

# CLOUD 101

## FORMATION PORTABLE

### VERSION FRANÇAISE



**BNP PARIBAS**

**Cloud**  
PROGRAM



# CLOUD 101 – VERSION FRANÇAISE

Approximativement 6hrs

CHART LEGEND :

	E-learning		theoretical		Content providers (BNPP, YouTube, IBM, online content)
--	------------	--	-------------	--	---

## AVANT DE COMMENCER

Guide de formation

10 min



Objectifs pédagogiques

10 min



## INTRODUCTION AU CLOUD COMPUTING

Introduction au Cloud Computing

10 min



Cloud : les enjeux de sécurité

10 min



## STRATÉGIE ET GOUVERNANCE CLOUD BNP PARIBAS

Introduction à la stratégie Cloud BNP Paribas et aux modèles de déploiement

30 min



Introduction à la gouvernance Cloud : Cloud Blueprint

90 min



## LE CLOUD EN ACTION

Introduction aux Conteneurs

15 min



Docker 101 : les concepts clés

30 min



Docker 101 : commandes principales

10 min



Introduction à Kubernetes

10 min



Introduction à l'approche Cloud Native

20 min



Introduction à l'architecture Microservices

5 min



## DÉCOUVRIR LE CLOUD PUBLIC IBM

Infrastructure du Cloud Public IBM

15 min



Catalogue du Cloud Public IBM

5 min



QUIZ FINAL (30 min) – à réaliser sur MySurvey  
**CLIQUEZ ICI POUR ACCÉDER AU QUIZ**



# AVANT DE COMMENCER



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



# GUIDE DE LA FORMATION

Cette **version du Cloud 101, entièrement portable**, vise à répondre aux problématiques de connexion au vu du contexte actuel.

Tous les contenus, qu'ils aient été créés spécifiquement pour BNP Paribas ou qu'ils soient issus de sources externes, ont été intégrés à cette version afin de vous permettre de continuer à être formé.

**Seules les vidéos Youtube nécessitent un accès Internet**, via vos outils BNP Paribas ou personnels (PCs, mobiles, etc).

**Le quizz reste cependant online**, via EchoNet.

Pour accéder facilement au portail, nous vous conseillons d'opter pour une connexion en heure creuse.



