an open source scheduling software for HPC jobs)
8. Submit SLURM Job
9. Obtain Insights

In the case of AWS managed services, such as Amazon SageMaker, all of the above steps are automated and triggered with single click in the AWS Management Console, single API call, single CLI command, or event based.

Let's dive deeper into each solution to review the components and value of each solution.

Fully Managed Solution - Use Amazon SageMaker

If you are looking for a solution to scale deep learning across your organization, Amazon SageMaker offers an end-to-end solution to support the different steps involved in a deep learning process. Not only does Amazon SageMaker provide native support in the form of a fully managed service, but it also provides flexibility to customize deep learning stacks to take advantage of most recent innovation in drivers and frameworks. The simplicity and flexibility that Amazon SageMaker offers meets the needs of advanced deep learning engineers and deep learning scientists working at the framework level as well as data scientists and developers contributing to deep learning project with minimal background in deep learning.

The following chart shows how different Amazon SageMaker components fit into the deep learning landscape to provide an end-to-end deep learning process.

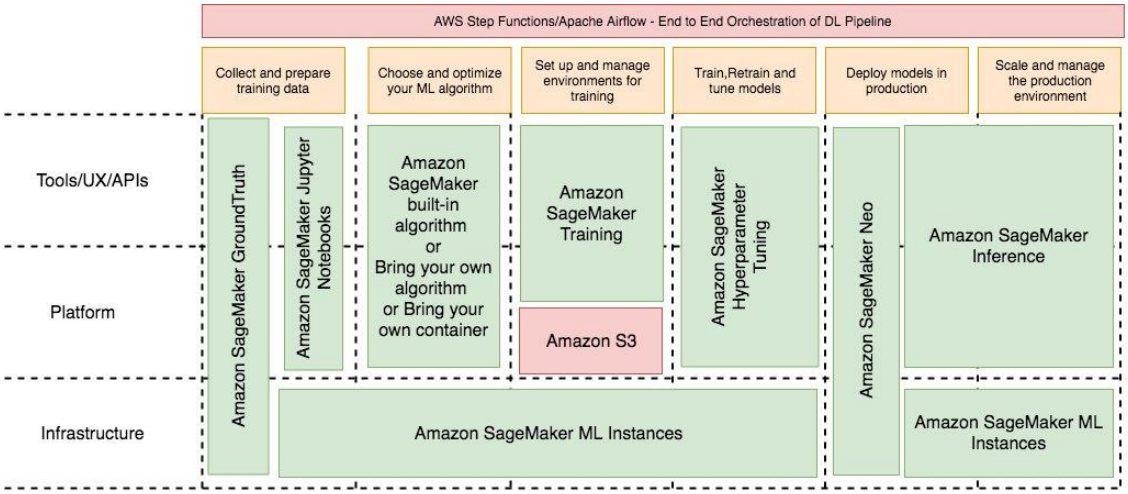

Figure 7: Amazon SageMaker solution for deep learning

Amazon SageMaker completely abstracts the infrastructure creation and termination tasks required for deep learning build, train and deploy environment. As a part of the infrastructure, it also handles the installation of common drivers such as NCCL, CUDA, and CUDNN; installation of common data processing libraries; and installation of common frameworks used for deep learning today. The notebook, training, and inference environment creation is made available as an API call, CLI command, Amazon SageMaker SDK, or as an option in the AWS Management Console. Amazon SageMaker allows you to automate a sequence of tasks into an automated workflow for an ML pipeline, such as retraining and redeploying new variants of a model with consistency.

Amazon SageMaker simplifies common deep learning tasks, such as data labeling, hyperparameter tuning, real time and batch inference. The simplification of these tasks allows you to accelerate and scale deep learning adoption within an organization without losing control. The standard sets of tools that are fully managed allows better collaboration and improved time to market for deep learning projects.

Amazon SageMaker also provides a single platform to both deep learning engineers and scientists and DevOps professionals in an organization to allow for a clean handshake between model authors who design algorithms and train models on data and DevOps team who are responsible for model deployment and monitoring.

Amazon SageMaker provides pre-built container images for most of the popular framework. You can extend the exiting Amazon SageMaker container images or build your own. Advanced deep learning engineers and scientists working at the framework level may want to try a custom DL framework such as TensorFlow (TF) to try a custom operator to accelerate deep learning training for a specific use case or may want to run two TF process on a single instance for improved performance. Amazon SageMaker allows you to configure and customize the environment using script mode and bring your own container mode. The script mode allows you to bring your custom script (such as a TF script) and run it on pre-built TF AWS DL containers. Bring your own container allows maximum flexibility and control as you can build the container from scratch with your custom TF build and run it on Amazon SageMaker.

DIY Partially Managed Solution: Use Kubernetes with Kubeflow on AWS

This pattern applies to customers who have decided to standardize on Kubernetes as an infrastructure layer and would like to leverage their existing investment in Kubernetes to run deep learning training and inference jobs. This setup introduces a lot of

undifferentiated heavy lifting and operational complexity to manage Kubernetes. Managing the Kubernetes control plane can be difficult. However, there is an opportunity to offload the management of Kubernetes master to AWS by using Amazon EKS, a managed service for Kubernetes, to simplify the Kubernetes control plane management.

It is important to note that Amazon EKS Kubernetes cluster is a persistent cluster. However, customers can manage the policy to scale-out and scale-in on-demand to provide sufficient resources to complete the training and inference jobs successfully. The training jobs rely on the underlying Kubernetes cluster for infrastructure and consume resources from it. If more compute capacity is required, you must add more worker nodes to the Kubernetes cluster to meet capacity requirement. You can leverage node level autoscaler (Kubernetes add-ons) to scale (in/out) GPU nodes.

For inference endpoint scaling, you can use horizontal pod scaling at the Kubernetes level. You can also deploy additional software, such as TensorBoard, for training visualization as a sidecar pattern on pods. A Kubernetes pod is a group of containers that are deployed together on the same host.

