

# Tests Logiciels - Master MS2D

Christophe Brun

Campus Saint-Michel IT

21 septembre 2023



# Table des matières

- 1 Programme du module
- 2 Généralités
- 3 Tests Unitaires
- 4 Le mutation testing
- 5 Le BDD
- 6 Le TDD
- 7 Tests assistés par l'IA
- 8 Les tests d'intégration
- 9 Intégration Continue
  - Généralité
  - GitHub Action
  - Jenkins
  - GitLab CI
  - Conclusion

# Tests Logiciels

Compétences acquises au cours des 3 jours du module

- Savoir développer et mettre en place des tests unitaires sur une application.
- Savoir développer et mettre en place des tests d'intégration sur une application.
- Savoir configurer un pipeline d'intégration continue sur une application.



# Tests Logiciels

Le programme des 3 jours du module

## Programme :

### ① Les tests unitaires

- Qu'est-ce qu'un test ?
- Les tests unitaires
- Les bonnes pratiques
- Le Test Driven Development
- Le code coverage
- Tests avec langage naturel

### ② Les tests d'intégration

- Les tests d'intégration
- Le fonctionnement
- Les bonnes pratiques

### ③ L'intégration continue

- Mise en place d'une plateforme d'intégration continue (GitLab CI)
- Conteneurisation d'une application (API)
- Configuration d'un pipeline de tests

# Intervenant sur le module Tests Logiciels

Christophe Brun, CTO d'In France

- 1<sup>ère</sup> année d'intervenant à Saint-Michel 😇.
- 7 ans de conseil en développement au sein d'SSII .
- 6 ans de conseil en développement à mon compte PapIT.
- Directeur technique et associé d'[In France](#).
- Passionné !



# L'histoire du testing

- ISTQB, l'International Software Testing Qualifications Board a été fondée en 1998<sup>1</sup>
- Dans son livre Extreme Programming Explained, Kent Beck parle de Test-first Programming en 1999
- Les standards modernes datent de la fin des années 90, début des années 2000
- JUnit, le framework de test le plus utilisé en Java date de 2002<sup>2</sup>
- Début du BDD (Behavior-Driven Development) avec JBehave, censé remplacer JUnit en utilisant le behavior au lieu de test, date de 2003<sup>3</sup>

---

<sup>1</sup>ISTQB, About Us, <https://www.istqb.org/about-us/who-we-are>

<sup>2</sup>Steven J Zeil, Unit Testing Frameworks,

<https://www.cs.odu.edu/~zeil/cs350/latest/Public/junit/index.html>

<sup>3</sup>Cucumber, <https://cucumber.io/docs/bdd/history/>

# Qu'est-ce qu'un test ?

Définition de l'International Software Testing Qualifications Board et IBM

L'ISTQB définit les termes suivants dans son glossaire<sup>4</sup> :

**Test** : Un ensemble d'un ou plusieurs cas de tests.

**Cas de test** : Un ensemble de conditions préalables, de données d'entrée, d'actions (le cas échéant), de résultats attendus et de postconditions, élaboré sur la base des conditions de test.

Selon IBM<sup>5</sup> :

“Le test logiciel est le processus qui consiste à évaluer et à vérifier qu'un produit ou une application logicielle fait ce qu'il ou elle est censé(e) faire.”

---

<sup>4</sup>ISTQB, Glossaire des termes utilisés en tests de logiciels,

[https://www.cftl.fr/wp-content/uploads/2018/10/Glossaire-des-tests-logiciels-v3\\_2F-ISTQB-CFTL-1.pdf](https://www.cftl.fr/wp-content/uploads/2018/10/Glossaire-des-tests-logiciels-v3_2F-ISTQB-CFTL-1.pdf)

<sup>5</sup>IBM, Qu'est-ce que le test logiciel ?,

<https://www.ibm.com/fr-fr/topics/software-testing>

# Qu'est-ce qu'un test unitaire ?

Définition de la taverne du testeur<sup>6</sup>

Il obéit au principe “F.I.R.S.T.” :

- **Fast** : S'exécute rapidement et est donc automatisé
- **Isolated** : Est indépendant des facteurs externes et des autres tests
- **Repeatable** : Isole les bugs automatiquement
- **Self-validating (autonome)** : N'est pas ambiguë (pas sujet à interprétation, ne demande pas une action manuelle pour vérifier le résultat)
- **Timely (tôt)** : Écrit en même temps que le code (même avant en TDD)

Si le test échappe à un de ces principes, il n'est probablement pas unitaire.

Pour isoler les bugs automatiquement, un test unitaire doit tester le code unitairement, et isolément. Il doit donc être écrit dans le but de tester la logique d'une ligne de code et si un test unitaire échoue vous pouvez connaitre la ligne de code incriminée.

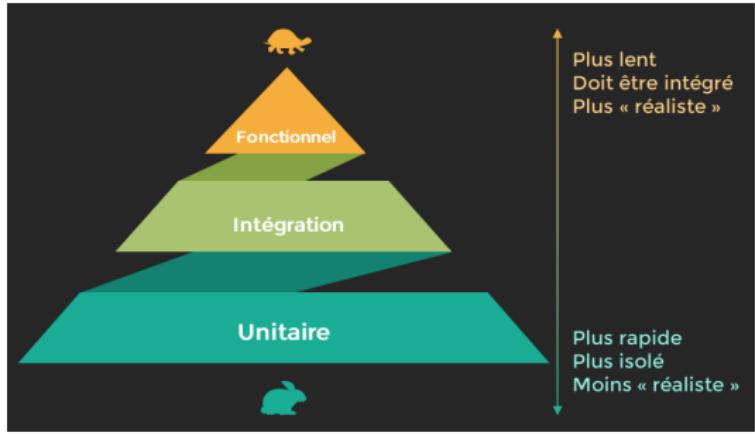
<sup>6</sup>Mais c'est quoi un test unitaire ?, <https://lataverne du testeur.fr/2018/04/11/mais-cest-quoi-un-test-unitaire/>

# Testing, les frameworks de test unitaire

- UnitTest, le framework de test standard de Python
- PyTest, un framework pour tout faire en Python
- JUnit, le framework de test le plus utilisé en Java
- PHPUnit, le framework de test standard de PHP
- Google Test, pour le C++
- Jest pour JS, Babel, pour TypeScript, Node, React, Angular, Vue et plus encore
- etc

# La Pyramide des tests

Différents types de tests peuvent être identifiés. La classification la plus classique étant la suivante<sup>7</sup> :



Mais d'autres valent le coup d'être découvertes...

<sup>7</sup>OPENCLASSROOMS, Testez votre code

Java pour réaliser des applications de qualité, <https://openclassrooms.com/fr/courses/6100311-testez-votre-code-java-pour-realiser-des-applications-de-qualite/6616481-decouvrez-les-tests-dintegration-et-les-tests-fonctionnels>

# Testing

- Un programme a pour entrée le standard input, et sorties les standard output et standard error, ce sont les standard streams
- Un programme se termine avec un code retour, le plus souvent un entier différent de 0 en cas de problème
- Les frameworks de tests retournent 3 statuts, OK, FAILED et ERROR
- Les OK si aucune erreur n'a lieu et FAILED en cas d'erreur d'assertion

```
christophe@christophe-HKD-WXX:~/Documents/Campus St Michel IT$ cat test_stdout_stderr.py
import sys

def test_hello():
    print("Hello testing")
    print("stderr during testing", file=sys.stderr)
    assert False

christophe@christophe-HKD-WXX:~/Documents/Campus St Michel IT$ python3 -m pytest test_stdout_stderr.py 1> /dev/null
christophe@christophe-HKD-WXX:~/Documents/Campus St Michel IT$ python3 -m pytest test_stdout_stderr.py 2> /dev/null
=====
platform linux -- Python 3.11.4, pytest-7.2.1, pluggy-1.8.0+repack
rootdir: /home/christophe/Documents/Campus St Michel IT
collected 1 item

test_stdout_stderr.py F [100%]

=====
FAILURES =====
test_hello

def test_hello():
    print("Hello testing")
    print("stderr during testing", file=sys.stderr)
>     assert False
E     assert False

test_stdout_stderr.py:6: AssertionError
----- Captured stdout call -----
Hello testing
----- Captured stderr call -----
stderr during testing
=====
short test summary info
FAILED test_stdout_stderr.py::test_hello - assert False
1 failed in 0.10s
christophe@christophe-HKD-WXX:~/Documents/Campus St Michel IT$ echo $?
1
```

# Brief sur les outils de test logiciel

- Les frameworks de test retournent 3 statuts, OK, FAILED et ERROR .
- OK si aucune erreur n'a lieu et FAILED en cas d'erreur d'assertion, `AssertionError` en Python et Java.
- Pas de standard universellement accepté mais un format domine, le XML JUnit. Un XML le définit par la grammaire <https://windyroad.com.au/dl/Open%20Source/JUnit.xsd>.
- Vient de l'écosystème Java avec le package du même nom, JUnit, mais est présent dans la plupart des frameworks de test comme PHPUnit, Pytest.
- L'interopérabilité entre les outils est permise par cette XSD commune, mais pas plus de contrainte. Par exemple, l'interopérabilité entre les frameworks de test et les outils de CI/CD .
- Certains outils, souvent des solutions propriétaires, rechignent toujours à exporter un JUnit contenant les résultats de test pour fermer leur environnement.

# L'assertion error

En Python

L'instruction `assert` vérifie une condition. Si la condition est vraie, cela ne fait rien et votre programme continue simplement à s'exécuter. Mais si la condition d'assertion est fausse, elle lève une exception `AssertionError`.

```
assert 23 % 2 == 0, "Le restant de la division est différent de 0"
```

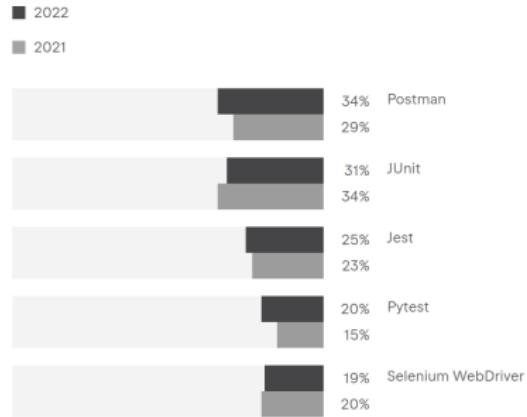
Étant toujours fausse, le programme crash.

```
chrichri@chrichri-HKD-WXX:~$ python3 -c 'assert 23 % 2 == 0, "Le restant de la
division est différent de 0"'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AssertionError: Le restant de la division est différent de 0
```

# Pourquoi Pytest pour le testing

“pytest is a mature full-featured Python testing tool that helps you write better programs.<sup>8</sup>”

Pytest est le framework de test en Python le plus utilisé selon les sondages de JetBrains<sup>9</sup>. Seuls JUnit et Pytest sont pour tous usages, les autres sont orientés web.



<sup>8</sup> pytest: helps you write better programs , <https://docs.pytest.org>

<sup>9</sup> JetBrains, Which test frameworks ,

<https://www.jetbrains.com/lp/devcosystem-2022/testing/>

# Pytest

## Rédiger un test

- Un module de test Pytest est un module Python préfixé par `test_`.
- Toutes les méthodes préfixées par `test_` sont exécutées par Pytest. Qu'elles soient dans une classe ou non. Les autres méthodes ne sont exécutées uniquement si les tests les appellent.

