

MLOps: introduzione ed esempi



Programma serata

- Prima parte: Introduzione MLOps
- Seconda parte: Esempio pratico di libreria MLOps: **mlflow**



MLOps: definizione

Insieme di pratiche per la messa in produzione di modelli di machine learning in maniera affidabile ed efficiente.

Applicazione concetti **DevOps** al mondo del **machine learning**.

In ambito ingegneria del software con DevOps si intende un insieme di pratiche per sviluppatori e esperti IT aventi lo scopo di efficientare lo sviluppo e la messa in produzione di strumenti informatici mantenendo alta qualità del codice scritto.

<https://papers.nips.cc/paper/2015/file/86df7dcfd896fcdf2674f757a2463eba-Paper.pdf>

Hidden Technical Debt in Machine Learning Systems

D. Sculley, Gary Holt, Daniel Golovin, Eugene Davydov, Todd Phillips
{dsculley, gholt, dgg, edavydov, toddphillips}@google.com
Google, Inc.

Dietmar Ebner, Vinay Chaudhary, Michael Young, Jean-François Crespo, Dan Dennison
{ebner, vchaudhary, mwyong, jfcrespo, dennison}@google.com
Google, Inc.

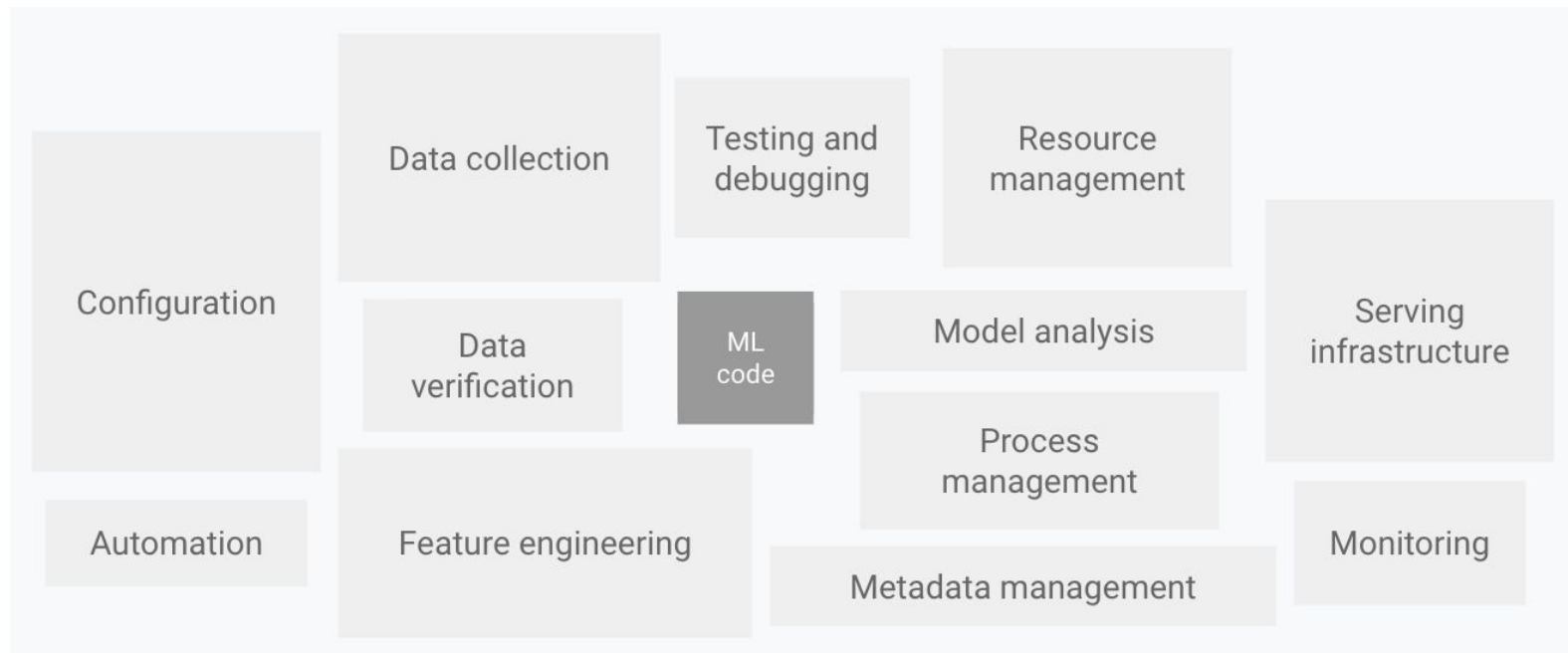
Abstract

Machine learning offers a fantastically powerful toolkit for building useful complex prediction systems quickly. This paper argues it is dangerous to think of these quick wins as coming for free. Using the software engineering framework of *technical debt*, we find it is common to incur massive ongoing maintenance costs in real-world ML systems. We explore several ML-specific risk factors to