A Kubernetes cluster provides the infrastructure layer for running deep learning training and inference in the container environment. However, you must deploy and manage more components to make this environment easy to use for deep learning projects.

You can use Kubeflow which provides a unified API platform that is tightly integrated with Kubernetes and allows deep learning engineers and scientists to build, train, and deploy on Kubernetes. Kubeflow is not an AWS managed service. Kubeflow is a Kubernetes add-on package that you must self-deploy and self-manage on Amazon EKS or Kubernetes on AWS.

Initially, Kubernetes and Kubeflow had support for TensorFlow only. However, it is expanding its support to other frameworks such as MXNet, PyTorch, and Chainer. It is also important to note that the community frequently updates Kubeflow and you may have to make frequent changes to your scripts to keep up with the latest version of the Kubeflow.

For the storage layer, you can choose Amazon S3, Amazon EFS, or Amazon FSx for Lustre (hydrated from data from Amazon S3). For deep learning and the highest level of performance, AWS recommends Amazon FSx for Lustre with hydration of data from Amazon S3. However, depending on the number of nodes used for distributed training,

you can also choose to use Amazon S3 and Amazon EFS. With Amazon S3 and Amazon EFS, performance is not as high as Amazon FSx for Lustre.

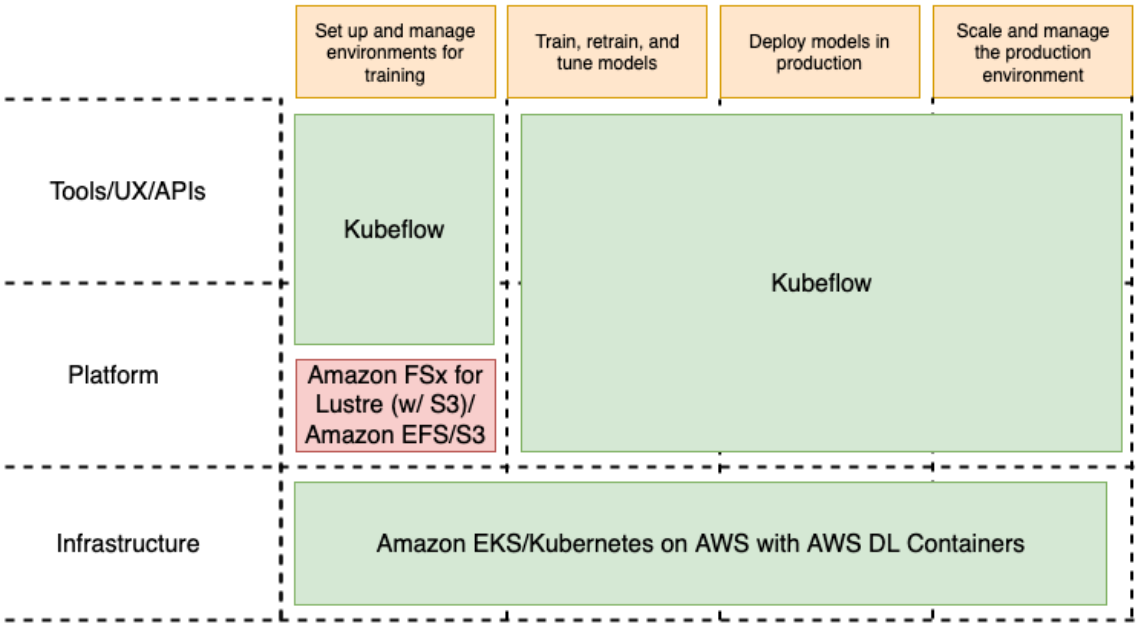

Figure 8: Amazon EKS and self-managed Kubeflow DL layers and DL process mapping

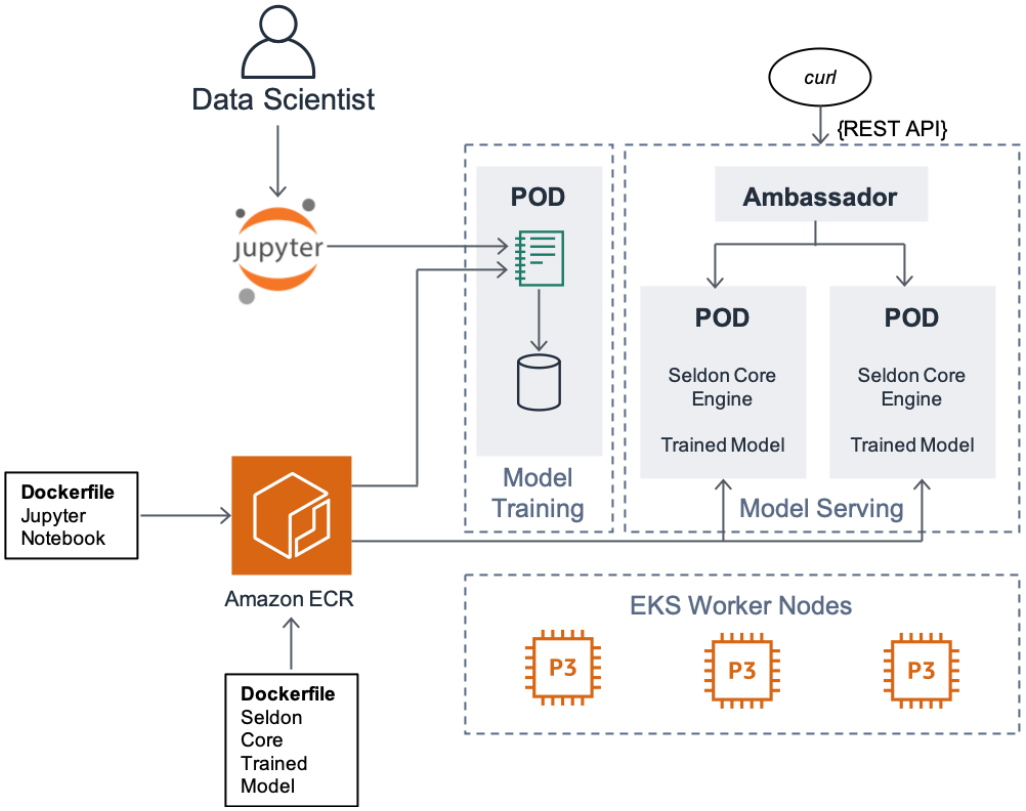

Figure 9: Amazon EKS with self-managed Kubeflow conceptual diagram[3]