Ici par exemple, la précédente assertion est intégrée dans une méthode nommée `test_divide` dans le module de test `test_division.py`.

```
def test_divide(): # Un test Pytest est préfixé par test_
    assert 23 % 2 == 0, "Le restant de la division est différent de 0."
```

# Pytest

## Lancer les tests

Lancer avec la commande `python -m pytest test_divison.py`, Pytest affiche le rapport de test.

```
...
def test_divide(): # Un test Pytest est préfixé par test_
> assert 23 % 2 == 0, "Le restant de la division est différent de 0."
E AssertionError: Le restant de la division est différent de 0.
E assert (23 % 2) == 0

test_divison.py:2: AssertionError
...
```

De très utiles et nombreuses options peuvent compléter cette ligne de commande. Pour les découvrir, lancez `python -m pytest --help` et “RTFM”.

# Pytest

## Les tests paramétriques

Les tests paramétriques sont des tests qui prennent un ensemble de paramètres en entrées.

Ils permettent de tester plusieurs cas avec un seul test.

Le rapport génère un cas de test par paramètre. Il est donc plus détaillé et permet de trouver les tests en échec plus facilement que si l'assert était dans une boucle, ce qui ne donne qu'un statut OK ou Fail dans le rapport.

```
import pytest
...
@pytest.mark.parametrize("dividend", range(100)) # Paramétrage du test
def test_divide_from_0_to_99(dividend): # Doit avoir un argument présent dans le
    # paramétrage
    assert dividend % 2 == 0, "Le restant de la division est différent de 0."
```

# Pytest

## Les tests paramétriques

Génère 100 cas de tests. Met en évidence les dividendes dont le restant de la division par 2 est différent de 0, ici 1 par exemple.

```
collecting ... collected 100 items

test_divison.py::test_divide_from_0_to_99[0] PASSED [ 1%]
test_divison.py::test_divide_from_0_to_99[1] FAILED [ 2%]
test_divison.py:7 (test_divide_from_0_to_99[1])
1~!= 0

Expected~:0
Actual ~:1
<Click to see difference>

dividend = 1

    @pytest.mark.parametrize("dividend", range(100)) # Paramétrage du test
    def test_divide_from_0_to_99(dividend): # Doit avoir un argument présent dans
        le paramétrage
> assert dividend % 2 == 0, "Le restant de la division est différent de 0."
E AssertionError: Le restant de la division est différent de 0.
E assert (1 % 2) == 0
```

# Pytest

Plantage dans un test, quel statut?

Ce test crash avant l'assert.

```
def test_fail_or_error(): # Une erreur donne un fail ou error?  
    dividende = 23 / 0  
    assert dividende % 2 == 0, \  
        "Le restant de la division est différent de 0."
```

Malgré l'absence d'assertionError, le test est en échec et non en erreur.

```
test_divison.py::test_fail_or_error FAILED [100%]  
test_divison.py:12 (test_fail_or_error)  
def test_fail_or_error(): # Une erreur donne un fail ou error?  
>     dividende = 23 / 0  
E ZeroDivisionError: division by zero  
  
test_divison.py:14: ZeroDivisionError
```

Pour éviter les faux négatifs, un test doit tendre, tant que faire se peut, vers un assert. Pour cela pensez à utiliser les fonctions parametrize et fixture.

# Pytest

## Les fixtures

Cf. [https://github.com/St-Michel-IT/testing/blob/main/test\\_customer\\_database.py](https://github.com/St-Michel-IT/testing/blob/main/test_customer_database.py)

Un `return` ou un `yield` envoie l'objet au test dans l'état voulu.

```
def customer_without_table():
    """
    ...
    ...
    customer = Customer() # Avant le test, c'est le setup
    yield customer # Un yield évite de sortir de la fonction
    customer.con.close() # Après le test, le teardown
```

Le test n'a qu'une seule ligne, qu'un `assert` l'échec ne pourrait venir que de là.

```
def test_instantiation(customer_without_table):
    """
    ...
    ...
    assert isinstance(customer_without_table.con, Connection)
```

En cas de plantage dans la fixture, i.e., avant ou après le test, la sanction serait erreur et non échec.

Le rapport reflétera fidèlement le test et sera exempt de faux négatif.

# Pytest

Les fixtures, le moyen du pattern A.A.A<sup>10</sup>

Le pattern du A.A.A, Arrange, Act, Assert, est facile à implémenter avec les fixtures. Arrange et Act sont isolé dans la fixture, Assert seul est dans le test.

```
def customer_without_table():
    """
    ...
    """
    customer = Customer() # Arrange et Act dans le setup avant yield ou return
    yield customer
    customer.con.close() # Pas de nom en A, ils l'ont oublié?
```

Le test tend vers un assert quasi seul.

```
def test_instantiation(customer_without_table):
    """
    ...
    """
    assert isinstance(customer_without_table.con, Connection) # Assert
```

Le B.D.D. suit le pattern A.A.A sous un autre nom : Given-When-Then. Le langage Gherkin utilise les étapes Given-When-Then pour spécifier les comportements dans les scénarios.

<sup>10</sup> Arrange-Act-Assert: A Pattern for Writing Good Tests, <https://automationpanda.com/2020/07/07/arrange-act-assert-a-pattern-for-writing-good-tests/>

# Pytest

Exercice 1, écrire un test avec une fixture

**Exercice :** Écrivez votre premier test Pytest avec une fixture en respectant les exigences suivantes :

- Le test doit utiliser une fixture avec setup et teardown.
- Le test doit respect le pattern A.A.A .

Pour le setup et teardown, pensez à un fichier .

Pour être évalué, créez un seul repo contenant tous les exercices de ce cours.

# Pytest

## Le scope des fixtures

L'argument `scope` du décorateur `pytest.fixture` définit la durée de vie de la fixture. Il peut prendre 3 valeurs :

- `function` : La valeur par défaut si on ne met rien. La fixture est exécutée à chaque fonction de test `def test_...` qui l'appelle directement ou indirectement, donc les éventuels `setup` et `teardown` de cette dernière aussi.
- `module` : Une fois par module `test_....py`.
- `session` : Une seule fois durant la session de test quel que soit le nombre de modules et de tests exécutés.

```
@pytest.fixture(scope="function") # Scope de la fixture, par default function
def customer_without_table():
    """Connection to in memory database using the Customer class"""


```

Pour tester une API en étant sûr le token n'est pas périmé, on peut utiliser le scope `function` pour en avoir un nouveau à chaque appel.

Si préparer les conditions initiales, le `setup`, prend du temps, on évitera si possible de le répéter à chaque test avec les scopes `module`, `session`.

# Pytest

Le `conftest.py`

Il n'a qu'une seule particularité, c'est d'être importé automatiquement par Pytest lorsqu'il est présent dans le dossier courant des tests.

Il permet de factoriser les fixtures et les paramétrages de tests utilisés dans plusieurs modules de tests, car ces derniers seront automatiquement disponibles sans même un import dans le module.

```
./  
└── conftest.py  
└── test_no_directory.py  
└── unit  
    └── test_integration.py  
└── functional  
    └── test_functional.py
```

Pour tous ces tests, s'ils sont lancés depuis la racine avec la commande `pytest`, le `conftest.py` sera importé automatiquement.

PyCharm intègre par défaut Pytest comme lanceur de tests et fournit l'autocomplétion pour les fixtures du `conftest.py`.



# Pytest

## Le coverage

Pas de support natif du coverage par Pytest, il faut installer le plugin `pytest-cov`<sup>11</sup>.

Pour appeler le plugin, il faut passer en argument le module à tester et le(s) test(s) de ce dernier.

```
pytest --cov=\textcolor{flatgreen}{customer_database} ./test_customer_database.py
...
rootdir: /home/chrichri/Documents/Campus-St-Michel-IT/testing
plugins: cov-4.1.0
collected 6 items

test_customer_database.py ..... [100%]

----- coverage: platform linux, python 3.11.4-final-0 -----
Name Stmts Miss Cover
-----
customer_database.py 9 0 100%
-----
TOTAL 9 0 100%
```

<sup>11</sup>Welcome to `pytest-cov`'s documentation!,

# Pytest

## Le coverage

Coverage for **customer\_database.py**: 100%

9 statements 9 run 0 missing 0 excluded

« prev ^ index » next coverage.py v7.3.1, created at 2023-09-28 22:38 +0200

```
1 import sqlite3
2
3
4 class Customer:
5     """
6         Customer class containing all the method to interact with the customer table
7     """
8
9     def __init__(self, path=":memory:") -> None:
10         """
11             Connect to in memory database by default, or to a database file if
12             specified.
13         """
14         self.con = sqlite3.connect(path)
15
16     def create_table(self) -> None:
17         """
18             Create the customer table if not exists
19         """
20         self.con.execute("""
21             CREATE TABLE IF NOT EXISTS customer (
22                 id INT PRIMARY KEY NOT NULL,
23                 email TEXT NOT NULL
24             )
25         """)
26
27     def insert(self, customer_id: int, email: str) -> None:
28         """
29             Insert a new customer in the table.
30
31             :param customer_id: The customer id as an int
32             :param email: The customer email as a string
33         """
34         self.con.execute("""
35             INSERT INTO customer (
36                 id,
37                 email
38             ) VALUES (
39                 ?,
40             )""", (customer_id, email))
41         self.con.commit()
```

« prev ^ index » next coverage.py v7.3.1, created at 2023-09-28 22:38 +0200

L'option `--cov-report=html` permet de générer un rapport HTML plus détaillé qui met en lumière quelles parties du code sont couvertes par les tests et lesquelles ne le sont pas.

**Exercice :** Trouvez quel test du module [https://github.com/St-Michel-IT/testing/blob/main/test\\_customer\\_database.py](https://github.com/St-Michel-IT/testing/blob/main/test_customer_database.py) couvre quelle partie de ce code:

//github.com/St-Michel-IT/  
testing/blob/main/test\_  
**customer\_database.py** couvre  
quelle partie de ce code:

# Pytest

Le secret de la réussite

Pytest est un framework complet voir complexe.  
Mais quasi toutes les fonctionnalités auxquelles on peut penser sont déjà implémentées et décrites une documentation de qualité.

Comme avec toutes les grosses libraries, il faut avoir confiance en leur design et chercher dedans avant de réinventer la roue.

La liste des fonctionnalités est trop longue, nous venons juste d'en découvrir les principales.

Donc une fois encore, comme pour toutes les bonnes librairies à connaître, le secret est “**RTFM**” !



# Pytest

Travaux dirigés sur les tests unitaires

**Exercice 2 :** Toujours à partir de la librairie du repo

<https://github.com/St-Michel-IT/testing/>, où le module `customer_database.py` est testé par `test_customer_database.py`. Ajoutez une méthode qui modifie les données d'un client et les tests qui vont avec.

**Exercice 3 :** Toujours dans le même repo, le module `witness_number.py` est un début implémentation d'une généralisation du petit théorème de Fermat expliquée sur la chaîne Youtube Numberphile par Matt Parker<sup>12</sup>. Cette librairie n'est pas déjà libre sur le web. Finissons son développement, en implémentant toutes les fonctionnalités de la vidéo de M. Parker avec des standards de qualité élevés grâce à nos connaissances en testing.