<https://papers.nips.cc/paper/2015/file/86df7dcfd896fcdf2674f757a2463eba-Paper.pdf>

ML
code

<https://papers.nips.cc/paper/2015/file/86df7dcfd896fcdf2674f757a2463eba-Paper.pdf>



DevOps vs MLOps

Cosa implica il considerare modelli di machine learning come strumenti software?



Data

+



Model

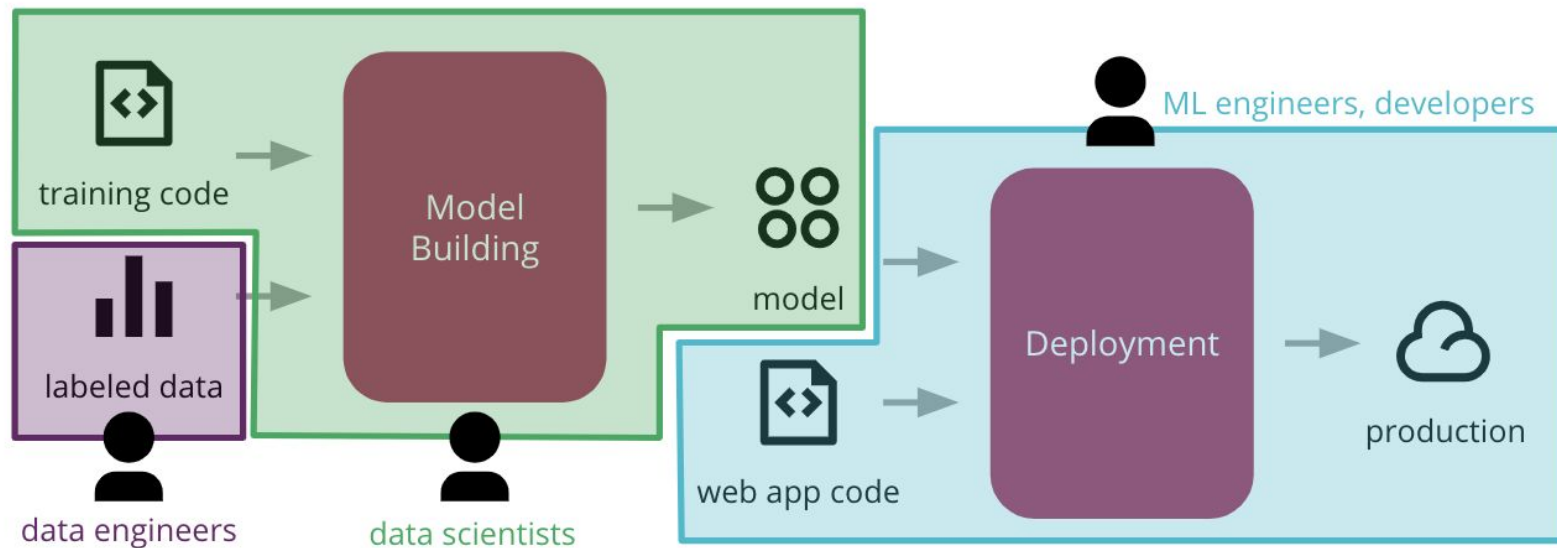
+



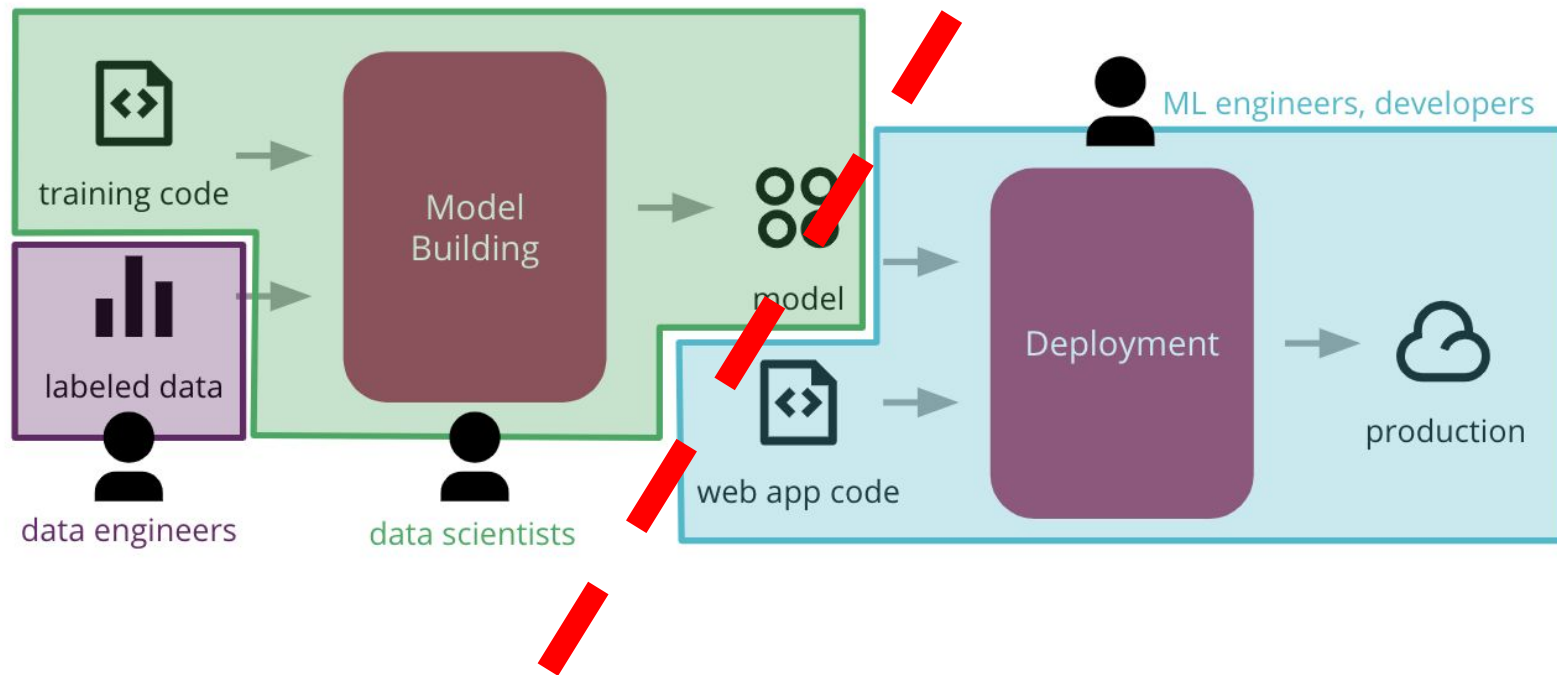
Code