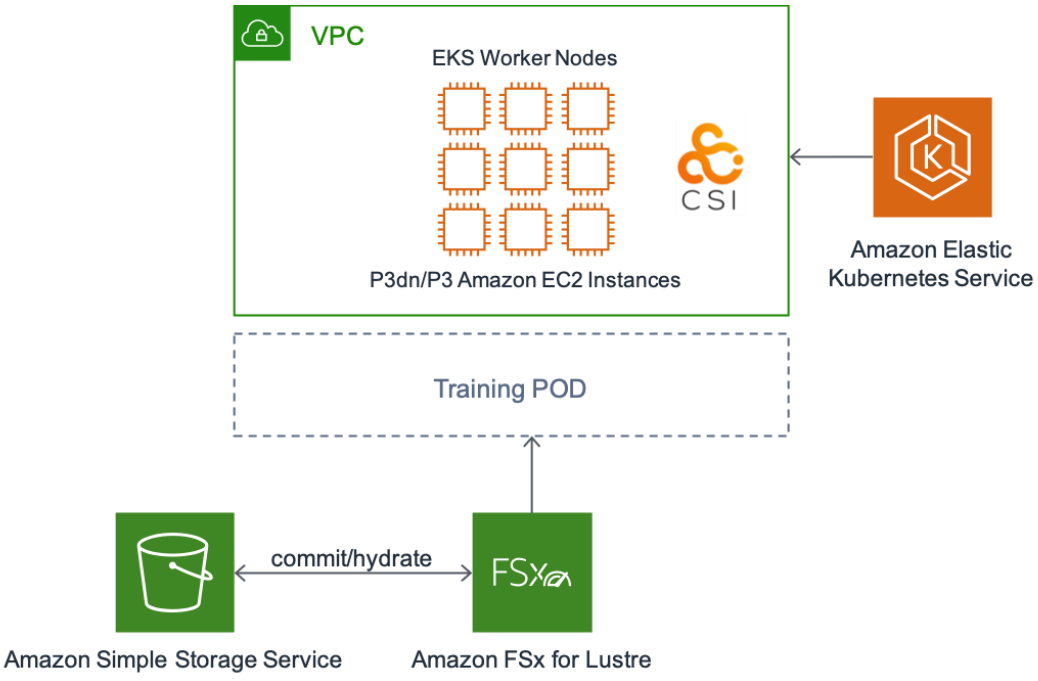

Figure 10: Amazon EKS with Amazon FSx for Lustre hydrated from Amazon S3

You can use Amazon SageMaker components with this stack for tasks such as data labeling and model optimization. You can use Amazon SageMaker for an end-to-end deep learning workflow or in parts. With Kubernetes and Kubeflow stack, you can still use Amazon SageMaker Ground Truth for data labeling and annotation and Amazon SageMaker Neo for model optimization.

Additional Considerations for DIY Solution

Amazon EKS is a managed service that is not specifically tuned and optimized for deep learning. Kubeflow is not a managed service offered by AWS. You must fine tune and optimize the Amazon EKS and Kubeflow stack for deep learning by implementing best practices. For more information, see Best Practices for Optimizing Distributed Deep Learning Performance on Amazon EKS on the AWS Open Source Blog.

Optionally, you can also use Amazon EKS Deep Learning Benchmark Utility, which is an automated tool for machine learning benchmarking on Kubernetes clusters.

Optionally, you can also use AWS Deep Learning Containers (AWS DL Containers), which are a set of Docker images for training and serving models in TensorFlow and MXNet on EKS. AWS DL Containers provide optimized environments with TensorFlow and MXNet, NVIDIA CUDA (for GPU instances), and Intel MKL (for CPU instances) libraries. AWS DL Containers are available in the Amazon Elastic Container Registry (Amazon ECR).

There are numerous initiatives to allow more native integration between Kubeflow and the AWS platform for deep learning. For the complete list of native integration between Kubeflow and AWS, see Kubeflow on AWS Features.

DIY Self-Managed Solution: Use Amazon EC2

There are organizations and deep learning engineers and scientists who may not adopt container strategy for build, train, and deploy, nor have the required skills to operate in a containerized environment. Or, deep learning engineers and scientists may want to use the latest drivers and libraries from the research community and may not have guidance for installation on a containerized environment. The installation and integration for this new software may not be available or easy.

In this type of scenario, you can set up a custom DIY cluster on top of Amazon EC2 to develop and scale your experiment.

Although you have the option to set up everything from scratch, you may want to use some tools and services described below to make the installation easy and to accelerate your training on AWS.

Customers can use the Deep Learning AMI that comes with GPU drivers installed and most of the popular framework and libraries installed. Customers have full control of this environment and can easily customize it to their needs. It is also easy to switch between CUDA driver versions.

For storage, customers can use Amazon S3, Amazon EFS, or Amazon FSx for Lustre as a data storage layer for the training environment. In choosing among Amazon FSx for Lustre, Amazon S3, and Amazon EFS, you are making a tradeoff between price and performance.

This pattern is useful for one-off projects that may have niche requirements. However, don't consider it as an alternative for a deep learning platform for the enterprise. You can clearly see the gaps in the following figure.