---

<sup>12</sup>Numberphile, Witness Numbers (and the truthful 1,662,803),  
[https://www.youtube.com/watch?v=\\_MscGSN5J6o](https://www.youtube.com/watch?v=_MscGSN5J6o)

# Mutation testing

Vérifier la qualité des tests unitaires

Imaginez un test sans assert, il ne fait qu'exécuter le code. Tout le code est couvert, mais le test ne sert à rien.

```
def test_fibonacci():
    fibonacci()
```

Quel est le coverage ?

# Mutation testing

Vérifier la qualité des tests unitaires

Imaginez un test sans assert, il ne fait qu'exécuter le code. Tout le code est couvert, mais le test ne sert à rien.

```
def test_fibonacci():
    fibonacci()
```

Quel est le coverage ? Il peut être de 100%. Encore une fois cette métrique n'est pas suffisante pour juger de la qualité des tests.

Le mutation est une étape qui intervient **quand tous les tests unitaires passent uniquement**. Cette étape consiste à modifier le code source pour voir si les tests échouent. C'est un raisonnement par l'absurde. Ils doivent en effet échouer pour prouver qu'ils testent le comportement du code et ne font pas que l'exécuter.

# Mutation testing

Fonctionnement des librairies comme `mutmut`<sup>13</sup>

La librairie de mutation essaie de modifier le code avec par exemple les règles suivantes :

- Changer les opérateurs mathématiques, comme `+` en `-`, `>` en `>=`
- Changer les opérateurs logiques : `and` en `or` et inversement
- Intervertir les mots-clés, comme `True/False`, `in/not in`
- Intervertir `copy` et `deepcopy`
- Remplacer `""` par `None`
- Changer les valeurs numériques en ajoutant `1`
- Changer les valeurs des chaînes de caractères en ajoutant `"xx"`
- Changer les noms des arguments des fonctions en ajoutant `"xx"`

---

<sup>13</sup> `mutmut` - python mutation tester, <https://mutmut.readthedocs.io/en/latest/>

# Mutation testing

Exemple avec mutmut

Dans le dossier `mutmut_fib` il y a 11 tests unitaires qui passent :

```
$ python -m pytest tests/test_fib.py
=====
platform linux -- Python 3.11.6, pytest-7.4.2, pluggy-1.3.0
rootdir: /home/chrichri/Documents/Campus-St-Michel-IT/testing/mutmut_fib
plugins: cov-4.1.0
collected 11 items

tests/test_fib.py ..... [100%]

===== 11 passed in 0.04s =====
```

Quand un mutant est détecter par les tests, il est “tué”. Les “survivants” indiquent que les tests ne sont pas suffisants. Ici `mutmut` crée 5 mutants, donc 5 versions différentes de la fonction `mutmut_fib.src.fib.fibonacci`, tous tués.

```
venv) chrichri@chrichri-HKD-WXX:~/Documents/Campus-St-Michel-IT/testing/mutmut$ mutmut show 3
--- src/fib.py
+++ src/fib.py
@@ -1,6 +1,6 @@
def fibonacci(n: int) -> int:
    """Get the n-th Fibonacci number"""
- a, b = 0, 1
+ a, b = None
    for _ in range(n-1):
        a, b = b, a + b
    return a
```

# Mutation testing

Example avec mutmut

```
$ mutmut run  
- Mutation testing starting -
```

These are the steps:

1. A full test suite run will be made to make sure we can run the tests successfully and we know how long it takes (to detect infinite loops for example)
2. Mutants will be generated and checked

Results are stored in .mutmut-cache.

Print found mutants with 'mutmut results'.

Legend for output:

🦋 Killed mutants.	The goal is for everything to end up in this bucket.
⏰ Timeout.	Test suite took 10 times as long as the baseline so were killed.
🤔 Suspicious.	Tests took a long time, but not long enough to be fatal.
😢 Survived.	This means your tests need to be expanded.
🚫 Skipped.	Skipped.

1. Running tests without mutations

⌚ Running...Done

2. Checking mutants

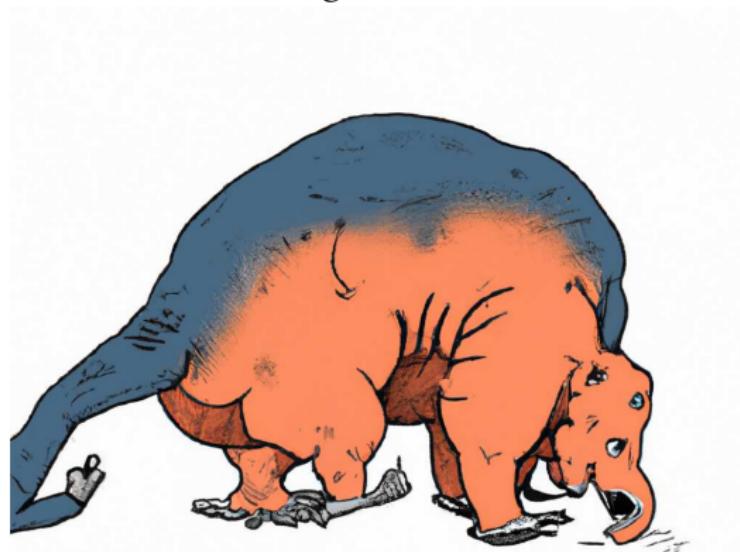
⌚ 5/5 🦋 5 ⏳ 0 🤔 0 😢 0 🚫 0

# Mutation testing

## Conclusion

Un rapport de test unitaire devrait contenir :

- Les rapport de test avec les résultats des tests unitaires
- Le rapport de test coverage
- Le rapport de mutation testing



# Tests avec langage naturel

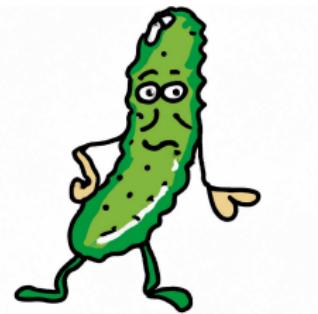
A.K.A le BDD

Les slides qui suivent sont truffés de biais négatifs sur le BDD suite à de mauvaises expériences 😅.

Le BDD est le sigle de Behavior-Driven Development.

Vous remarquerez qu'il n'y a ici aucune mention liée au testing?

Alors pourquoi est-il régulièrement associé au testing ?



Parce que le BDD est un outil de communication entre les développeurs et les métiers qui permet à ceux qui spécifient le produit de le décrire par rapport au comportement (behavior) attendu. Le tout dans une syntaxe proche du langage naturel. Ce langage peut être utilisé pour générer des tests. On pourrait presque finir par croire que le métier peut écrire les tests.

# Tests avec langage naturel

Cucumber ne serait même pas un outil de test

Dans cette [discussion sur Ycombinator](#), le créateur de Cucumber affirme plusieurs choses intéressantes dont :

- “The biggest problem with Cucumber is that most people trying it out don’t understand what it is.”
- “Cucumber is not a tool for testing software.”
- “Cucumber is a tool that facilitates collaboration and software design (especially domain-driven design).”
- “The purpose of Cucumber is to bridge the communication gap between business and IT by providing a small set of essential scenarios to illustrate core behaviour of unwritten software.”

Mais comme c'est au programme et que ça ne choque plus grand monde on va s'en servir d'outil de test quand même. 😊

# Spécifier avec le BDD

Exemple de Cucumber, le plus répandu

Développé en début des années 2000 par Daniel Terhorst-North, il fait entre autre le constat que : “Behaviour” is a more useful word than “test”<sup>14</sup>.

Il utilise les mots clés “Given”, “When” et “Then” pour décrire le comportement attendu du produit en développement dans un scénario.

```
Given some initial context (the givens),  
When an event occurs,  
Then ensure some outcomes.
```

Par exemple :

```
Given I just opened a new private window in my browser  
When I browse the https://in-france.fr website  
Then I want to discover the french economy by activity  
And by region.
```

On comprend facilement que ce sont des critères d’acceptation haut niveau.  
Les tests liés seront donc des tests d’acceptation/fonctionnels.

<sup>14</sup>Daniel Terhorst-North, Introducing BDD,  
<https://dannorth.net/introducing-bdd/>

# Spécifier avec le BDD

Exemple de Cucumber<sup>16</sup>

GIVEN

- In this step we are putting the system into known state by defining start data. For example we can put some data into database, set up environment data and so on.

WHEN

- This step defines a key action. It means that in this part of the test system does think what we expect from him.

THEN

- This is a verification step. In this part we observe system output, we check if system behave in the expected way or not and we draw conclusions.

GIVEN  
WHEN  
THEN

- Truck with driver "Teddy"
- Cargo loaded on truck
- Destination point loaded on truck GPS

- "Teddy" is driving to destination point

- Cargo is delivered to destination

“And” peut être utilisé pour ajouter des conditions supplémentaires aux 3 mots clés précédents<sup>15</sup>.

<sup>15</sup>Getting Started with BDD,

<https://cucumber.io/blog/bdd/getting-started-with-bdd-part-1/>

<sup>16</sup>Given-When-Then pattern in unit tests, <https://www.j-labs.pl/blog-technologiczny/given-when-then-pattern-in-unit-tests/>

# Spécifier avec le BDD

Exemple de Cucumber, le plus répandu

Les données d'un test paramétrique sont définies dans un tableau<sup>17</sup>.

Example

```
[Arguments] ${periodClosed} ${periodOpenAndModified} ${importDay} ${oldManagerValidUntil} ${newManagerValidFrom}
```

Given initialized criteria for bonus commercial

And a branch B with branch manager M\_OLD and employee E1

And evaluation for E1 for period \${periodClosed} which is closed

And evaluation for E1 for period \${periodOpenAndModified} which is open and modified

When M\_NEW becomes new manager of branch B

And import service is called on \${importDay}

Then the new branch manager of branch B is M\_NEW valid from \${newManagerValidFrom}

And branch manager M\_OLD manages employee E until \${oldManagerValidUntil}

And branch manager M\_NEW manages employee E from \${newManagerValidFrom}

And Evaluations for E1 still have the same content

*Test Case*	*Closed Period*	*Open Period*	*Run Import On*	*Old Manager Stops*	*New Manager Starts*
1   Example   1.11.2009 - 30.11.2009   1.12.2009 - 31.12.2009   11.11.2009   30.11.2009   1.12.2009					
2   Example   1.11.2009 - 30.11.2009   1.12.2009 - 31.12.2009   1.11.2009   31.10.2009   1.11.2009					

<sup>17</sup> Given/When/Then And Example Tables Using the Robot Framework,  
[https://www-codecentric-de.translate.goog/wissens-hub/blog/givenwhenthen-and-example-tables-using-the-robot-framework?\\_x\\_tr\\_sl=en&\\_x\\_tr\\_tl=fr&\\_x\\_tr\\_hl=fr&\\_x\\_tr\\_pto=sc&\\_x\\_tr\\_hist=true](https://www-codecentric-de.translate.goog/wissens-hub/blog/givenwhenthen-and-example-tables-using-the-robot-framework?_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=sc&_x_tr_hist=true)

# BDD qui a-t-il derrière ce langage ?

Quelques exemples en Python et Java

Avec Behave en Python<sup>18</sup> :

```
features/  
features/everything.feature  
features/steps/  
features/steps/steps.py
```

Derrière une phrase :

```
from behave import then  
  
@then('the result page will include "{text}"')  
def step_impl(context, text):  
    if text not in context.response:  
        fail('%r not in %r' % (text, context.response))
```

Avec Cucumber en Java<sup>19</sup> :

```
@When("the stock is traded at $price")  
public void theStockIsTradedAt(double price) {  
    stock.tradeAt(price);  
}
```

C'est une illusion de simplicité, derrière le langage naturel, il y a quasiment

# Exercice 4 de BDD

Exemple de Cucumber, le plus répandu

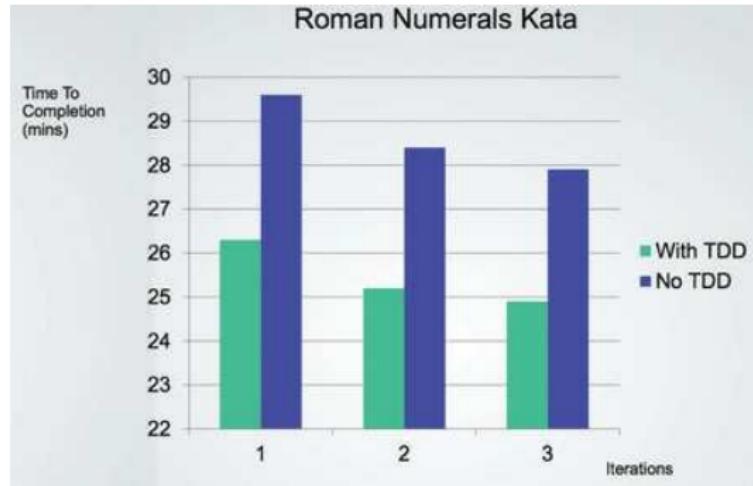
**Exercice :** En utilisant un maximum du code de l'exercice précédent sur les nombres témoins, réécrivez l'équivalent des tests pytest ou autre en scénarios Behave.