<https://martinfowler.com/articles/cd4ml.html>

Ruoli

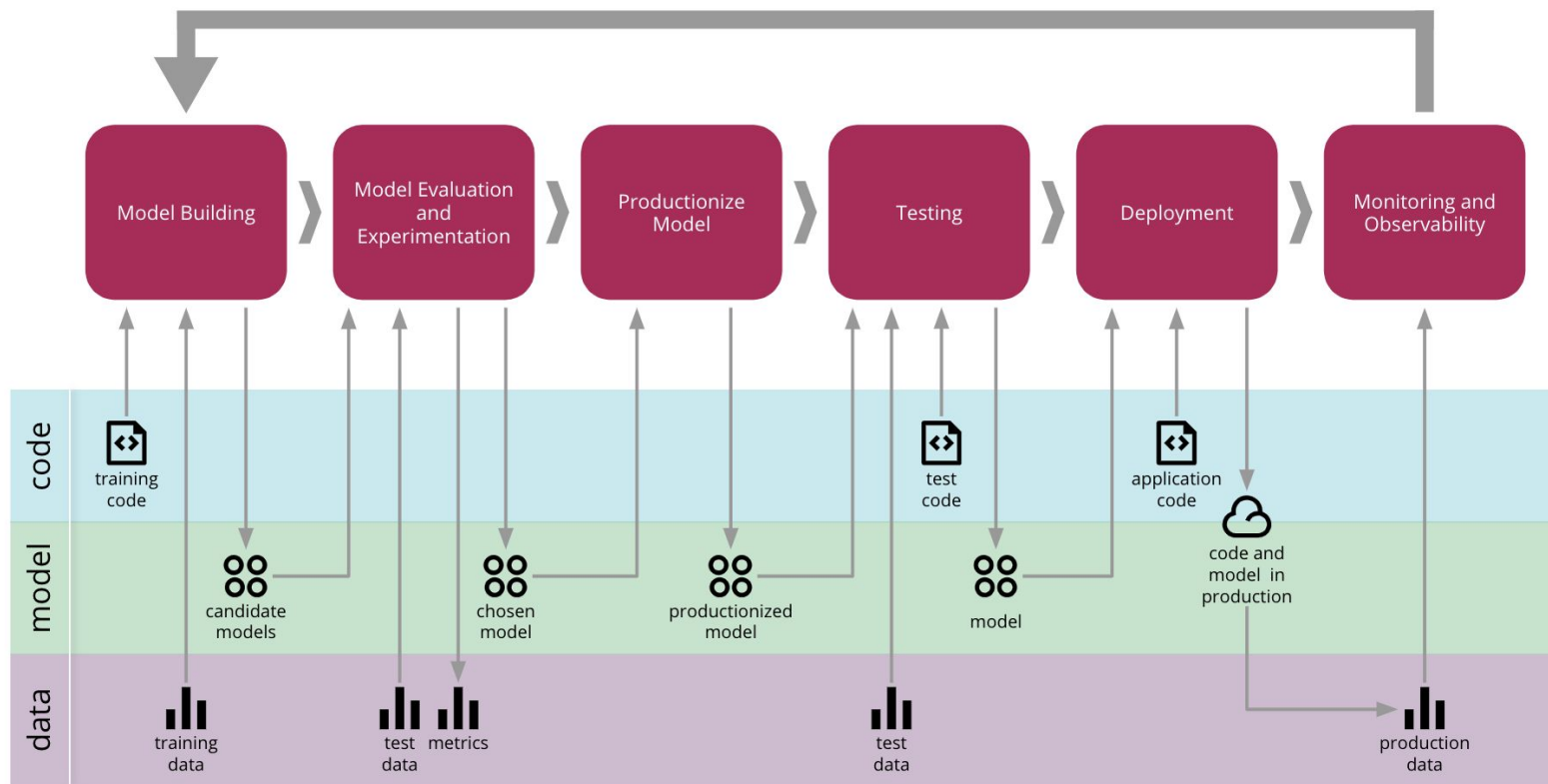


Ruoli



<https://martinfowler.com/articles/cd4ml.html>

Machine learning in produzione



Il cuore del DevOps: CI/CD

Continuous Integration/ Continuous Delivery

Facilitare l'interazione tra sviluppo e produzione dando la possibilità di migliorare continuamente codice tramite piccoli interventi che vengono automaticamente messi in produzione.

Il cuore del DevOps: CI/CD

Continuous Integration/ Continuous Delivery

Facilitare l'interazione tra sviluppo e produzione dando la possibilità di migliorare continuamente codice tramite piccoli interventi che vengono automaticamente messi in produzione.

Piccoli interventi → Affidabili, riproducibili e utilizzabili in produzione in qualunque momento

