<주요 Q&A>

SDS Cloud 환경에서 Kubeflow를 활용하여 쉽게 구현하는 MLOps

Q1. 현실에서의 머신러닝 프로젝트를 효과적으로 수행하려는 경우 중점적으로 검토하고 점검해야 할 사항들에 대해서 질문 드립니다.

머신러닝 알고리즘 자체의 성능이 검증되어야 하고, 운영환경 규모와 안정성을 고려한 아키텍처와 지속적으로 모델을 업데이트할 수 있는 자동화와 관리체계가 필요합니다.

Q2. 원활한 머신러닝을 위해서는 GPU 어느 정도 사양이상을 추천 하는지요?

GPU를 필요로 하는 모델이 단순하면 1장이 될 수도 있지만, Bert, GPT와 같이 Heavy한 Job은 수십 개 수백 개 GPU를 필요로 해서 상황마다 다를 것 같습니다.

Q3. 더 효율적으로 자원을 관리하는 가운데 데이터 사이언티스트와 개발자의 편의성을 높이는 방안으로 MLOps를 주목하게 되는데 특히 동시에 여러 AI/ML 프로젝트를 수행하는 경우에 MLOps의 이점은 무엇인가요?

MLOps는 이점은 개발라이프사이클을 단축하고 운영환경에 지속적으로 관리하고 개선하는데 이점을 두고 있습니다.

Q4. 머신러닝 시스템 관련하여 개발, 학습, 튜닝, 배포 등 환경 구성의 어려움을 지혜롭게 해결하고 극복할 수 있는 방법에 대해서 질문 드립니다.

MLOps도 체계라 문화적인 측면도 중요하지만, IT관점에서는 지원하는 시스템들을 잘 선별하여 적용해야 할 것 같습니다.

Q5. MLOps는 자원 확보, 데이터 준비, 개발 환경 마련 등이 자동화 기반으로

이루어진다는 것이지요?

모든 걸 자동화 하는 건 힘든 얘기이고, MLOps 플랫폼 혹은 클라우드 등을 활용하여 많은 부분에 있어 자동화 할 수 있는 부분을 반영하고자 합니다.

Q6. DataOps의 업무에 대해 질문 드립니다. 데이타옵스 업무 같은 경우 대부분 데이터 엔지니어의 업무의 일부분 아닌가요?

옙 맞습니다.

Q7. 머신러닝 혹은 딥러닝에 필요한 라이브러리(e.g. Tensorflow, PyTorch) 버전 업데이트가 이루어지면 어떻게 되나요?

비밀키 테이블은 따로 존재하지 않습니다. public data에 포함되어 있습니다. 다만 공격자는 그 값을 알 수가 없고요

Q8. MLOps는 모델 구현, 훈련, 배포 과정이 자동화 기반으로 이루어져 데이터사이언티스트와 개발자 모두 효율적으로 프로젝트를 수행할 수 있게 되는 것인가요?

모든 걸 자동화 하는 건 힘든 얘기이고, 모델개발과 운영에 필요한 자동화가 가능한 요소 중심으로 자동화합니다.

Q9. kubeflow가 쿠버네티스 환경에서 바로 MLOps를 지원하면 가장 이상적인 환경 같은데 기존 데이터 파이프라인을 지원하는 솔루션과 비교해서 단점은 없는 것인가요?

데이터 파이프라인과 ML 파이프라인은 다른 task인 것 같고요, Workflow를 자동화한다는 점은 유사하지만 목적이 다른 것 같습니다.

Q10. SCP가 GCP를 사용했을 때보다 Kubeflow를 더 잘 활용할 수 있는 게 있나요?

GCP가 여러 서비스들이 많기 때문에 장점이 많을 수 있겠지만, SCP에서는 Kubernetes 위 바로 오픈소스 Kubeflow 바로 구성 가능한 점과 기능을 확장한 Enterprise 서비스가 출시되면, 부분적으로 더 잘 활용할 수 있는 부분이 있을 것 같습니다.

Q11. 클러스터 구성과 쿠버플로우가 기 탑재된 배포이미지를 미리 생성해서 배포가 가능한지 궁금합니다.

기술적으로는 가능할 것 같으나, 클라우드 상품이 Kubernetes Engine, Container Registry 등 별도로 과금/미터링 구조로 되어 있어 미리 생성해서 배포하는 구조로 서비스는 현재 없습니다.

Q12. kubeflow service의 보안 부분도 궁금합니다.

기본적으로 VM 인프라 및 Kubernetes 보안을 준수하고 있고, Kubeflow 서비스는 Kubeflow 구성모듈 보안 패치, 제공하는 Tensroflow, PyTorch 등 ML Framework 이미지 보안 등이 포함됩니다.

Q13. 혹시 쿠버플로우 버전 업데이트가 나오면 어느 정도 주기를 가지고 scp 버전 업데이트를 진행하나요?

최근 Kubeflow는 5~6개월 마다 새로운 버전을 내는데요, 향후 SCP Kubeflow + 2개월을 목표로 하고 있습니다.

Q14. 타사 클라우드의 쿠버네티스 엔진들과 비교했을 때, scp 만의 장점은 무엇이 있을까요?

아무래도 Enterprise 기업을 목표로 하다 보니 Managed Service와 보안 패치 등 보안관리가 장점 일 것 같습니다.

Q15. hyper parameter tuning시 tensorboard 같은 monitoring 도구도 지원 가능한지요?

네, Docker Image 자체에 탑재하여 지원 가능합니다.

Q16. 혹시 Serving에 대한 기능도 지원하나요??

Kubeflow 기본 구성요소인 KFServing 기능을 사용합니다.

Q17. Kubeflow를 사용하려면 먼저 삼성 클라우드 사용을 신청해야 하는지 궁금합니다.

Samsung Cloud Platform 사용을 신청해야 하는데, 기업 고객 대상이라 개인 사용에는 제한이 있을 수 있습니다.

Q18. 이미 kubernetes 기반 CI/CD pipeline이 있는 경우에, kubeflow 연동이 주는 강점이 있을까요?

CI/CD는 주로 소스코드 기반 자동화이고, 모델 중심의 Workflow 자동화를 추구하는 분산모델 학습, 튜닝, 서빙, 등 ML 영역의 고유 특성 기능을 연동할 수 있는 장점이 있을 것 같습니다.

Q19. Kubeflow는 오픈소스 기반이라 아무나 사용가능한지요?

Kubeflow는 여러 오픈소스로 구성되어 있어 관련 오픈소스 라이선스에 해당하는 정책을 준수하는 범위에서 사용 가능할 것으로 보입니다.