**BNP PARIBAS**

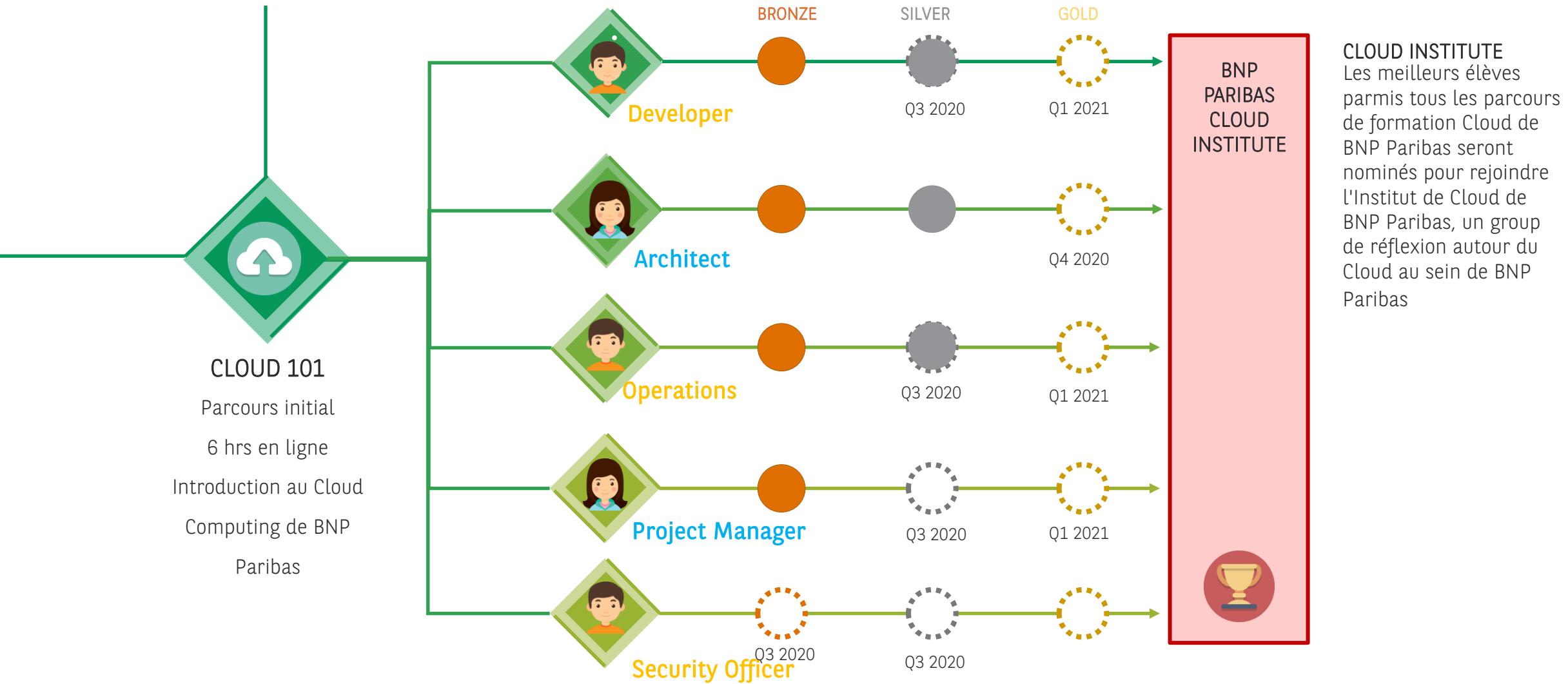
La banque d'un monde qui change



# Learning paths

## LEARNING PATHS

5 parcours principaux, combinant compétences méthodologiques et techniques. Chaque parcours de formation comporte 3 niveaux de maîtrise, liés à des certifications internes



**BNP PARIBAS**

The bank for a changing world



# Que retrouvons-nous derrière chaque niveau ?



## Cloud 101

Introduction théorique aux concepts généraux du Cloud Computing pour BNP Paribas



## Niveau Bronze

Le Cloud pour les néophytes : comprendre & appliquer les cas d'utilisation basiques du Cloud ( CD toolchain initialisation, lancer une application, supervision de l'utilisation d'un service...)



## Niveau Argent

Niveau intermédiaire : un mélange de formations basées sur des cas d'utilisation complexes (serverless development, micro-services mesh, ....) et d'une analyse par un expert d'une première expérimentation Cloud-native



## Niveau Or

Niveau avancé: des sessions de formation pratique de pointe pour se perfectionner, l'analyse par un groupe d'experts de cas d'expérimentation Cloud-native standards et complexes, une participation à la communauté Cloud (revue des niveaux Silver, animation de formations,...)



## Cloud Institute

Les meilleurs participants de chaque parcours de pourront être nominés pour rejoindre le Cloud Institute