Il cuore del DevOps: CI/CD

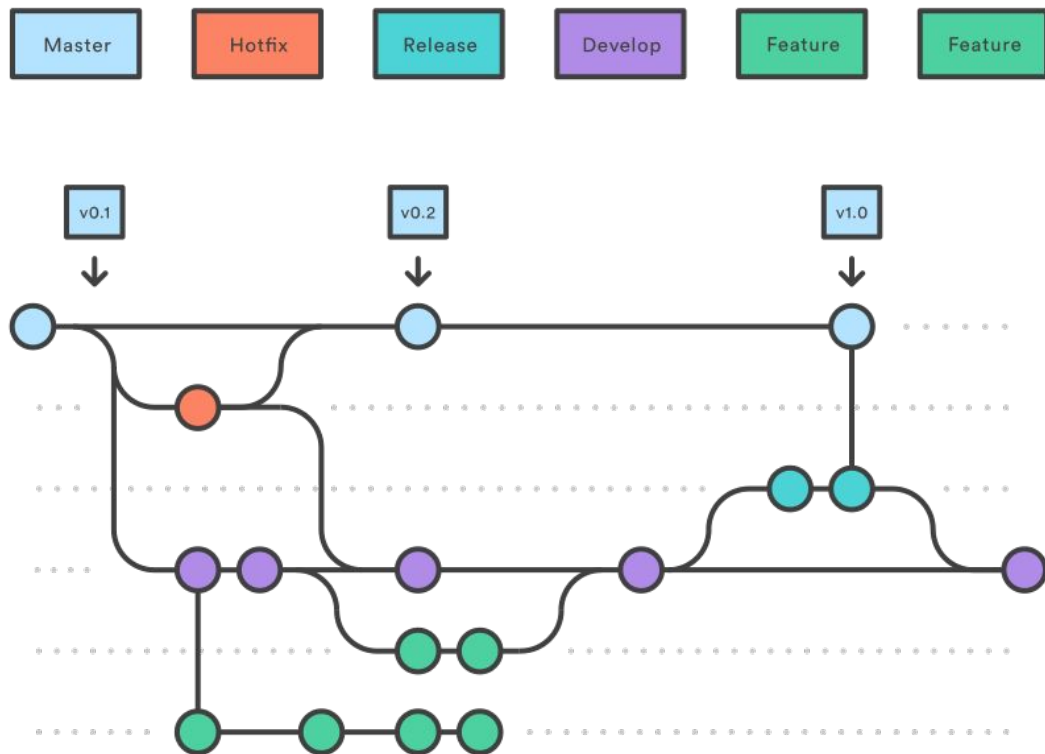
Continuous Integration/ Continuous Delivery

Pratiche piú importanti:

1. **Version control**
2. **Testing**

Primo passo per il CI/CD: version control

Primo passo per il CI/CD: version control

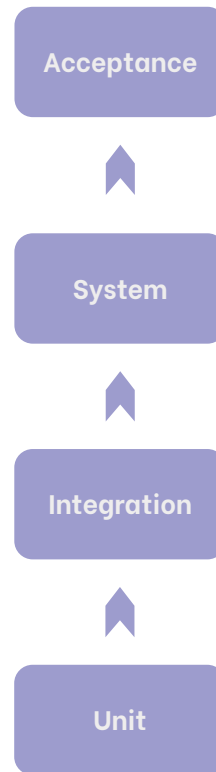


Secondo passo per il CI/CD: testare, testare, testare

Ogni piccola modifica al codice deve essere sicura

Non deve rompere nulla (e nel caso rompa qualcosa si deve essere immediatamente in grado di tornare all'ultima versione funzionante)

Tipologie di test diverse a seconda di cosa si stia testando.



Cosa vuol dire fare versioning e testing di modelli ML?



Code

<https://martinfowler.com/articles/cd4ml.html>

Cosa vuol dire fare versioning e testing di modelli ML?