# Le TDD

## Test Driven Development

Vouloir aller plus vite sans faire de test semble être une mauvaise idée.  
Ce qui pratiquent le TDD vont plus vite dès le début d'un projet<sup>20</sup> !  
Entre autre, les tests unitaires font réduire la taille des classes, functions et  
des méthodes, ce qui améliore architecture.

“The only way to go fast, is to go well<sup>20</sup>.”



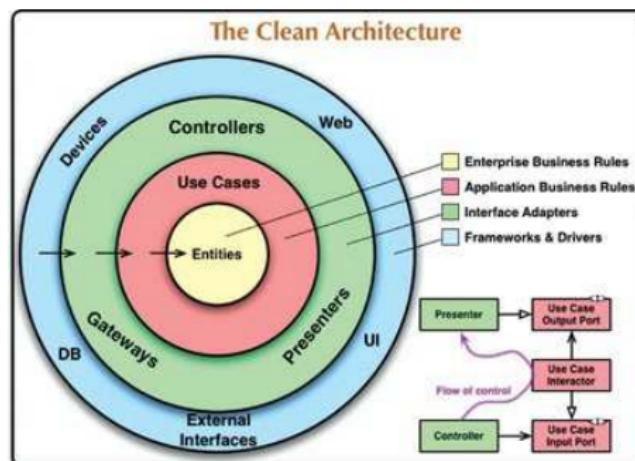
<sup>20</sup>Clean architecture, Robert C. Martin

# Le TDD

Quel type(s) de test ?

Tous les types de tests possibles sont à écrire dès que possible avant même de commencer à coder. Les tests unitaires sont en général les plus simples à écrire et les plus rapides à exécuter.

Les éléments centraux, les règles de gestions, les “business rules” doivent être testables sans les éléments périphériques<sup>20</sup> :



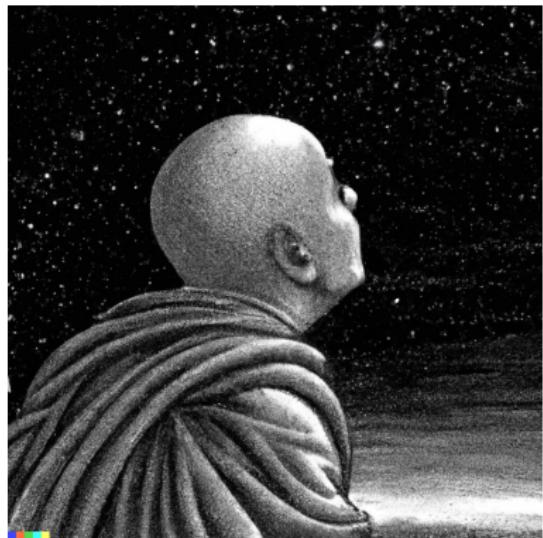
# Le TDD

Quel types de test ?

Edsger Dijkstra : “Testing shows the presence, not the absence of bugs.”

Autrement dit, l'univers des tests est infini, on n'a jamais la certitude de suffisamment tester.

Même le coverage est une mauvaise mesure.



# Le TDD

## Exercices 5

De nombreux exercices de TDD sont disponibles sur le web comme par sur GitHub, <https://github.com/gabbloquet/entrainement-au-tdd>.

En 30 minutes, sans assistant du type ChatGPT, réaliser l'un des plus classique d'entre eux, le "FizzBuzz", <https://github.com/gabbloquet/entrainement-au-tdd/tree/master/src/main/java/io/github/gabbloquet/tddtraining/FizzBuzz> .

Respecter l'esprit du TDD qui veut que l'on écrive les tests avant le code :

- ① Écrire un test par requirement.
- ② Écrire l'algorithme.
- ③ Refactoriser.
- ④ Revenir à l'étape 2 jusqu'à ce que tous les test passent.

# Tests assisté par l'IA

Test de GitHub Copilot le 30 mai 2024

Based on your request, here are some unit tests for the `Customer` class in the `customer_database.py` module. These tests cover the happy path and some edge cases for the `create_table` and `insert` methods. The test names are self-explanatory and do not start with “test”. The tests are written using the `unittest` module, which is a built-in module in Python for writing tests.

```
import sqlite3
import unittest
from unittest.mock import Mock

from customer_database import Customer

class CustomerDatabaseTests(unittest.TestCase):
    def setUp(self):
        ...
    def creating_customer_table(self):
        self.customer.create_table()
        ...
```

These tests use the `unittest.mock` module to mock the `sqlite3.connect` function, allowing us to test ...

# Tests assisté par l'IA

Test de GitHub Copilot le 30 mai 2024

```
(venv) chrichri@chrichri-HKD-WXX:~/Documents/Campus-St-Michel-IT/testing$ python  
-m unittest test_customer_database_with_copilot.py
```

```
Ran 0 tests in 0.000s
```

```
OK
```

“All tests should start with def `test_` no ? To be compliant with `unittest`? ”

Yes, you’re correct. In Python’s `unittest` module, test methods should start with `test_`. This is how the test runner identifies which methods represent tests. Here’s how you can modify the test methods in your `CustomerDatabaseTests` class:

# Tests assisté par l'IA

Test de GitHub Copilot le 30 mai 2024

```
class CustomerDatabaseTests(unittest.TestCase):
    def setUp(self):
        ...
    def test_creating_customer_table(self):
        ...
```

Now, each test method starts with `test_`, making them compliant with `unittest`.

```
Error
Traceback (most recent call last):
  File "/home/chrichri/Documents/Campus-St-Michel-IT/testing/ble_to_rpc_client.py", line 9, in setUp
    self.customer = Customer(self.mock_db)
                    ^
  File "/home/chrichri/Documents/Campus-St-Michel-IT/testing/customer_database.py", line 14, in __init__
    self.con = sqlite3.connect(path)
                ^
TypeError: expected str, bytes or os.PathLike object, not Mock
```

En conclusion, on a encore besoin de l'humain...

# Tests assisté par l'IA

## Cover Agent

Un framework open source qui utilise la puissance de l'IA pour générer des tests unitaires. Compatible avec la plupart des LLMs grâce à [LiteLLM handles loadbalancing, fallbacks and spend tracking across 100+ LLMs. All in the OpenAI format.](#) Voir sa page GitHub<sup>21</sup>.

Exercice 6 : Tester le code [https://github.com/St-Michel-IT/testing/blob/main/test\\_customer\\_database.py](https://github.com/St-Michel-IT/testing/blob/main/test_customer_database.py) avec Cover Agent.

---

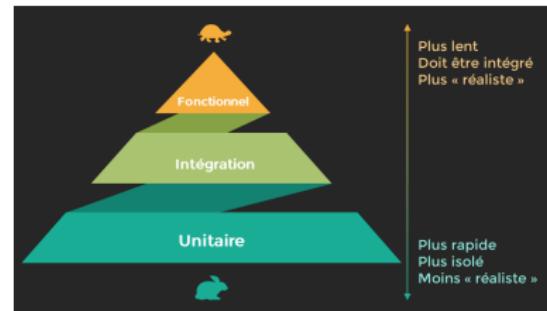
<sup>21</sup>Cover Agent, <https://github.com/Codium-ai/cover-agent>

# Les tests d'intégration

## définition

Les tests d'intégrations sont des tests effectués entre les composants afin de s'assurer du fonctionnement des interactions et de l'interface entre les différents composants. Ces tests sont également gérés, en général, par des développeurs<sup>22</sup>.

C'est aussi la définition de l'ISTQB<sup>23</sup> .



---

<sup>22</sup>Les niveaux de test,

<https://lataverneadutesteur.fr/2017/11/03/les-niveaux-de-test/>

<sup>23</sup>Glossaire CFTL/ISTQB des termes utilisés en tests de logiciels,

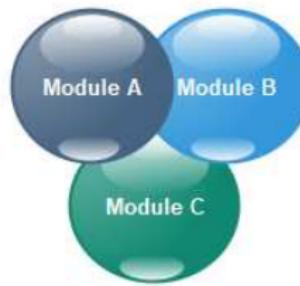
<https://www.cftl.fr/wp-content/uploads/2018/10/>

[Glossaire-des-tests-logiciels-v3\\_2F-ISTQB-CFTL-1.pdf](https://www.cftl.fr/wp-content/uploads/2018/10/Glossaire-des-tests-logiciels-v3_2F-ISTQB-CFTL-1.pdf)

# Les tests d'intégration

## définition

Autrement dit, les tests unitaires testent chaque composant, ceux d'interactions testent les interactions entre les composants.

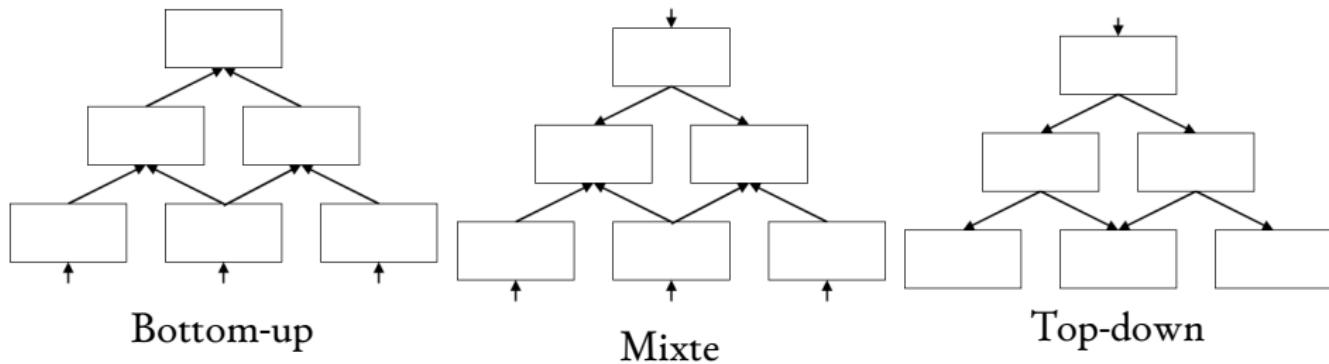


# Les tests d'intégration

les différentes approches, les top-down, bottom-up et mixte<sup>24</sup>

La top-down consiste à tester les composants les plus hauts de la hiérarchie en premier.