**Chaque niveau est validé par un quiz final.  
Si le test est réussi vous obtiendrez une certification interne**



**BNP PARIBAS**

La banque d'un monde qui change

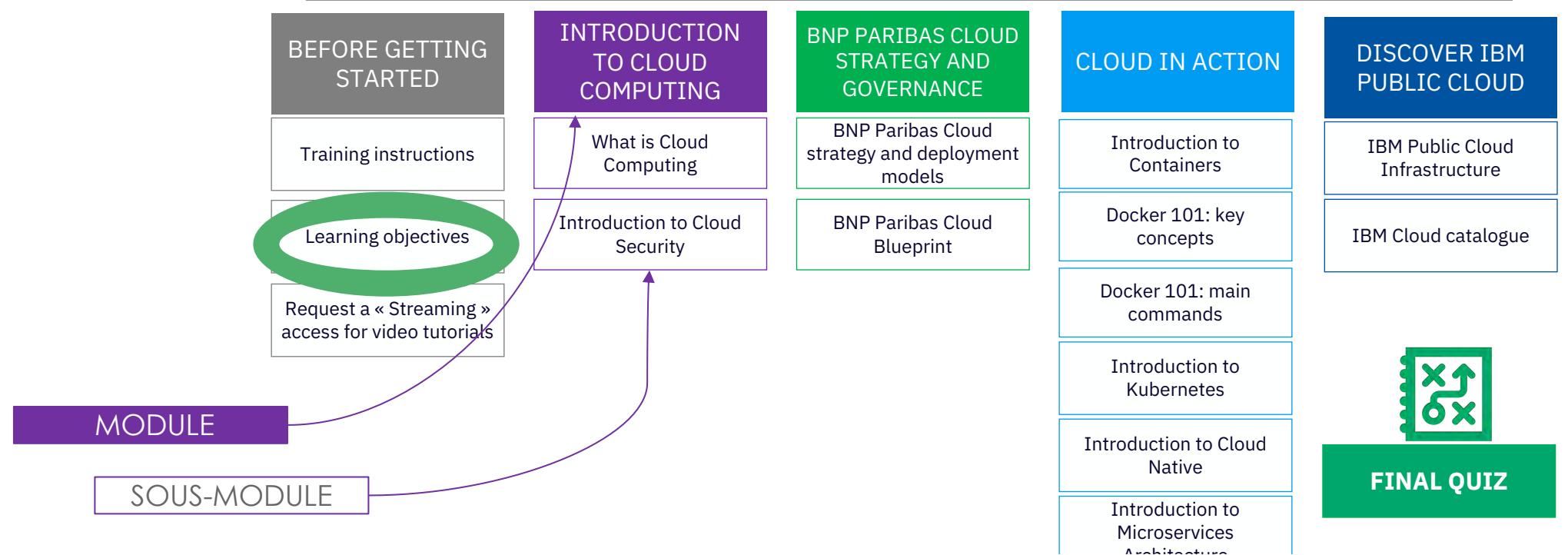


BNPP Classification : Internal

# L'architecture des cours

L'architecture de la formation est basée sur les objectifs d'apprentissage de chaque cours. Le cours est structuré en MODULES et SOUS-MODULES. Nous avons défini pour chaque module les objectifs d'apprentissage et vous proposons différents sous-modules pour atteindre ces objectifs

## CLOUD 101 – Training architecture



# Caractéristiques des contenus de formations

## L'approche adoptée pour l'alimentation des parcours est la suivante :

- Réutiliser les contenus externes considérés comme pertinents et adaptés aux objectifs pédagogiques de chaque cours. Ces contenus peuvent provenir de plusieurs sources (YouTube, site internet, articles...)
- Produire les contenus spécifiques au contexte BNP Paribas

## INFORMATIONS IMPORTANTES

Nous pouvons vous proposer des articles sur le web ou des vidéos sur YouTube dans le cadre des formations :

- Nous ne sommes pas responsables des publicités ou des listes de lecture vidéos suggérées automatiquement par YouTube.
- Nous n'approuvons ni ne soutenons les messages publicitaires que ces contenus peuvent contenir.
- Concernant les vidéos YouTube : ne soyez pas surpris par les blagues ou le « style» des YouTubers. Leur objectif est de populariser des concepts clés auprès d'un très large public. Ils peuvent parfois utiliser des analogies ou s'exprimer de manière non conventionnelle pour mieux faire passer leurs messages.



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal

# Validation des niveaux de formations

A la fin de chaque niveau, vous serez amener à passer un **court test pour valider les connaissances acquises.**

Dorénavant **les tests sont corrigés manuellement** - veuillez nous accorder un jour ou deux de délais.

En cas de réussite au test, vous obtiendrez une certification, félicitations !

En cas de non réussite, nous vous ferons un retour et vous aurez la possibilité de repasser le test.

   
**Chaque niveau est validé par un quiz final.**  
**En cas de réussite au test, vous obtiendrez une certification**





[RETOURNER AU SOMMAIRE  
DE LA FORMATION](#)



**BNP PARIBAS**

La banque d'un monde qui change



10

BNPP Classification : Internal



# OBJECTIFS DE LA FORMATION

## INTRODUCTION AU CLOUD COMPUTING

- Saisir les principales caractéristiques du Cloud Computing et les enjeux auxquels il répond
- Maîtriser les différents types de services Cloud (IaaS, PaaS, SaaS) et les différents modèles de déploiement (privé, public, hybride...)
- Appréhender les enjeux de sécurité liés à l'utilisation du Cloud

## STRATEGIE ET GOUVERNANCE CLOUD BNP PARIBAS

- Comprendre la stratégie Cloud de BNP Paribas et les différents modèles de déploiement de services Cloud
- Appréhender l'offre Cloud BNP Paribas et les principales règles encadrant l'utilisation de services Cloud au sein du Groupe
- Découvrir les nouveaux rôles pour accompagner le déploiement du Cloud
- Se familiariser avec le Cloud Blueprint BNP Paribas et la gouvernance mise en place