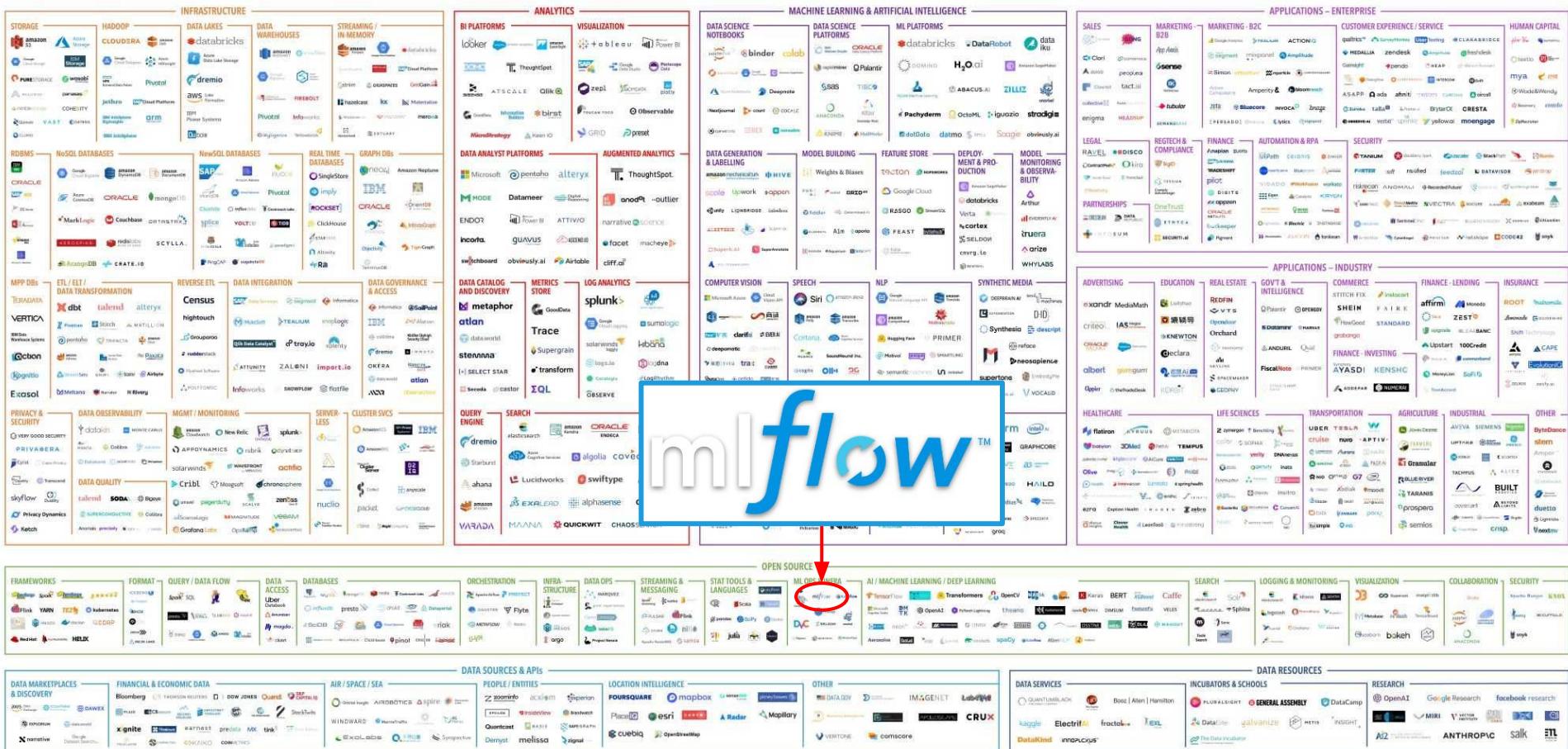
<https://martinfowler.com/articles/cd4ml.html>

Il mondo MLOps

Mercato MLOps in continua evoluzione. Nuovi prodotti e soluzioni sviluppati sia da grandi compagnie (Google, Amazon, etc) che da startups.

Secondo Deloitte nel 2025 il mercato MLOps avrà un valore di 4 miliardi di dollari.

MACHINE LEARNING, ARTIFICIAL INTELLIGENCE, AND DATA (MAD) LANDSCAPE 2021

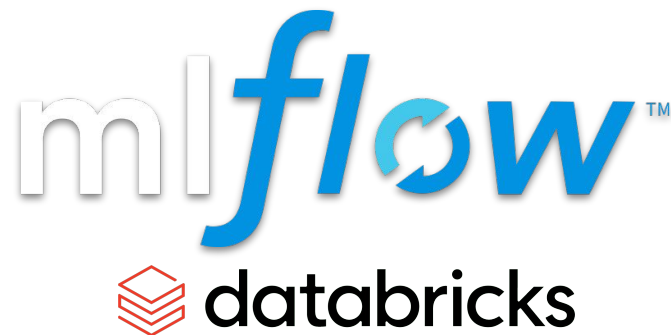


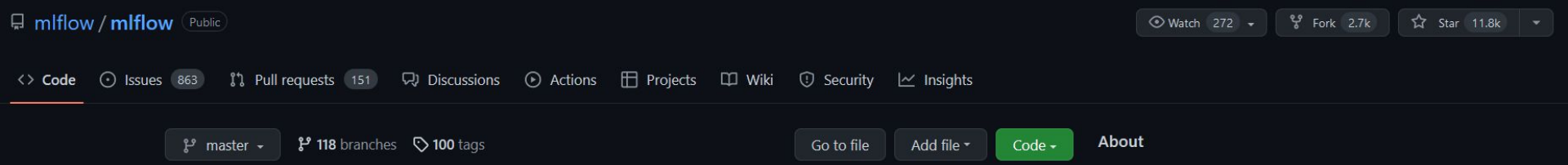
mlflow

Piattaforma open source per la gestione del ciclo vita del machine learning. Permette di:

- Catalogare esperimenti e di riprodurli
- Organizzare registri di modelli centralizzati
- Impacchettamento e messa in produzione modelli

Sviluppato e mantenuto da databricks, un bel po' di ore uomo dedicate al progetto

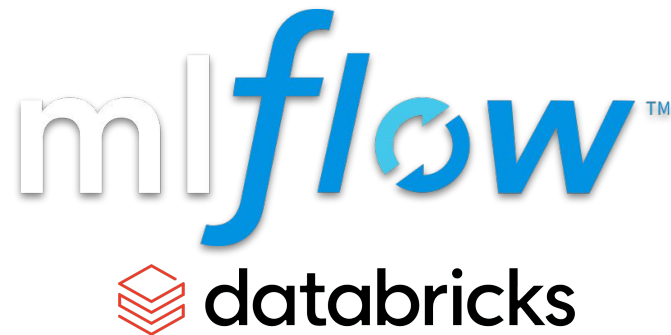




Piattaforma open source per la gestione del ciclo vita del machine learning. Permette di:

- Catalogare esperimenti e di riprodurli
- Organizzare registri di modelli centralizzati
- Impacchettamento e messa in produzione modelli

Sviluppato e mantenuto da databricks, un bel po' di ore uomo dedicate al progetto

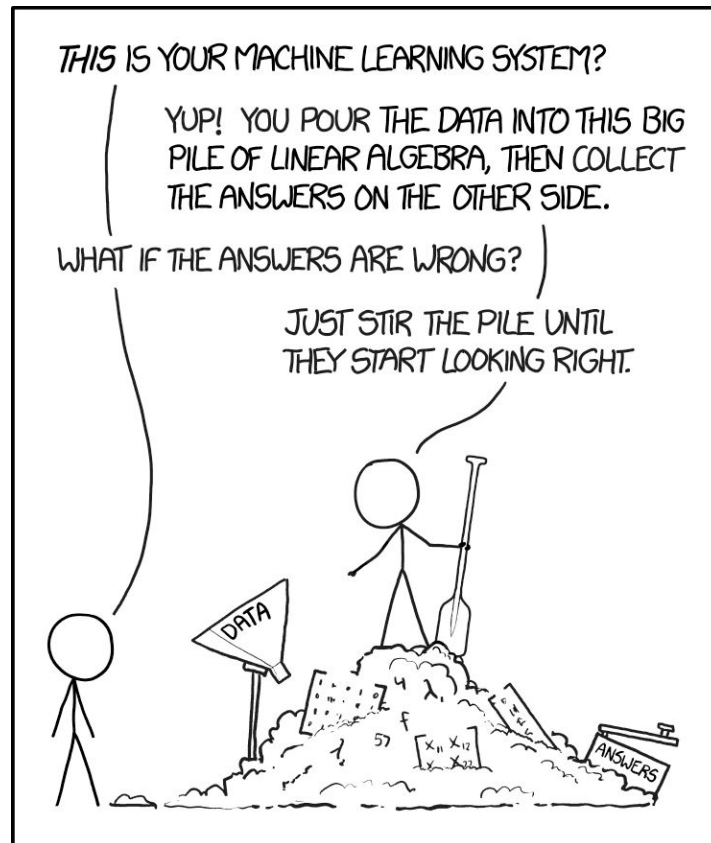


Gestione esperimenti ML

Lo sviluppo di modelli di machine learning sta diventando sempre più associato a **'trial and error'**

→ Problemi di riproducibilità e potenziali perdite di tempo.

Gestire esperimenti ML vuol dire essere in grado di tracciare metriche ottenute nel tempo e di riprodurre i modelli con cui sono state ottenute.