La bottom-up consiste à tester les composants les plus bas de la hiérarchie en premier.



---

<sup>24</sup> Tests d'intégration,

<https://mbf-iut.i3s.unice.fr/lib/exe/fetch.php?media=undefined:7-testintegration-2016.pdf>

# Les tests d'intégration

## Bonnes pratiques

- Ne pas tester la logique métier, c'est le rôle des tests unitaires.
- Ne pas les mélanger à d'autres tests, unitaire ou autre.
- Ils testent les interfaces.
- Ils sont généralement plus longs à jouer, il est donc conseillé de bien séparer les suites de test pour pouvoir lancer un sous-ensemble précis.

# Les tests d'intégration

## Exemple

Les 15 lignes de code [https:](https://github.com/St-Michel-IT/testing/blob/main/ble_to_rpc.py)

[//github.com/St-Michel-IT/testing/blob/main/ble\\_to\\_rpc.py](https://github.com/St-Michel-IT/testing/blob/main/ble_to_rpc.py)  
permettent de récupérer des données du Bluetooth Low Energy (BLE) et les distribuer “over” HTTP au format JSON RPC .

C'est donc l'intégration de 3 librairies :

- [bleak](#) pour le BLE .
- [Werkzeug](#) pour le serveur HTTP .
- [json-rpc](#) pour le format des données.

Le tester est donc bien un test d'intégration de ces librairies.

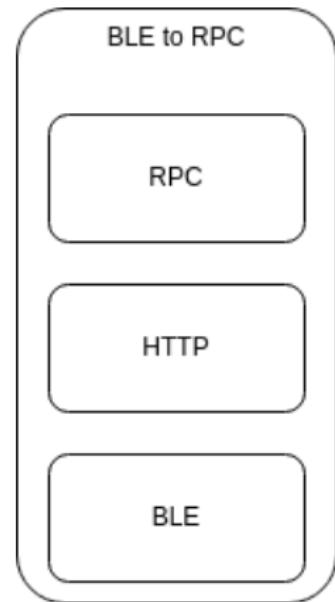
# Les tests d'intégration

## Exercice 7

Proposer et rédiger des tests d'intégration pour le code [https://github.com/St-Michel-IT/testing/blob/main/ble\\_to\\_rpc.py](https://github.com/St-Michel-IT/testing/blob/main/ble_to_rpc.py). Dans la techno de votre choix.

Tester les 3 protocoles intégrés.

Ajouter la fonction de connection BLE à un appareil défini par son adresse et lire la caractéristique “GATT” 2A24. Rédiger également les tests correspondant.



# Les tests d'intégration

## Exercice 8

Ils peuvent aussi être utilisés en embarqué, IOT, etc.

En lisant la documentation Arduino

[https://github.com/St-Michel-IT/testing/  
blob/main/doc/Arduino%C2%AE%20UNO%20R3%  
20Datasheet.pdf](https://github.com/St-Michel-IT/testing/blob/main/doc/Arduino%C2%AE%20UNO%20R3%20Datasheet.pdf), ajouter des tests d'intégration au  
module de test  
[https://github.com/St-Michel-IT/testing/  
blob/main/test\\_arduino.py](https://github.com/St-Michel-IT/testing/blob/main/test_arduino.py).

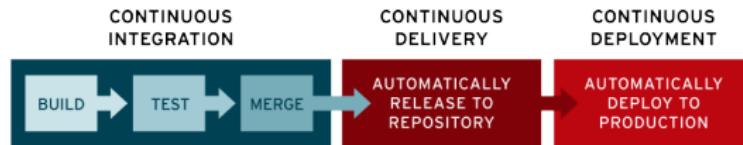


# Intégration continue A.K.A. CI

## Les définitions du CI/CD

CI/CD est l'acronyme de “Continuous Integration/Continuous Delivery” ou “Continuous Deployment”.

“le but ultime du processus CI/CD qui consiste à supprimer l'intervention humaine pour gagner en temps et en efficacité. Le code est compilé et testé sur l'ordinateur grâce à ce que l'on appelle un build automatisé. S'il n'y a pas de bug le tout est mis en production automatiquement. Cette approche permet aux développeurs de se concentrer sur la conception et le développement et sur les fonctionnalités de l'application.”<sup>25</sup>



<sup>25</sup>Qu'est-ce que l'approche CI/CD - Qu'est-ce que le processus CI/CD ?,  
<https://www.oracle.com/fr/cloud/definition-approche-ci-cd/>

# Intégration continue A.K.A. CI

## Les définitions du CI/CD

Plusieurs remarques :

- Une des avancées est l'automatisation de multiples tâches.
- Le mot intégration fait penser qu'on a plusieurs systèmes, logiciels, développeurs, équipes, etc.
- L'"ordinateur" n'est pas défini, on verra qu'il peut être celui du développeur ou un serveur distant voir un ordinateur inconnu.
- "S'il n'y a pas de bug le tout est mis en production automatiquement." vous y croyez?
- Le but est toujours le même, éliminer un maximum de bug.



# Histoire du CI/CD

Une histoire récente d'une vingtaine d'années

- 2005, première version de Hudson, le précurseur de Jenkins par Kohsuke Kawaguchi.
- 2010, le terme “Continuous Integration” est utilisé pour la première fois dans un livre par Jez Humble<sup>26</sup>.
- 2011, Jenkins est libéré.
- 2024, plus de 38 plateformes mainstream<sup>27</sup>.

---

<sup>26</sup>Continuous Delivery, <https://www连续交付.com/>

<sup>27</sup>38 Best CI/CD Tools For 2024,

<https://www.lambdatest.com/blog/best-ci-cd-tools/>

# Les avantages du CI/CD

Si tout peut être réalisé en local, pourquoi utiliser un serveur ?

- Les plateformes de CI/CD sont avant tout des outils collaboratifs. Elles permettent le partage des développements dans l'équipe et dans l'entreprise. On peut suivre en direct l'état d'avancement et la qualité des développements de ses collègues.
- Elles s'intègrent à de nombreux outils comme les SSO, Git, les outils de gestion de projet et de qualité comme ceux d'Atlassian (Jira, Confluence, Bitbucket, etc).
- Une UX/UI plus simple que des données un terminal. La prise en main peut-être faite par des métiers autre que celui de développeur (Testeur, Release Manager, Hardware).
- Permet de partager les ressources hardware requises pour la compilation, les tests, entre des machines plus ou moins disponibles. E.g., dans l'embarqué, cela permet de ne pas multiplier le hardware et de limiter le nombre de bancs de test. En générale la compilation qui peut prendre beaucoup de ressources CPU et peut être délocalisée sur un serveur dédié.

# Les avantages du CI/CD

Quelles différences avec le DevOps ?

Le CI/CD est un des outils du DevOps.

C'est l'outil dédié au développement et à la livraison de logiciels de qualité.  
On confond parfois les deux car le terme DevOps étant plus hype que  
CI/CD, est plus souvent utilisé.



# Le fondamental du CI/CD

Livre et site web de Jez Humble<sup>26</sup>

Jez Humble fait un travaille academic depuis les années 2000 pour mesurer l'impact du CI/CD sur les professionnels de l'IT .

En plus de plusieurs paramètres liés à la qualité logiciel, il mesure même un impact positif sur l'ambiance de travail !

Son livre sur le sujet, “Continuous Delivery”, est une référence dans le domaine. Son site web <https://www.continuousdelivery.com/> contient déjà beaucoup de ressources.

# Le business du CI/CD

Ce n'est pas une simple technologie mais un marché, attention aux coûts

Git, Python, que nous avons vu, sont des technologies open source devenues des standard. Toutes leurs fonctionnalités sont disponibles gratuitement. Contrairement à elles, certaines plateformes de CI/CD sont payantes.

Parmi les business model, on trouve :

- Le freemium, une version gratuite limitée en fonctionnalités.
  - Github est gratuit jusqu'à une certaine consommation de ressources (temps CPU, disque, etc) et est limité en fonctionnalités.
  - Gradle est toujours "full featured" en local mais Devlocity, le SaaS qui va avec et rajoute des fonctionnalités est payant.
  - Gitlab Community Edition VS Entreprise edition.
- L'auto-hébergement d'une solution complète open source et le on-premise.
  - Jenkins.
- Les solutions propriétaires.
  - TeamCity est payant en auto-hébergement et on-premise.
  - Travis CI .

# Les différences entre plateformes

A lire absolument, un comparatif des différentes plateformes par Atlassian  
<https://www.atlassian.com/fr/continuous-delivery/continuous-integration/tools>.

Les différences sont nombreuses, on peut citer :

- Certains permettent de créer des clusters sur n'importe quelles machines. Par exemple Jenkins avec son cluster formé de “slave(s)” et d'un “master”. Tout ce qui se passe sur les “slaves” est visible sur l'IHM du “master”.
- AWS CodePipeline permet d'avoir de multiples nodes mais sur des machines AWS uniquement .
- Devlocity n'a qu'une instance centrale du serveur
- Leur communauté, une communauté open source peut développer des plugins, des scripts, des outils, etc, pour virtuellement toutes les applications qui ne sont pas prévues dans la version de base. De ce point de vue, Jenkins est dans les premiers.
- L'organisation en jobs ou en pipelines de jobs.

# Les limites du CI/CD

Quelles sont les limites du CI/CD ?

# Les limites du CI/CD

Quelles sont les limites du CI/CD ?

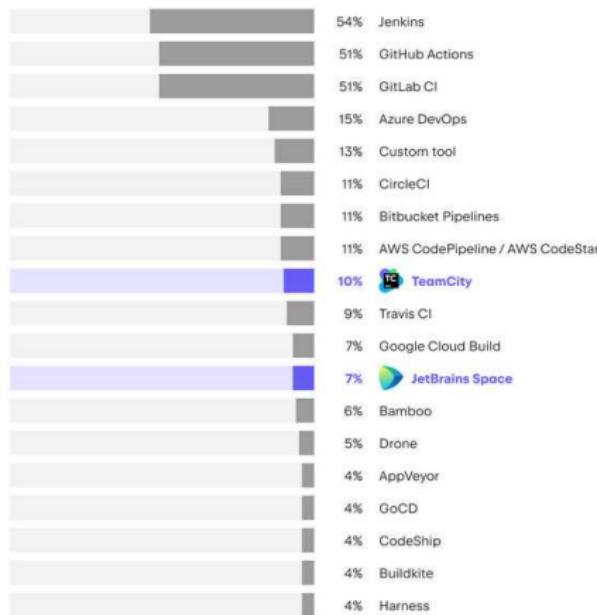
- le coût des licences ou des machines.
- Pas de limites sur le type de logiciel, on peut y connecter un banc de test pour l'embarqué et l'IOT, dans le web, la data, etc...
- Les ressources des machines disponibles.
- La complexité des tests, plus ils sont nombreux et plus ils sont longs à faire tourner et analyser.



# Les plateformes les plus utilisées CI/CD

Résultat de l'enquête JetBrains 2023 sur le CI/CD<sup>28</sup>

Which Continuous Integration (CI) systems do you regularly use?