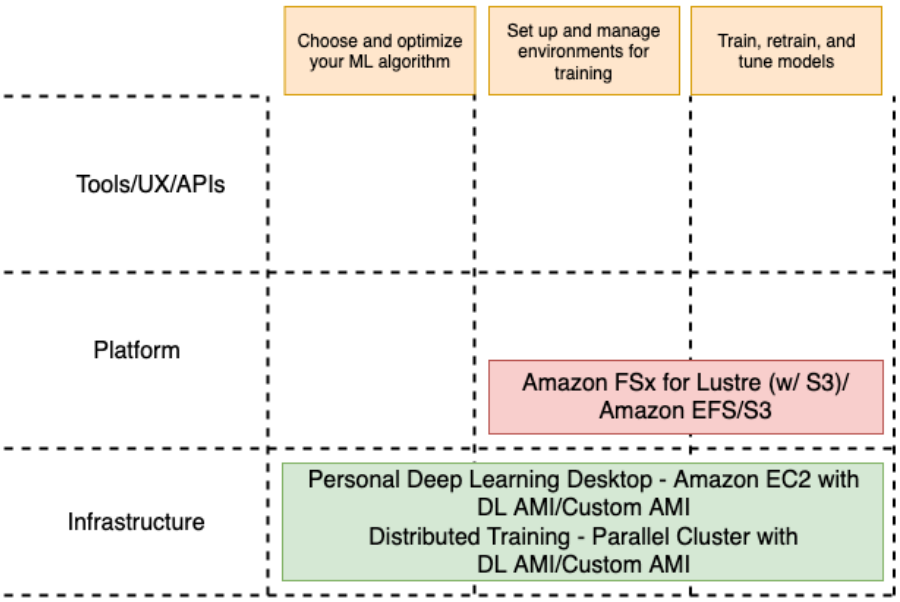

Figure 11: Amazon EC2 with DL AMI DL layers and ML process mapping

If you want to scale your experiment on a large dataset on multiple nodes in a custom environment using Amazon EC2, you can use tools such as AWS Parallel Cluster to help you set up the cluster. AWS Parallel Cluster is an open source cluster management tool that makes it easy for scientists, researchers, and IT administrators to deploy and manage High Performance Computing (HPC) clusters in the AWS Cloud.

With AWS Parallel Cluster, many AWS Cloud native products are used to launch a cluster environment that should be familiar to those running HPC workloads.

You can use a job scheduler such as SLURM to schedule your training jobs on cluster. The following figure shows how this set up appears when used with Amazon EFS as the storage tier. If you want to further improve the performance of cluster, you can use Amazon P3dn Instances, with Elastic Network Adapter (ENA) and Amazon FSx for Lustre hydrated from Amazon S3.

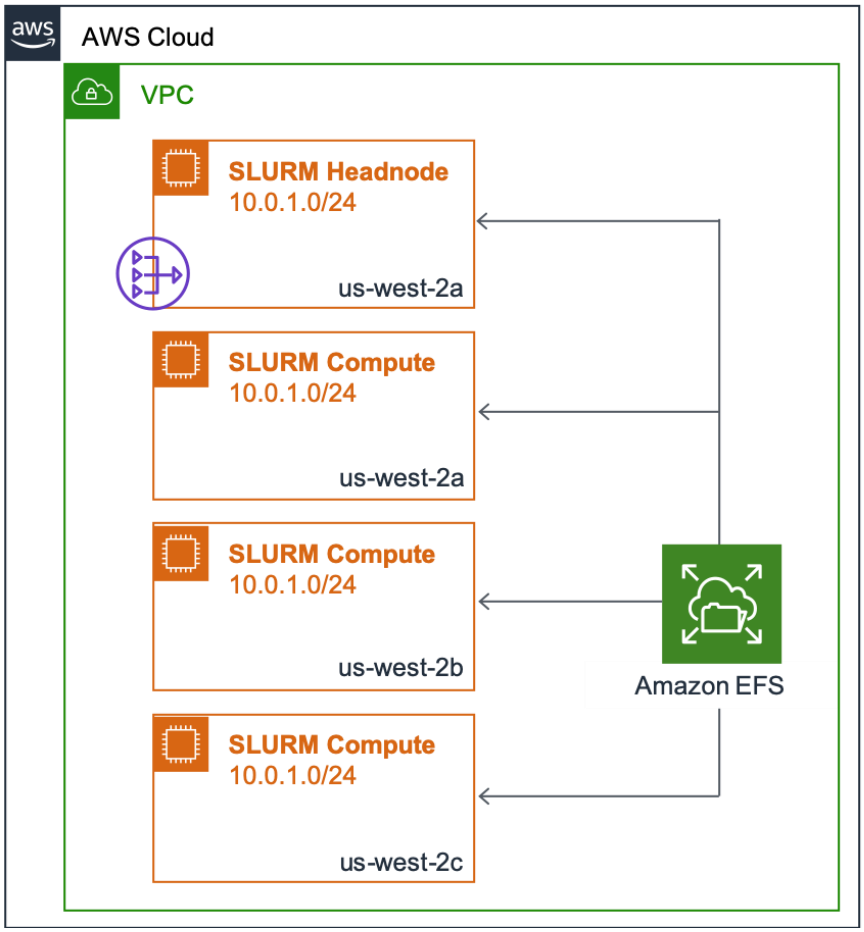

Figure 12: SLURM Architecture using Amazon EC2 and Amazon EFS

Advanced Use Cases: Use Amazon SageMaker with Other AWS Services

You may have an advanced use case where you must leverage other AWS services to extend the capabilities of the Amazon SageMaker provided deep learning solutions. In

this section, we review some advanced use cases using Amazon SageMaker and other AWS services.

Orchestrate Your End-to-End Machine Learning Pipeline using AWS Step Functions

AWS Step Functions allow you to build resilient serverless workflows. In AWS Step Functions, a workflow is implemented as a finite state machine. The states can be a task, a choice, a branch of logic, a set of parallel tasks, an error handler, and so on. The workflow is implemented as a Directed Acyclic Graph (DAG) and uses GoTo logic. AWS Step Functions also allows you to throw an exception and do error handling to make the flow more robust.