## LE CLOUD EN ACTION

- Comprendre le nouveau paradigme technologique introduit par l'approche Cloud Native
- Maîtriser les enjeux et opportunités sous-jacentes
- Appréhender les impacts en termes d'architecture, technologies et méthodes de travail
- Se familiariser avec les nouveaux concepts et technologies Cloud : Conteneurs Docker, Kubernetes et Microservices.
- Comprendre en quoi DevOps est un accélérateur du "move to Cloud"



**BNP PARIBAS**

La banque d'un monde qui change





RETOURNER AU SOMMAIRE  
DE LA FORMATION



**BNP PARIBAS**

La banque d'un monde qui change



12

BNPP Classification : Internal

# INTRODUCTION AU CLOUD COMPUTING



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



# INTRODUCTION AU CLOUD COMPUTING

## LIEN YOUTUBE :

<https://youtu.be/RwbIMBSr8o8>

## Comment retrouver la vidéo via la barre de recherche Youtube :



**Le cloud computing expliqué en 7 minutes**  
Cookie connecté • 112 k vues • il y a 2 ans  
Dans cette vidé, je vous explique tout ce qu'il y a à savoir sur le Cloud computing : - Que signifie l'expression "c'est dans ..."  
Sous-titres



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



RETOURNER AU SOMMAIRE  
DE LA FORMATION



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



# LES ENJEUX DE SÉCURITÉ

## IT TRADITIONNELLE vs CLOUD

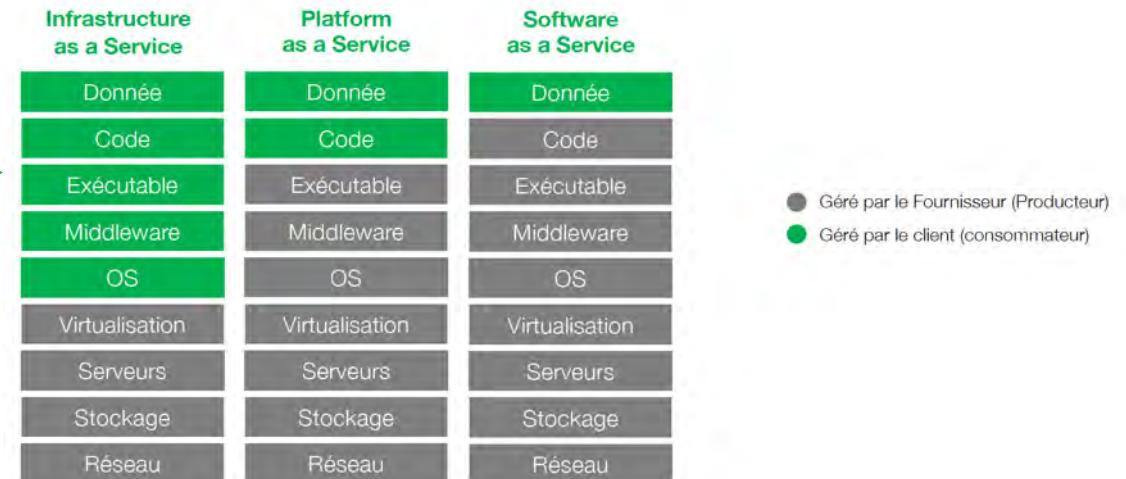
Traditionnellement, une entreprise avec une architecture dite « sur site » est responsable de la sécurité physique de ses infrastructures IT (centres de données, serveurs d'exécution, matériels réseau, etc).

Parmi les solutions fréquemment mises en place au sein d'entreprises, on retrouve : les pare-feu (ou firewall), proxy, anti-virus, solutions anti-spams, l'utilisation de VPN (réseau privé virtuel), les mises à jour régulières des moyens de protection, les sauvegardes de données, etc.

## CLOUD, VERS UNE RESPONSABILITÉ PARTAGÉE

Avec le Cloud Computing et la mise à disposition par un fournisseur d'un réseau informatique facilité, la responsabilité n'est plus portée seule par l'entreprise mais partagée avec le fournisseur. On distingue ainsi généralement la « Sécurité du Cloud », qui est sous la responsabilité du fournisseur, de la « Sécurité dans le Cloud », sous la responsabilité de l'entreprise cliente.