<sup>28</sup>Best Continuous Integration Tools for 2024 – Survey Results,

<https://blog.jetbrains.com/teamcity/2023/07/best-ci-tools/>

# Exemple de CI/CD

## Exemple de CPython sur GitHub<sup>29</sup> Actions

Une partie seulement de CPython, l'implémentation classique officielle de Python est sur GitHub, il y en a aussi sur Azure DevOps. On y trouve 21 workflows différents !

The screenshot shows the GitHub Actions interface. On the left, a sidebar lists various actions categories: Actions, All workflows, Workflows, Coverage (which is selected), Check labels, CodeSpaces Prebuilds, Coverage, Dots, Dots, JIT, Lint, Mark static pull requests, MyPy, new bugs announce newsletter, Read the Docs PR preview, Tests, TestAllBld, Update GH projects, Verify bundled pip and setuptools, Management, and Caches. The main area displays a table of 21 workflow runs, each with a green circular icon, a title, a timestamp, a status (either "In progress" or "Completed"), a branch name, and three vertical dots for more options. The workflow titles include: "[3.8] gh-151597: Stop resolving host in urllib.request proxy bypass ...", "[3.9] gh-151597: Stop resolving host in urllib.request proxy bypass ...", "[3.8] gh-115398: Expose Expat >2.6.0 reparse deferral API (CVE-2023-...)", "[3.8] gh-151598: Expose Expat >2.6.0 reparse deferral API (CVE-2023-...)", "[3.9] gh-107077: Raise SSLCertVerificationError even if the error is ...", "[3.8] gh-107077: Raise SSLCertVerificationError even if the error is ...", "[3.8] Upgrade bundled libexpat to 2.6.0 (GH-115399) (GH-115476)", "[3.8] Upgrade bundled libexpat to 2.6.0 (GH-115399) (GH-115476)", "[3.8] Fix tests for XMLPullParserParser with Expat 2.6.0 (GH-115133) (GH-115133)", "[3.8] gh-97032: avoid test\_squeeze crash on macOS buildbots (GH-1155...)", and "[3.8] gh-97032: avoid test\_squeeze crash on macOS buildbots (GH-1155...). The timestamps range from "2 hours ago" to "2 months ago".

<sup>29</sup>CPython implémentation,

<https://github.com/python/cpython?tab=readme-ov-file>

# Exemple de CI/CD

Exemple de CPython sur GitHub<sup>30</sup> Actions

5 workflows “triggered” par un push et une PR !

The screenshot shows a list of GitHub Actions runs for a repository. There are five entries, each representing a workflow triggered by a push to the main branch:

- gh-116417: Move limited C API complex.c test...**: Status: Succeeded, Triggered by a pull request labeled #117014 unlabeled by vstinner, pushed by bedevere-app (bot). Started 6 minutes ago, completed 13s ago.
- gh-116417: Move limited C API complex.c test...**: Status: In progress, Triggered by a commit 61c659e pushed by vstinner. Started 7 minutes ago, currently Queued.
- gh-116417: Move limited C API complex.c test...**: Status: In progress, Triggered by a lint commit 61c659e pushed by vstinner. Started 7 minutes ago, completed 36s ago.
- gh-116417: Move limited C API complex.c test...**: Status: In progress, Triggered by a mypy commit 61c659e pushed by vstinner. Started 7 minutes ago, completed 33s ago.
- [main]: gh-116417: Move limited C API comple...**: Status: In progress, Triggered by Codespaces Prebuilds #4897 by github-codespaces (bot). Started 7 minutes ago, currently In progress.

<sup>30</sup>CPython implémentation,

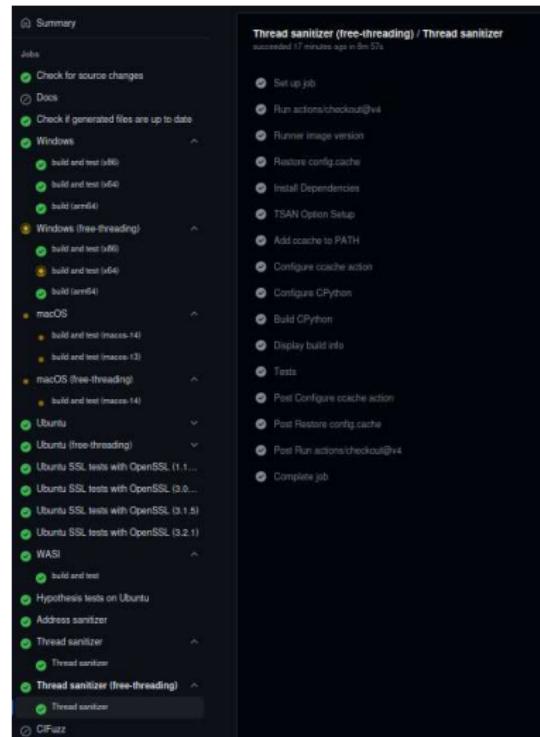
<https://github.com/python/cpython?tab=readme-ov-file>

# Exemple de CI/CD

Exemple de CPython sur GitHub<sup>31</sup> Actions

1 seul workflow compte des dizaines de jobs !

1 seul job compte plusieurs steps !



<sup>31</sup>CPython implémentation,

<https://github.com/python/cpython?tab=readme-ov-file>

# Exemple de CI/CD

Exemple de workflow GitHub<sup>32</sup>

Definition :

- Un workflow est une suite de jobs.
- Un job est une tache à réaliser.
- Un step est une étape de la tache.
- Un artefact est un fichier généré par un step.

---

<sup>32</sup>Automate your workflow from idea to production,

<https://github.com/features/actions>

# Exemple de CI/CD

Exemple de workflow GitHub de ce repository, exercice de 15 minutes

Que peut-on faire comme workflow, GitHub Actions, etc, sur les dépôts de ce cours ?

- <https://github.com/St-Michel-IT/qualite-code-source/>
- <https://github.com/St-Michel-IT/testing/>



# Exemple de CI/CD

Exemple de workflow GitHub de ce repository<sup>33</sup>

Les workflows sont dans les fichiers suivants :

```
$ tree .github/
.github/
--- workflows
    --- build-document.yml
    --- checkmytex.yml
    --- shell-check.yml
```

- `build-document.yml` pour générer le document PDF que vous lisez.
- `shell-check.yml` pour vérifier la syntaxe des scripts Shell.
- `checkmytex.yml` pour lister les erreurs dans le fichier LaTex.

---

<sup>33</sup>Workflow de génération des documents à partir de Latex, <https://github.com/St-Michel-IT/qualite-code-source/blob/master/.github/workflows/>

# Exemple de CI/CD

Exemple de workflow GitHub du repository testing<sup>34</sup>

Les workflows sont dans les fichiers suivants :

```
$ tree .github
.github
--- workflows
    --- build-document.yml
    --- checkmytex.yml
    --- pylint.yml
    --- shell-check.yml
    --- black-formatter.yml
    --- unit-tests.yml
```

- `unit-tests.yml` lance les tests avec `pytest`.
- `pylint.yml` un linter qui génère un rapport des erreurs et des warnings.
- `black-formatter.yml` Black formatter qui fait un check sans rien changer.

---

<sup>34</sup>Workflow de génération des documents à partir de Latex,

<https://github.com/St-Michel-IT/testing/blob/master/.github/workflows/>

# Exemple de CI/CD

Pas de runner officiel des workflows GitHub en local

Tout les workflows doivent tourner sur des machines GitHub. Avec les coûts et la latence que cela implique.

Quelles sont donc les bonnes pratiques pour éviter les pièges des plateformes comme GitHub, Circle CI, Jenkins, etc ?

---

<sup>35</sup> Accelerate developer productivity, <https://gradle.org/>

# Exemple de CI/CD

Pas de runner officiel des workflows GitHub en local

Tout les workflows doivent tourner sur des machines GitHub. Avec les coûts et la latence que cela implique.

Quelles sont donc les bonnes pratiques pour éviter les pièges des plateformes comme GitHub, Circle CI, Jenkins, etc ?

- Éviter des fonctionnalités propres à ces plateformes. C'est à dire agnostiques aux plateforme.
- Écrire des scripts qui peuvent être exécutés en local. Par exemple (scripts BASH, scripts PowerShell, scripts Gradle<sup>35</sup>, Dockerfiles, scripts Ansible)
- Ces scripts peuvent-être appelés dans les jobs du CI/CD .
- Nettoyer vos environnements après le build pour économiser les ressources.

---

<sup>35</sup>Accelerate developer productivity, <https://gradle.org/>

# Gradle

Gradle comme une passerelle entre le local et la plateforme de CI/CD

Gradle<sup>35</sup> est un outil de build open source. On script en Groovy<sup>36</sup> ou Kotlin<sup>37</sup>, en local des tâches de build, équivalente au jobs des plateformes de CI/CD .

On débug en local, on teste en local, on commit en local. Cela fait gagner un temps considérable (pas de commit/push...) dans le développement du CI/CD . Et donc, cela fait également économiser des ressources de CI/CD .

Toutes les plateformes de CI/CD ont un plugin/workflow Gradle. La portabilité est donc assurée.

---

<sup>36</sup>Groovy, A multi-faceted language for the Java platform, <https://groovy-lang.org/>

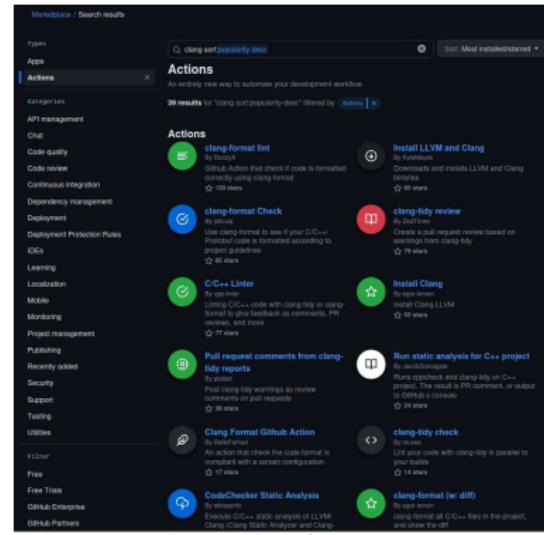
<sup>37</sup>Kotlin, <https://kotlinlang.org/>

# Les marketplaces des plateformes de CI/CD

Un “market” gratuit ou payant

Ne pas avoir peur du nom marketplace, beaucoup de plugins Jenkins ou de workflows GitHub sont gratuits.

- Plus de 1 900 plugin Jenkins<sup>38</sup>.
- Plus de 22 000 actions GitHub<sup>39</sup>.



Ils sont essentiels pour développer plus rapidement les jobs (reuse, comme dans n’importe quel code).

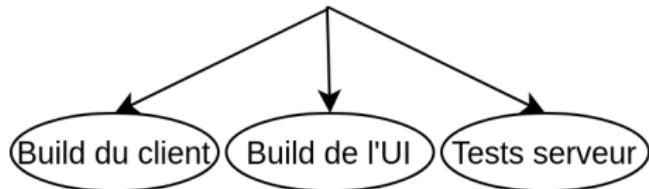
<sup>38</sup>Jenkins Plugins, <https://plugins.jenkins.io/>

<sup>39</sup>GitHub Actions, <https://github.com/marketplace?type=actions>

# Les exemples de CI/CD dans le développement d'API

Grâce à Swagger et OpenAPI

Swagger est un fichier de définition d'une API . Il est écrit en YAML ou en JSON. Et les données pour décrire l'API sont dans la OpenAPI Specification<sup>40</sup>.