In AWS Step Functions, the task states do most of the heavy lifting. There are two types of task states: Activity task and Lambda task. In Activity tasks, worker requests work from AWS Step Functions, then takes the work and returns the results. The Lambda task is a synchronous call to an AWS Lambda function from AWS Step Functions. The Lambda task has a maximum timeout of 15 minutes as defined by the max execution duration of the Lambda function. AWS Step Functions also allows you to insert human actions such as approval and rejection into the state machine. The actions can be used in the workflow to approve or deny the model push into the production environment.

Using all of the capabilities of AWS Step Functions, you can build a complex end-to-end deep learning workflow. You can trigger the workflow when the new data arrives in Amazon S3, start the training job, and deploy the newly trained model. You can make the workflow more robust and transparent by adding notifications and error handling to it. The following workflow diagram is a sample representation of an end-to-end deep learning workflow implemented using AWS Step Functions for retraining and redeployment.

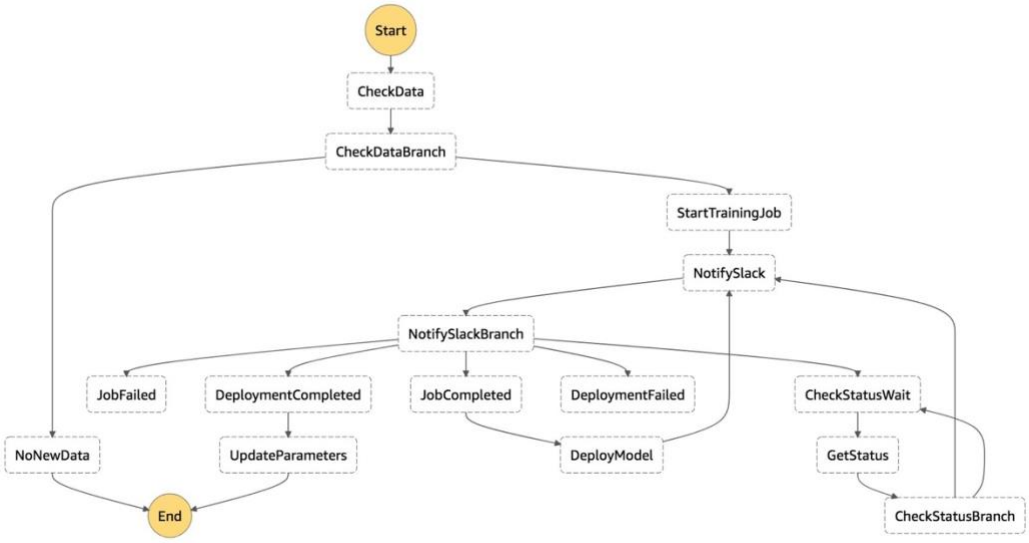

Figure 13: Workflow for retraining and redeployment

Orchestrate Your Hyperscale Deep Learning jobs using AWS Batch with Amazon SageMaker as Backend in Multiple AWS Regions

Some customers have use cases that requires training on a very large dataset where data must remain local within the sovereign boundaries of the region in which it was generated either due to cost, performance, or regulatory concerns. This data could be the 4K video data of an autonomous vehicle generated locally or campaign data generated locally, transferred locally to nearest AWS Regions, and labeled within the same Region. You can use Amazon SageMaker to train your model locally in the same region. Optionally, you can launch multiple Amazon SageMaker training jobs to train parallelly in each Region. You can use AWS Batch to orchestrate and monitor multiple jobs running on Amazon SageMaker in multiple AWS Regions from a central region. This event-driven architecture triggers the training job as data is uploaded from the on-premises environment to nearest AWS Region.

You can generate data coming into Amazon S3 into a relation table in one central place. The central table keeps the index of all the data files sourced from different campaigns running in different geographic locations. From this central table, you can issue a query to generate an AWS Batch array job. AWS Batch array jobs are submitted just like regular jobs. However, you specify an array size (between 2 and 10,000) to define how many child jobs should run in the array. If you submit a job with an array size of 1,000, a single job runs and spawns 1,000 child jobs. The array job is a reference or pointer to the parent job to manage all the child jobs. This feature allows you to submit large

workloads with a single query. For this setup, you build two Docker images: one for Amazon SageMaker training and the other for orchestrating training in multiple Regions using Amazon SageMaker APIs. The orchestrator image run by AWS Batch has the logic to spawn multiple child jobs in different AWS Regions with different parameters, but it will be using the same job configuration in all four Regions.