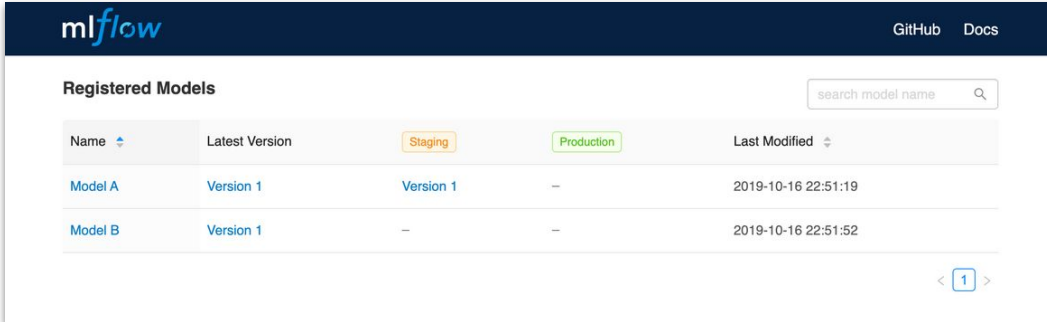


xkcd.com

Registri di modelli

Versioning di modelli in produzione può essere effettuato utilizzando registri di modelli.

Lo scopo di tali registri e' di tracciare versioni di modelli in pre e post produzione permettendo ad esempio fallback, analisi post-hoc, confronti tra versioni diverse, etc.



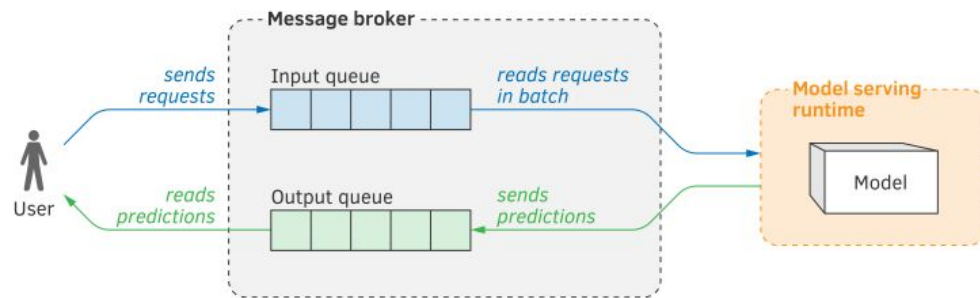
The screenshot shows the 'Registered Models' page in the mlflow web interface. At the top, there's a dark blue header with the 'mlflow' logo on the left and 'GitHub' and 'Docs' links on the right. Below the header, the title 'Registered Models' is displayed on the left, and a search bar with the placeholder 'search model name' is on the right. The main content is a table with the following columns: 'Name', 'Latest Version', 'Staging', 'Production', and 'Last Modified'. There are two rows of data: 'Model A' and 'Model B'. 'Model A' has 'Version 1' in the 'Latest Version' column, 'Version 1' in the 'Staging' column, a hyphen in the 'Production' column, and a timestamp '2019-10-16 22:51:19'. 'Model B' has 'Version 1' in the 'Latest Version' column, a hyphen in the 'Staging' column, a hyphen in the 'Production' column, and a timestamp '2019-10-16 22:51:52'. At the bottom right of the table, there are navigation controls: a left arrow, a box containing the number '1', and a right arrow.

Name	Latest Version	Staging	Production	Last Modified
Model A	Version 1	Version 1	—	2019-10-16 22:51:19
Model B	Version 1	—	—	2019-10-16 22:51:52

Messa in produzione

Impacchettare un modello di machine learning all'interno di uno strumento software.

Modello deve essere in grado di dialogare all'interno di una soluzione esistente tramite, ad esempio, un'API.



'Machine Learning Engineering', A. Burkov

Demo mlflow

Nel corso di questa demo:

1. Alleneremo un modello su un dataset giocattolo (LendingClub)
2. Ottimizzeremo i parametri del modello usando mlflow per tracciare i vari esperimenti.
3. Salveremo il modello in un registro.
4. Impacchetteremo il modello in una soluzione di produzione.

Limiti di mlflow

Nonostante venga definito un tool end-to-end mancano ancora diverse features per quanto riguarda la parte di messa in produzione. E' invece già molto avanzato per quanto riguarda la gestione esperimenti.

Le loro librerie per impacchettare modelli producono output decisamente pesanti rispetto a soluzioni ottenute 'a mano'





Thanks for Reading

Feel free to contact us:



www.clearbox.ai



support@clearbox.ai



[@ClearboxAI](https://twitter.com/ClearboxAI)