En fonction du modèle de Cloud choisi par l'entreprise (IaaS, PaaS, SaaS), les responsabilités de chacun et la répartition des tâches sécuritaires varient :





# LES ENJEUX DE SÉCURITÉ

## 3 PILIERS SECURITAIRES

Pour une entreprise, le passage au cloud induit ainsi un changement dans l'approche de la sécurité : au contrôle traditionnel des accès s'ajoute le contrôle des usages. La sécurité doit alors être approchée sous l'angle d'un cycle de vie et les règles de sécurité étroitement liées aux données.

Quel que soit le modèle choisi, 3 piliers sécuritaires restent toujours de la responsabilité de l'entreprise pour une sécurité maximisée :

### 1 - La protection des données

La nature du cloud public permet une collaboration mondiale. En conséquence, des données peuvent accidentellement être là où elles ne devraient pas. Cela est particulièrement problématique à l'heure où le règlement général de l'UE sur les données personnelles (RGPD) et les réglementations du régulateur bancaire se font de plus en plus strictes.

Pour protéger ses données, l'entreprise doit :

- **Identifier et classifier ses données** en fonction qu'elles soient publiques, confidentielles ou sensibles (cf. Blueprint)
- **Chiffrer ses données** enregistrées sur les supports persistants (données au repos), ses données en mémoire sur les supports non persistants (données en usage) et ses données qui peuvent être interceptées alors qu'elles circulent sur le réseau (données en transit) avec un chiffrement pour se protéger de l'exploitation par un tiers non autorisé
- **Mettre en place une gestion des clés de chiffrement** afin d'être en capacité de générer, distribuer, stocker et détruire les clés cryptographiques selon ses besoins.





# LES ENJEUX DE SÉCURITÉ

## 2 - La gestion des identités et des accès

Pour sécuriser un environnement Cloud, il faut également pouvoir **définir qui a besoin de quoi et qui peut faire quoi**. Cela passe ainsi par la **mise en place d'une gouvernance d'identités** basée sur la gestion des identités et du contrôle d'accès (IAM, Identity and Access Management).

Associer des rôles et des priviléges à des identités permettra ainsi de maîtriser l'accès aux données, services, applications, etc.

Avec cette gouvernance, l'entreprise pourra s'assurer qu'une application accède bien aux données dont elle a besoin ou qu'un utilisateur détient les bons accès pour faire tourner cette application.

## 3 - Le monitoring actif

Enfin, il convient de mettre en place un contrôle de sécurité et de conformité actif, permettant aux équipes Sécurité de gagner en visibilité, en continu, sur l'intégralité de l'environnement et donc de prévenir de potentielles vulnérabilités.

Le Cloud offrant la possibilité de créer et de déployer rapidement des applications à l'échelle mondiale, il est nécessaire de pouvoir identifier rapidement et de manière dynamique les configurations risquées, les menaces réseau, les comportements suspects des utilisateurs, les malwares, fuites de données, vulnérabilité des hôtes, etc.

Ce monitoring actif permet ainsi **d'assurer une protection continue et d'être en capacité de réagir immédiatement**.





# LES ENJEUX DE SÉCURITÉ

## DE DEVOPS À DEVSECOPS

Si l'approche DevOps a fait ses preuves en permettant de livrer des applications et logiciels qualitatifs dans des délais courts tout en apportant de la valeur aux entreprises, elle semble cependant négliger une facette importante du développement : la sécurité.

En effet, investir dans plus de sécurité réseau, pares-feux, etc. ne permet pas de résoudre les problématiques de sécurité générées par les développements.

Il faut donc repenser la manière dont les projets de développement sont conçus, pour une sécurité de bout en bout : construction, gestion et fonctionnement

L'approche DevOps doit donc évoluer vers celle de DevSecOps afin de réfléchir à comment la sécurité va s'intégrer dans tous les aspects du cycle de vie et des étapes du projets afin de sécuriser, et les applications créées, et les systèmes d'information.

C'est toute l'architecture qui s'en trouvera impactée : la façon de concevoir l'application, le type de données à utiliser, le degré de classification, la gestion des accès, les charges de travail, etc.