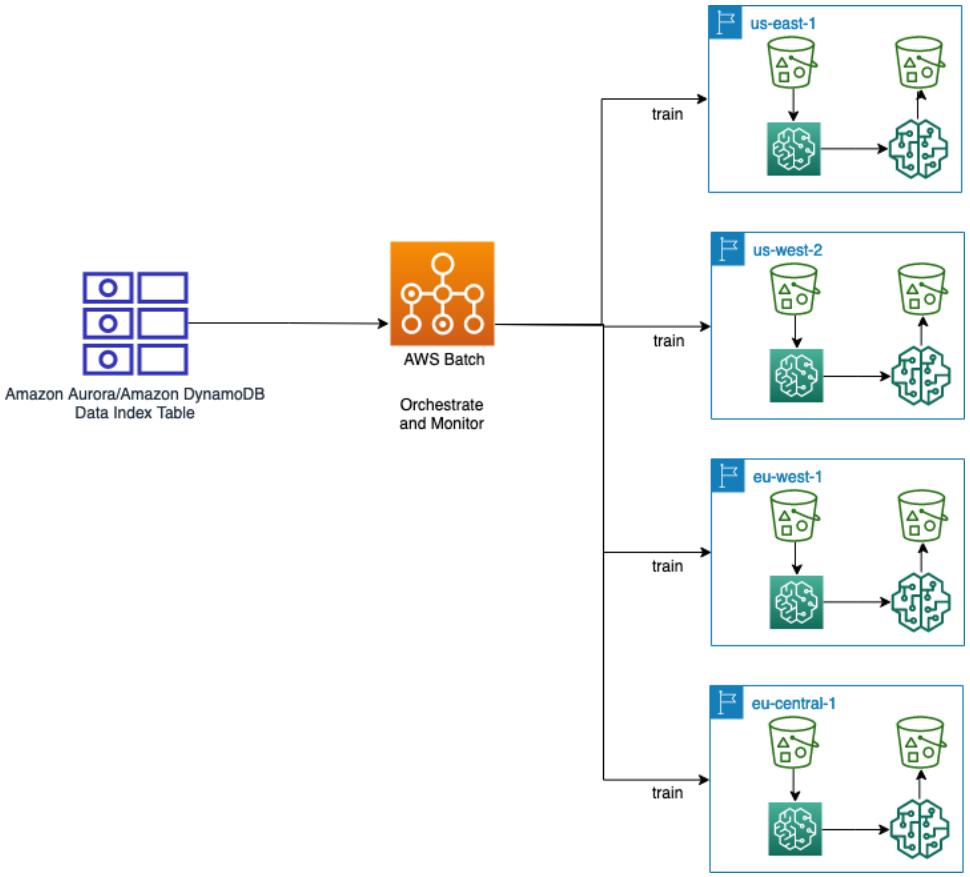

Figure 14: Reference architecture to orchestrate Amazon SageMaker jobs in multiple Regions

Use Amazon S3 and Amazon DynamoDB to Build a Feature Store for Batch and Real-Time Inference and Training

Many organizations that want to be a data-centric company or may already be one are either in the process of building a data lake solution or may already have a data lake solution to democratize their data for analytics and AI/ML.

Data lake creation is a critical step in the machine learning process because your entire organization's data is managed and shared from a single repository. However, the question that arises is how deep learning engineers and scientists, who are not data engineers, can easily acquire new features to solve new problems. How do deep

learning engineers and scientists extract meaningful features from the mountain of data sitting in a data lake? It takes time and a different set of skills to build a dataset of features from a data lake for use in deep learning.

A feature is a measurable property of phenomena under observation. It could be a raw word, pixel, sensor value, row in a data store, field in a CSV file, an aggregate (min, max, sum, mean), or a derived representation (embedding or cluster).

A feature pipeline is shown in the following diagram. You can imagine the amount of work that is required to build a feature set using such a complex pipeline. Based on the anecdotal evidence derived from customer conversations, feature engineering can consume 25% or more of the time spent on a deep learning project.

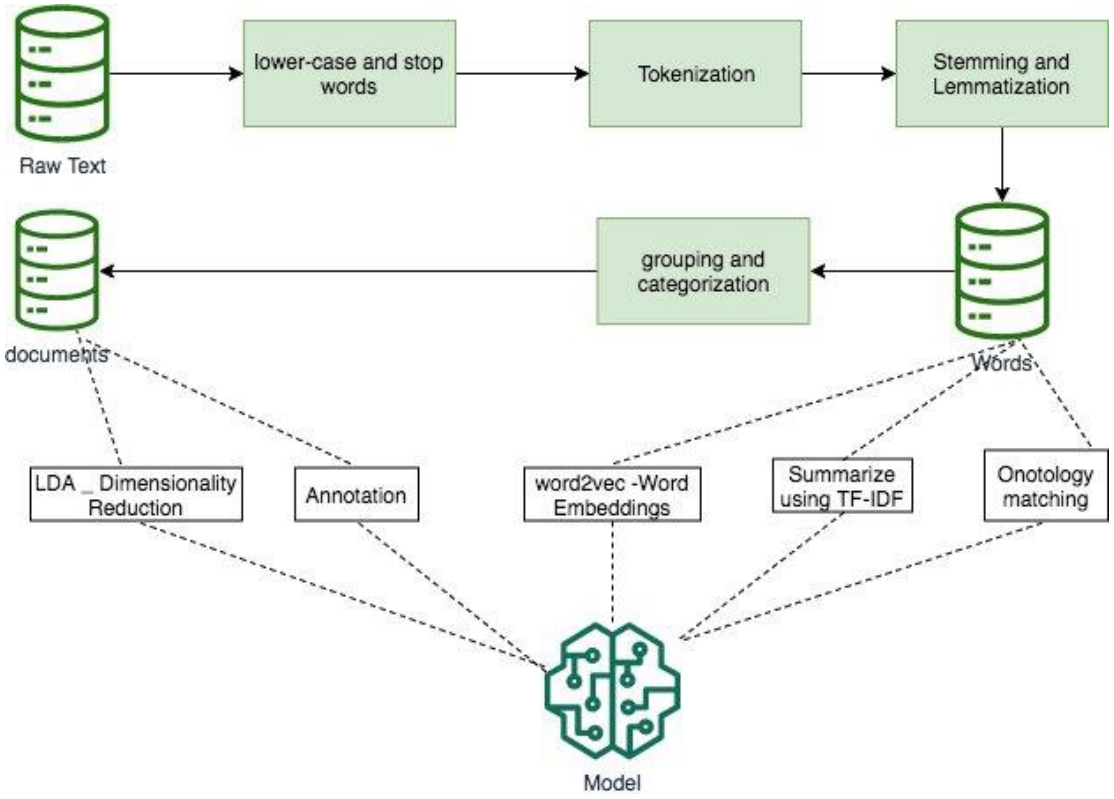

Figure 15: Example feature pipeline

As with most of the technology solutions, there are two ways to solve this problem: develop a technique to automate feature engineering or reuse the existing feature and models. Although the research on automated feature engineering is making progress, the interest and patterns around feature reuse have begun to surface in few organizations. The concept of the feature store is getting attention and traction. It is still

early stage, and there are few open source initiatives and few third-party ISV vendors who have solutions targeted around this new idea.