<sup>40</sup> API Development for Everyone <https://swagger.io/>

# Les exemples de CI/CD dans le développement d'API

Grâce à Swagger et OpenAPI

```
/lists:  
  get:  
    summary: Gets all available data lists.  
    description: Returns all custom data lists available to the current user.  
    tags:  
      - Lists  
    responses:  
      200:  
        description: 'OK'  
        content:  
          application/json:  
            schema:  
              type: array  
              items:  
                # Reuse du schema de DataList !  
                $ref: '#/components/schemas/DataList'  
      401:  
        # Reuse des responses !  
        $ref: '#/components/responses/Unauthorized'  
      5XX:  
        $ref: '#/components/responses/ServerError'
```

# Les exemples de CI/CD dans le développement d'API

Une UI pour découvrir l'API

L'UI est un espace convivial pour découvrir l'API . Il fait aussi office de documentation. Par exemple <https://api.recherche-entreprises.fabrique.social.gouv.fr/#/Recherche/search>.

The screenshot shows the Swagger UI interface for the API recherche-entreprises. At the top, there's a navigation bar with the Swagger logo, the URL '/swagger.json', and a 'Explore' button. Below the navigation, the API title 'API recherche-entreprises 1.0.0' is displayed, along with the base URL 'api.recherche-entreprises.fabrique.social.gouv.fr/api/v1' and the file 'swagger.json'. A note indicates it's a 'Documentation de l'API recherche-entreprises'. Below this, there are links for 'Contact the developer', 'Apache-2.0', and 'Source sur GitHub'. A dropdown menu for 'Schemes' is open, showing 'HTTPS' selected. The main content area is titled 'Recherche' and contains a 'GET /search Recherche d'entreprise par nom' section. It includes a description: 'Recherche d'entreprise par nom d'établissement, raison sociale, siren, siret'. A 'Parameters' table lists three fields: 'query' (string, required, description: 'Texte de la recherche', value: 'Michelin'), 'address' (string, description: 'Localisation de l'entreprise', value: 'Lyon'), and 'limit' (integer, description: 'Nombre de résultats max', value: '100'). A 'Cancel' button is located in the top right corner of the parameters table.

# Les exemples de CI/CD dans le développement d'API

Toutes les fonctionnalités sont déjà dans la marketplace (ou les plugins pour Jenkins)

The screenshot shows the GitHub Marketplace search results for the query "swagger sort.popularity-desc". The results are filtered by "Actions" and sorted by "Most installed/starred". There are 23 results displayed.

- rdme 🚧 Sync to ReadMe** By readme0: A GitHub Action that syncs OpenAPI-Swagger (OAS) definitions and Markdown documentation from your GitHub repository to your ReadMe developer hub. (89 stars)
- Swagger Editor Validator** By charron: This GitHub Action validates OpenAPI (OAS) definition file using Swagger Editor. (43 stars)
- Swagger UI Action** By Legion2: Generates Swagger UI for API documentation. (38 stars)
- OpenAPI Diff** By mverger: A GitHub Action to identify differences between Swagger or OpenAPI specifications. (22 stars)
- swagger ui** By pjoel-team: Generates swagger ui by json files. (9 stars)
- Validate Swagger and OpenAPI using Swagger CLI** By mbowman100: Access to the swagger-cli via a github action. (7 stars)
- Swagger Codegen** By tyerkko: Runs Swagger Codegen with Github Actions. (5 stars)
- Sync Swagger to Postman** By salokhart: Syncs a Swagger 2.0 file to a Postman collection. (4 stars)
- Open API Specification Lint action** By valibov-jahn: Runs Swagger validation on your OAS JSON or YAML file. Supports Swagger 2.0 or OpenAPI 3.0 format. (3 stars)
- api-client-gen** By supov: Generates API Clients by Swagger. (2 stars)
- Swagger-cli** By impernic: Runs Swagger validation on your OAS JSON or YAML file. Supports Swagger 2.0 or OpenAPI 3.0 format. (2 stars)
- OpenApi Specification Lint action** By crudo: Runs OpenAPI validation on your OAS JSON or YAML file. Supports OpenAPI 3.0 format. (2 stars)

# Les exemples de CI/CD avec le déploiement d'une image Docker

GitHub ou Docker Hub peuvent héberger des images Docker<sup>41</sup>

```
- name: Log in to Docker Hub
  uses: docker/login-action@f4ef78c080cd8ba55a85445d5b36e214a81df20a
  with:
    username: ${{ secrets.DOCKER_USERNAME }}
    password: ${{ secrets.DOCKER_PASSWORD }}
- name: Extract metadata (tags, labels) for Docker
  id: meta
  uses: docker/metadata-action@9ec57ed1fcdbf14dcef7dfbe97b2010124a938b7
  with:
    images: my-docker-hub-namespace/my-docker-hub-repository
- name: Build and push Docker image
  uses: docker/build-push-action@3b5e8027fcad23fda98b2e3ac259d8d67585f671
  with:
    context: .
    file: ./Dockerfile
    push: true
    tags: ${{ steps.meta.outputs.tags }}
    labels: ${{ steps.meta.outputs.labels }}
```

<sup>41</sup>Publishing Docker images, <https://docs.github.com/en/actions/publishing-packages/publishing-docker-images>

# Les exemples de CI/CD avec la publication de builds

Pour publier un soft compilé ou packagé sur sa page du dépôt GitHub<sup>42</sup>

```
name: Releases

on:
  push:
    tags:
      - '*'

jobs:
  build:
    runs-on: ubuntu-latest
    permissions:
      contents: write
    steps:
      - uses: actions/checkout@v3
      - uses: ncipollo/release-action@v1
        with:
          artifacts: "release.tar.gz,foo/*.txt"
          bodyFile: "body.md"
```

---

<sup>42</sup>Create Release, <https://github.com/marketplace/actions/create-release>

# Les exemples de CI/CD avec la publication de builds

Publication de VS Code packagé<sup>43</sup>

The screenshot shows two GitHub release pages for VS Code:

- February 2024 Recovery 2**: Published 2 weeks ago by justschén. Version 1.87.2, commit hash 863d258. Includes a 'Source code (zip)' asset and a 'Source code (tar.gz)' asset. It has 56 likes, 9 comments, 19 forks, 14 stars, 19 issues, 11 pull requests, and 82 people reacted.
- February 2024 Recovery 1**: Published 2 weeks ago by justschén. Version 1.87.1, commit hash 1e798d7. Includes a 'Source code (zip)' asset and a 'Source code (tar.gz)' asset. It has 60 likes, 13 comments, 26 forks, 26 stars, 22 issues, 15 pull requests, and 87 people reacted.

<sup>43</sup> microsoft/vscode, <https://github.com/microsoft/vscode/releases>

# Quelques exemples d'étapes de compilation du CI/CD

Quelles types de jobs pour passer d'un code source à un exécutable?

# Quelques exemples d'étapes de compilation du CI/CD

Quelles types de jobs pour passer d'un code source à un exécutable?

- Compilation de C/C++ en binaire avec GCC et Vagrant pour cibler plusieurs les architectures.
- Compilation de Python en bytecode.
- Compilation de Java en Jar.
- Packaging de NodeJS en NPM .
- Packaging de Python en Wheel.
- Compiler LaTex en PDF .
- etc...

# Quelques notions de base de Jenkins

Les jobs VS les pipelines

Les jobs sont des tâches unitaires.

Un job est plus simple, c'est principalement un ensemble de commandes de "build".

Ce sont des commandes shell, console ou PowerShell en fonction de l'environnement.

Les pipelines sont des enchainements de jobs. Le pipeline est écrit en Groovy<sup>36</sup> et mais le principe est similaire au fichier Gradle ou workflow GitHub<sup>44</sup>.



<sup>44</sup>Pipeline Examples, <https://www.jenkins.io/doc/pipeline/examples/>

# Quelques notions de base de Jenkins

## Exemple de pipeline avec Gradle

Pour être agnostique à une plateforme de CI/CD, on peut exécuter dans la plateforme de CI/CD un build Gradle.

Jenkins, comme les autres plateformes, permet évidemment de faire cela dans les builds ou les pipelines<sup>45</sup>.

Si un maximum de tâches, d'intelligence, de scripting sont dans le build Gradle, il sera plus simple de changer de plateforme de CI/CD .

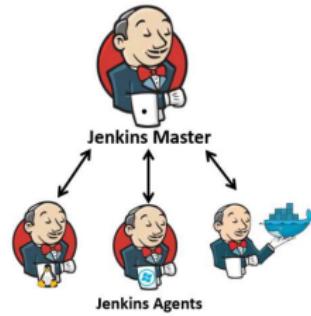
---

<sup>45</sup>Jenkins Gradle plugin, <https://plugins.jenkins.io/gradle/>

# Quelques notions de base de Jenkins

Les clusters de slaves et master<sup>46</sup>

Différentes machines esclaves peuvent être reliées à une machine maître. Soit pour répartir la charge, soit pour avoir des machines avec des environnements ou des configurations différentes. Ce sont des Jenkins slave agents aussi appelés node.



---

<sup>46</sup>Jenkins master-slave setup,

<https://www.linkedin.com/pulse/jenkins-slave-node-soma-sekhar-k-gusdc/>

# GitLab

Histoire et présentation de GitLab<sup>47, 48</sup>

GitLab est une plateforme de gestion de développement de logiciels au sens large. Son développement a commencé en 2011 .

Le nombre de ces fonctionnalités ne cesse d'augmenter mais elle est surtout connue comme VCS pour son intégration de Git.

GitLab se tourne vers le CI/CD en 2018.

Mais on y trouve encore de nombreuses autres fonctionnalités :

- Gestion de projet
- Bug tracking
- WiKi
- Many more...

---

<sup>47</sup>What we do, <https://about.gitlab.com/company/>

<sup>48</sup>GitLab, <https://gitlab.com/st-michel/>

### Community ou Entreprise Edition :

The image displays a comparison chart for GitLab editions. It features two main sections: 'Enterprise Edition' on the left and 'Community Edition' on the right. Both sections have a purple header bar with the word 'Recommended' in white. Below each header is a large bold title. Under each title is a bulleted list of features or characteristics. At the bottom of each section is a dark button with white text.

Enterprise Edition	Community Edition
<ul style="list-style-type: none"><li>Take advantage of all of GitLab's features</li><li>Free tier available*</li><li>Support**</li><li>Easily upgrade to paid tier in the future</li></ul>	<ul style="list-style-type: none"><li>Open source</li><li>Free tier only</li><li>No support</li><li>Will need to migrate to Enterprise Edition to upgrade to a paid tier in the future</li></ul>
<a href="#">Install GitLab Enterprise edition &gt;</a>	<a href="#">Install GitLab Community edition &gt;</a>

\*See our pricing page for features available on each tier.  
\*\*Support available on paid tiers only.

If you're an organization using GitLab Community Edition looking for paid support, please contact Sales for options.

La version CE est à installer sur une de ses propres machines.

La version EE se décline en Premium et Ultimate.

Les fonctionnalités de ces 3 versions sont bien différentes, voir

<https://about.gitlab.com/pricing/feature-comparison/>.

On ne paye donc pas que pour les ressources utilisés comme chez GitHub mais aussi pour les fonctionnalités.