In simple terms, a feature store is a curated repository of deep learning features that can be reused across different projects to train, evaluate and infer deep learning models.

The fundamental difference between a deep learning feature store and other stores (such as a data warehouse) is that features are the primary entity in the deep learning feature store.

You can develop a simple feature store using AWS services and continue to iterate and refine it over time. Following capabilities are required to support a feature store.

- **Reuse:** Use the existing feature store pipeline developed by data engineers to recompute and cache features in a feature store.
- **Store:** Store the metadata of features such as a description, documentation, and statistical measures of features in the feature store.
- **Discover:** Make the metadata searchable through an API to ML practitioners.
- **Govern:** Add a data management layer on top of the feature store for governance and access control.
- **Consume:** Allow ML practitioners to query and consume features using an API to export the features for training or real-time inference.

The feature store can bring down the cost of ML project significantly. Savings are direct result of reuse of the curated feature set by subsequent projects. Besides cost, reusing a feature store can help you with faster time to delivery as ML practitioners are working on a curated list of features and not working on a heap of data in a data lake. The feature store provides an abstraction between your role as a data engineer and ML practitioner. The feature store also allows you to ensure consistency in training and inference. The following figure shows the relationship graph between cost of an ML project and feature reuse. As shown, the cost of the project drops as more and more features are reused from the feature store.

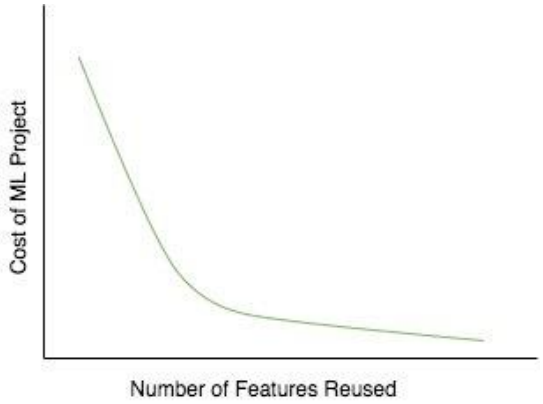

Figure 16: Cost of ML project vs. feature reuse

You can use Amazon S3 as source of truth for the feature store. You can version and govern your feature store using controls provided by Amazon S3.You can use Amazon S3 as storage layer for Amazon SageMaker training and Amazon SageMaker Batch Transform jobs. For low latency online inference, you can copy the feature dataset into Amazon DynamoDB and use it for inference. If you want to make features discoverable and searchable, you can push feature metadata to Amazon DynamoDB and make the metadata searchable using Amazon Elastic Search.

The following figure shows the reference architecture for feature store.

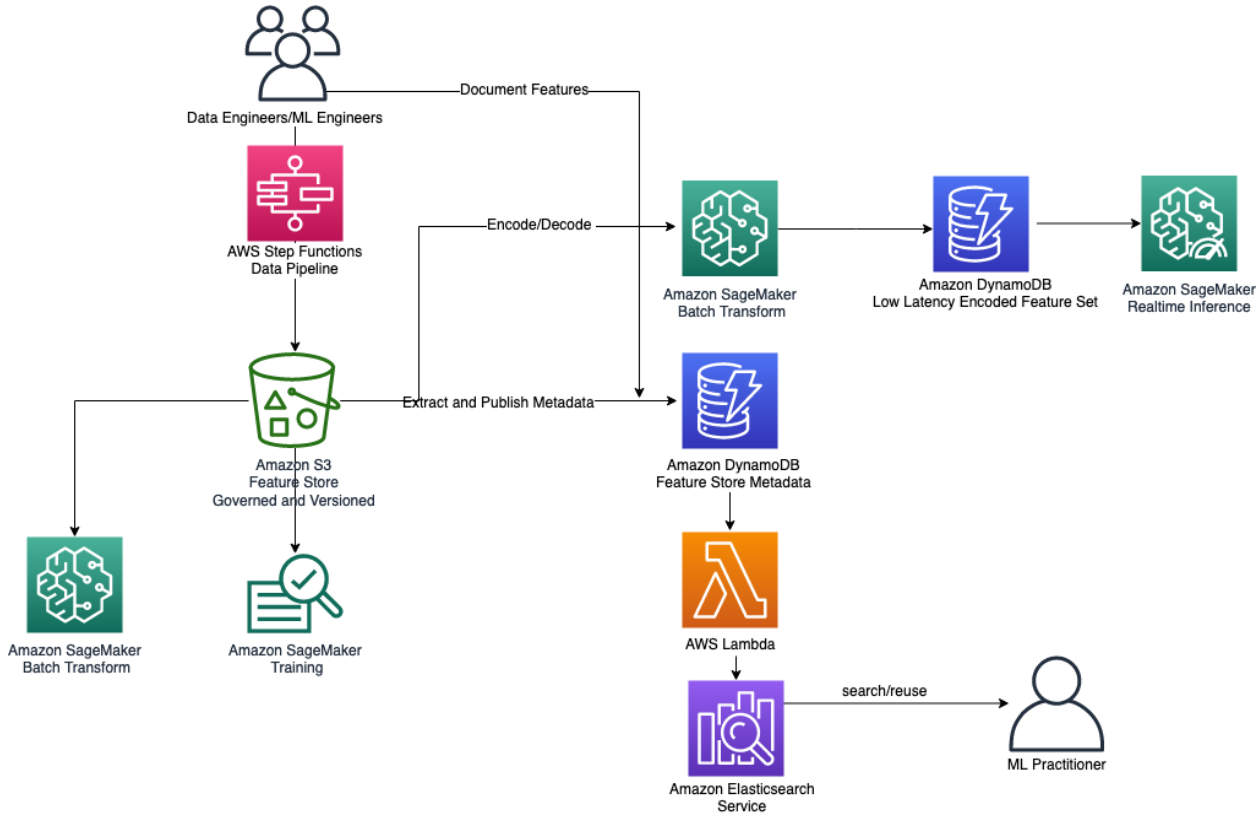

Figure 17: Feature store reference architecture on AWS

The following figure shows how the data lake, data warehouse, and feature store are positioned relative to each other at the enterprise level.

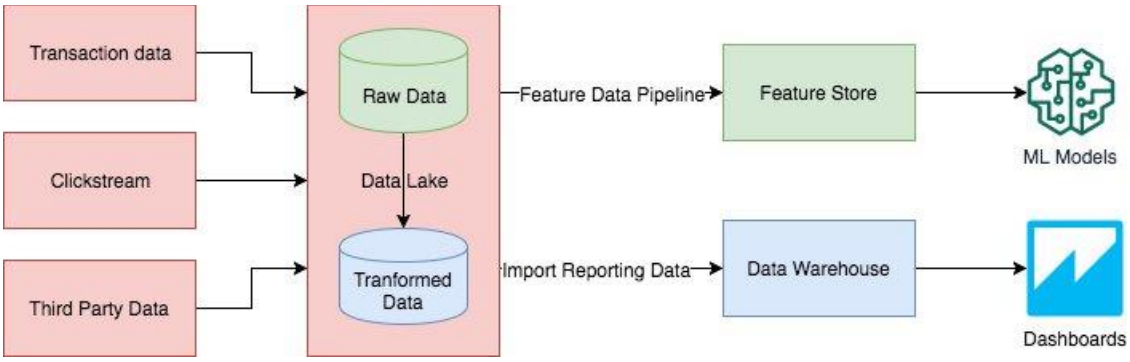

Figure 18: Conceptual composite view of data lake, data warehouse, and feature store

AWS Guidance

In this guide, we described the deep learning stack and the deep learning process. We discussed AWS services that can be used to address the deep and broad needs of deep learning engineers and scientists. We also described design patterns that deep learning engineers and scientists can leverage to adopt and scale deep learning in their organization. We discussed features that are available out of the box and are ready to use in Amazon SageMaker, a fully managed service for machine learning. We also discussed cases where you would want to build deep learning environments on your own using other AWS services such as Amazon EC2 and Amazon EKS. With AWS, you get the flexibility to choose the approach that works best for you.

Below are some of the popular scenarios in which customers are leveraging different options offered by the AWS AI/ML stack.

If you are a start-up, you want to spend less on buying high-performance GPU compute and managing the infrastructure. Most likely, you have a small team of developers and data scientists and your focus would be to roll out new deep learning capabilities with small teams. Amazon SageMaker is an ideal choice for you.

If you are working as a research scientist in an organization developing a new product feature, using deep learning capabilities, you may need more autonomy, more isolation, and more control. It is possible your organization may not have a directive or a policy to use a standard platform for deep learning. You can continue to use Amazon EC2 with AWS DL AMI as your deep learning desktop, but you may also want to consider Amazon SageMaker for training with automatic hyperparameter tuning to scale experiments.

If you are a product team working to keep your deep learning model performing well under changing customer preferences, you can implement an end-to-end automated deep learning pipeline to retrain and deploy your models using AWS Step Functions and Amazon SageMaker.

If you are the technology leader in your organization who has been tasked to accelerate deep learning adoption in the organization, you can use Amazon SageMaker as a fully managed service for building, training, and deploying deep learning models in your organization. Amazon SageMaker allows you to achieve more with smaller deep learning teams. The fully managed service helps keep operations lean, eliminates compute infrastructure waste, improves productivity of deep learning engineers and scientists, allows cost efficient experimentation, and a shorter time to market.

If you belong to an organization that has decided to standardize infrastructure on Kubernetes, you can use Amazon EKS as an infrastructure layer. You can add open source components such as Kubeflow to simplify build, train, and deployment of deep learning models on Amazon EKS. Amazon EKS is a persistent cluster. The cluster can scale-in and scale-out. However, it is a general-purpose compute platform that requires tuning to make it efficient and performant for deep learning jobs. It requires advanced expertise and skills to manage and operate it. Optionally, with Kubernetes and Kubeflow stack, you can use Amazon SageMaker Ground Truth for data labeling and annotation and Amazon SageMaker Neo for model optimization.

Conclusion

This guide provided you with a comprehensive overview of all the technology building blocks, solution and patterns used when deploying deep learning on AWS. Additionally, we also highlighted some advanced use cases that may be of interest to you. We understand that research in deep learning is advancing fast and the tools used in deep learning domain are constantly changing and evolving.

The current state of options offered by the AWS landscape, ranging from fully managed to DIY, cover both the definitive and exploratory requirements of most deep learning projects. However, it is possible that you encounter a use case or a requirement that may require deeper engagement and conversations to address special requirements of your projects. For these special requirements or for clarification on content published in this guide, reach out to your respective AWS account teams.

Contributors

Contributors to this document include:

- Vikrant Kahlir, Solutions Architect, Strategic Accounts
- Christian Williams, Machine Learning Specialist, AWS Solutions Architecture
- Amr Ragab, HPC Global Consultant, AWS Professional Services

Further Reading

For additional information, see:

- AWS Whitepapers & Guides page
- Machine Learning on AWS
- AWS Machine Learning Blog
- AWS Machine Learning Training

Notes

[1] Yuji Roh, Geon Heo, Steven Euijong Whang, “A Survey on Data Collection for Machine Learning: a Big Data - AI Integration Perspective,” (November 2018): 3, https://arxiv.org/pdf/1811.03402.pdf

[2] For pricing information, see Model Deployment on the Amazon SageMaker Pricing page.

[3] https://aws.amazon.com/blogs/opensource/kubeflow-amazon-eks/

[4] http://wiki.lustre.org/Introduction_to_Lustre