### Community ou Entreprise Edition :

The image shows a comparison chart for GitLab editions. It features two main sections: 'Enterprise Edition' on the left and 'Community Edition' on the right. Both sections have a purple header bar with the edition name and a 'Recommended' badge. Below each header is a bulleted list of pros and cons. At the bottom of each section is a button labeled 'Install GitLab [Edition] edition >'. A note at the bottom left says 'See our pricing page for features available on each tier'. A note at the bottom right says 'If you're an organization using GitLab Community Edition looking for paid support, please contact Sales for options.'.

Enterprise Edition	Community Edition
<ul style="list-style-type: none"><li>Take advantage of all of GitLab's features</li><li>Free tier available*</li><li>Support**</li><li>Easily upgrade to paid tier in the future</li></ul>	<ul style="list-style-type: none"><li>Open source</li><li>Free tier only</li><li>No support</li><li>Will need to migrate to Enterprise Edition to upgrade to a paid tier in the future</li></ul>

\*See our pricing page for features available on each tier

\*\*Support available on paid tiers only

If you're an organization using GitLab Community Edition looking for paid support, please contact Sales for options.

La version CE est à installer sur une de ses propres machines.

La version EE se décline en Premium et Ultimate.

Les fonctionnalités de ces 3 versions sont bien différentes, voir

<https://about.gitlab.com/pricing/feature-comparison/>.

On ne paye pas donc que pour les ressources utilisés comme chez GitHub mais aussi pour les fonctionnalités.

# GitLab

## Le pipeline<sup>49</sup>

Très similaire aux workflows GitHub c'est un ensemble de "Jobs" spécifiés dans un fichier YAML .

Il doit être à la racine du projet et se nommer .gitlab-ci.yml.

```
stages:
  - build
  - test

job_build:
  stage: build
  script:
    - echo "Building the project"

job_test:
  stage: test
  script:
    - echo "Running tests"
```

Ce Pipeline doit être exécuté dans un runner.

---

<sup>49</sup>Tutorial: Create and run your first GitLab CI/CD pipeline,  
[https://docs.gitlab.com/ee/ci/quick\\_start/](https://docs.gitlab.com/ee/ci/quick_start/)

# GitLab

Développement du pipeline dans la web UI de GiLab.com

La web UI de GitLab permet de développer le pipeline et de valider la syntaxe en live dans le “Pipeline editor” :

The screenshot shows the GitLab Pipeline Editor interface. On the left, there's a sidebar with project navigation (Getting Started, Issues, Merge requests, Project, etc.) and a "Pipeline editor" section selected. The main area displays a pipeline configuration file (`.gitlab-ci.yml`) with the following content:

```
1 stages:
2   - test
3
4 job_build:
5   tags:
6     - test
7   stage: build
8   script:
9     - echo "Building the project"
10
11 job_test:
12   stage: test
13   tags:
14     - test
15   script:
16     - echo "Running tests"
```

Below the code editor, there's a "Commit message" field containing "Update .gitlab-ci.yml file" and a "Branch" dropdown set to "main". At the bottom, there are "Cancel changes" and "Reset" buttons.

# GitLab

## Le runner<sup>50</sup>

Le “runner” est l’équivalent du Jenkins Slave.

Il peut fonctionner via de nombreuses interfaces :

- SSH
- Shell
- VirtualBox
- Docker
- Kubernetes
- ...

La machine peut-être un PC, un serveur, un banc de test, Windows, Mac, Linux, etc.

Suivre le tutoriel officiel<sup>50</sup> pour configurer un runner et le lancer. Une fois que le programme `gitlab-runner run` est lancé, le runner est prêt à exécuter les pipelines.

À paramétrier comme service pour qu'il tourne en permanence en tâche de fond.

---

<sup>50</sup>Tutorial: Create, register, and run your own project runner, [https://docs.gitlab.com/ee/tutorials/create\\_register\\_first\\_runner/index.html](https://docs.gitlab.com/ee/tutorials/create_register_first_runner/index.html)

# GitLab

Exécution d'un pipeline sur un runner donné

Par défaut si dans le pipeline, aucun runner n'est spécifié, le pipeline est exécuté sur un runner disponible et compatible sans que l'on puisse prédire lequel.

Lors de la configuration du runner, on peut lui donner de(s) tag(s).

Ce tag peut être spécifié dans les jobs du pipeline pour forcer l'exécution sur un/des runner(s) donné(s).

```
job_build:  
tags:  
- Ubuntu
```

Ou :

```
job_build:  
tags:  
- Ubuntu  
- Docker
```

The screenshot shows the GitLab interface for managing runners. On the left, under 'Project runners', it says 'These runners are assigned to this project.' and has a button 'New project runner'. On the right, under 'Instance runners', it says 'These runners are available to all groups and projects. Each CI/CD job runs on a separate, isolated virtual machine.' and has a switch 'Enable instance runners for this project' which is turned on. Below that, it lists 'Available instance runners: 100' and shows a table with one entry: 'gitlab-ci-multi-runner' (status: green, last check: 10 minutes ago). The URL for this runner is listed as 'gitlab-ci-multi-runner-gitlab-org.runners-manager.gitlab.com'.

Une machine match avec le tag Ubuntu

# GitLab

Exécution d'un pipeline sur un runner donné

La liste des exécutions des pipelines est dans Build > Pipelines :

The screenshot shows the GitLab web interface with the following details:

- Project:** St-Michel / Industrialisation du développement Epreuve 2023-2024
- Pipelines:** Two pipelines are listed:
  - Status:** Passed  
**Pipeline ID:** #1313693024  
**Created:** 00:00:14 ago  
**Last Run:** 00:00:48 ago
  - Status:** Passed  
**Pipeline ID:** #1313693030  
**Created:** 00:00:58 ago  
**Last Run:** 00:00:58 ago
- Build Status:** 2 green circles
- CI Test:** 2 green circles
- Run Pipeline:** Button

# GitLab

Exécution d'un pipeline sur un runner donné

Il y a aussi une vue qui liste les Jobs est dans Build > Jobs :

The screenshot shows the GitLab web interface with the URL <https://gitlab.com/st-michel/industrialisation-du-developpement-europeen-2023-2024>. The left sidebar is open, showing the 'Build' section with 'Jobs' selected. The main content area displays a table of completed jobs for a pipeline. The table has columns for Status, Job, Pipeline, and Coverage.

Status	Job	Pipeline	Coverage
Passed	#0901355440: job_test	#130891024 created by [user]	Stage test
Passed	#0901355431: job_build	#130891024 created by [user]	Stage build
Passed	#0901280398: job_test	#130876939 created by [user]	Stage test
Passed	#0901280393: job_build	#130876939 created by [user]	Stage build

# GitLab

Exécution d'un pipeline sur un runner donné

Une vue détaillée des Jobs d'un Pipeline donné dans Build > Pipelines :

The screenshot shows a browser window with several tabs open, all related to a GitLab project named "Industrialisation du développement Epreuve 2023-2024". The main content area displays the "Pipelines" page for the ".gitlab-ci.yml" file. At the top, it shows a message from Christophe Brun: "Christophe Brun created pipeline for commit: adaf0d2f 55 minutes ago, finished 55 minutes ago". Below this, under the "For build" section, it says "2023-2024" and "2023-2024" with "2023-2024" being the active pipeline. It indicates "2023-2024" has 2 jobs, queued for 14 seconds, and finished 1 second ago. The pipeline itself is visualized as a sequence of stages: "build" followed by "test". Each stage contains a single job: "job\_build" and "job\_test" respectively. The left sidebar provides navigation through various GitLab features like Issues, Merge requests, and Artifacts, with "Pipelines" currently selected.

# GitLab

Exécution d'un pipeline sur un runner donné

Une vue détaillée d'un Job avec les logs horodatées du runner :

The screenshot shows a GitLab interface with a job log for a pipeline named 'job\_build'. The log details the execution of a script, starting with cloning a repository and moving through various stages of setup and build.

**Job Log Details:**

- Duration: 9 seconds
- Started: 57 minutes ago by Christophe.Brun
- Ended: 57 minutes ago
- Queue: 0 seconds
- Timestamp: 1h (from project)
- Runner: #37529841 [edDe4uyy] Ubuntu desktop machine
- Tag: dev

**Log Output:**

```
1 Running with gitlab-runner 17.0.0 (44faccff)
2 on ubuntu-vd0u4uyy, system ID: e_a385b544de07b
3 Preparing the "shell" executor
4 Using Shell (bosh) executor...
5 Preparing environment
6 Running on chrischr1-HDX-8XX...
7 Getting source from GIT repository
8 Fetching changes with git depth set to 20...
9 Rebuilt Git珍惜 initialize data /home/chrischr1/Documents/Campus-St-Michel-IT/testing/builds/vd0u4uyy/0/st-michel/industrialisation-du-developpement-epreuves-2023-20
10 Created fresh repository.
11 Checking out edfe6425 as detached HEAD (ref is main)...
12 Skipping EGit automatics setup
13 Executing "step_script" stage of the job script
14 $ echo "Building the project"
15 Building the project
16 Cleaning up project directory and file based variables
17 job succeeded
```

**Related Jobs:**

- job\_build

# Risques cyber lié au CI/CD

Quels sont les risques cyber lié au CI/CD ?

---

<sup>51</sup>Echoes of SolarWinds, <https://www.scmagazine.com/news/echoes-of-solarwinds-jetbrains-teamcity-servers-under-attack-by-russia-backdoor/>

<sup>52</sup>The CircleCI secrets hack is a red flag for security teams on software supply chain risk, <https://www.reversinglabs.com/blog/circleci-hack-is-a-red-flag-for-security-teams-on-the-software-supply-chain/>

# Risques cyber lié au CI/CD

Quels sont les risques cyber lié au CI/CD ?

Une mauvaise configuration des droits, une faille non patchée, un secret exposé peuvent permettre d'accéder au données du CI/CD . Donc probablement le code source.

Exemples de hacks majeurs liés au CI/CD :

- TeamCity non patché dans l'attaque de SolwarWinds<sup>51</sup>. Un fournisseur de services et logiciels de supervision de réseau. Les hackers ont ensuite exploité les failles de Solar Winds et accédé aux réseaux des clients comme MS qui a vu un source de Windows fuiter.
- Circle CI a vu des secrets exposés<sup>52</sup>. Le hack n'a pas touché ceux qui avait mis en place Open ID Connect, la configuration est donc importante.

---

<sup>51</sup>Echoes of SolarWinds, <https://www.scmagazine.com/news/echoes-of-solarwinds-jetbrains-teamcity-servers-under-attack-by-russia-backdoor/>

<sup>52</sup>The CircleCI secrets hack is a red flag for security teams on software supply chain risk, <https://www.reversinglabs.com/blog/circleci-hack-is-a-red-flag-for-security-teams-on-the-software-supply-chain-risk/>

# Conclusions sur le CI/CD

- C'est un outil de plus pour améliorer la qualité des livrables (documentation, rapport de tests, librairies, exécutables, etc).
- Pour éliminer du bug.
- Un outil collaboratif pour partager les résultats dans l'équipe et l'entreprise.
- Faire d'abord en local puis exécuter dans la plateforme CI/CD .
- S'inspirer des outils qu'on a vue dans ou l'IDE ou en testing pour écrire des scripts.
- Attention aux ressources sur les machines locales.
- Attention aux coûts sur le cloud.