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



RETOURNER AU SOMMAIRE  
DE LA FORMATION



**BNP PARIBAS**

La banque d'un monde qui change



20

BNPP Classification : Internal

# STRATÉGIE ET GOVERNANCE CLOUD BNP PARIBAS



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal

# BNP PARIBAS CLOUD STRATEGIE ET MODELES DE DEPLOIEMENT



**BNP PARIBAS**

**Cloud**  
PROGRAM

# SOMMAIRE DU DOCUMENT

---

## STRATEGIE CLOUD

Comprendre la stratégie Cloud de BNP Paribas

## LES CLOUDS BNP PARIBAS

Découvrir les offres et modèles de déploiement du Cloud au sein de BNP Paribas

## NOUVEAUX ROLES

Se familiariser avec les nouveaux rôles pour soutenir le déploiement du Cloud au sein du groupe

## FAQ CLOUD

S' informer en consultant les questions les plus fréquemment posées



**BNP PARIBAS**

The bank for a changing world



# CLOUD STRATEGIE

Comprendre la stratégie BNP Paribas



**BNP PARIBAS**

The bank for a changing world



# TRAJECTOIRE CLOUD DE BNP PARIBAS



→ Après 4 ans dans un environnement Cloud Privé, BNP Paribas étend sa stratégie Cloud pour :

- Bénéficier des avantages de chaque environnement (Public, Privé ou Dédié) et avoir le choix du Cloud le plus approprié en fonction des besoins
- Augmenter le panel des services mis à sa disposition et bénéficier d'un meilleur accès aux innovations déployées dans les Clouds Publics
- Réduire le risque de vulnérabilité vis-à-vis des problèmes de panne de datacenters
- Avoir une meilleure maîtrise de la localisation du stockage des données sensibles
- Optimiser ses coûts en adaptant les solutions et Clouds en fonction des besoins



**BNP PARIBAS**

The bank for a changing world



# BNP PARIBAS INVESTIT DANS SA TRANSFORMATION VERS LE CLOUD

Les Echos

À la une Idées Économie Politique Monde Tech-Médias Entreprises Bourse Finance - Marchés Régions >

## « Notre budget IT dépasse les 6 milliards d'euros à l'année »

Six jours avant l'ouverture de VivaTech, le patron de la première banque française explique sa stratégie numérique. Face aux GAFA, il défend notamment la solution de paiement LyfPay, développée avec Crédit Mutuel, et qui probablement demain le sera avec d'autres grandes banques européennes.

Lire plus tard | Banque & Assurances | [Twitter](#) [Facebook](#) [LinkedIn](#)



### Quelles ont été vos grandes orientations sur le plan technologique ?

Notre client est au centre du dispositif. Ce qu'il nous demande, c'est davantage de données pertinentes, afin de le guider - que ce soit en termes de pilotage de l'épargne, de trésorerie, de conseil en investissement, de nouveaux usages... - dans un univers toujours plus complexe, en raison justement de la profusion de données. Dans ce contexte, il nous faut être très agile, mais aussi parfaitement sécurisé. Derrière cela, il y a un **enjeu de technologie**. On connaît tous le « **cloud public** » qui est un modèle très ouvert avec des données presque accessibles par tous. Mais s'agissant de la banque, les données de nos clients sont privées sauf pour un usage qui permet de mieux les conseiller. Les technologies cloud dans notre secteur sont en train de se construire, on les appelle **cloud privé-public ou hybride**. Elles nous donneront **la puissance d'un cloud public, mais avec la sécurité d'une infrastructure privative**. Nous sommes parmi les seules banques en Europe à avoir déjà un **cloud privé**, que nous avons développé seuls ; et nous développons maintenant le futur **cloud hybride** avec IBM.

Accédez à l'article complet [ici](#)



BNP PARIBAS

The bank for a changing world



# UNE TRANSFORMATION CONTINUE POUR RELEVER LES PRINCIPAUX DÉFIS

## MODIFICATION DU COMPORTEMENT ET DES ATTENTES DES CLIENTS

Permet d'interagir numériquement avec différents domaines d'activité, d'accéder à un code open-source et à des services avancés, de développer des applications bancaires numériques en quelques minutes

## CONTEXTE RÉGLEMENTAIRE STRICT

Répondre aux exigences réglementaires extrêmes de l'industrie financière pour être à jour sur plus de 200 exigences de conformité européennes et internationales

## DES DONNÉES BANCAIRES DE PLUS EN PLUS SENSIBLES

Fournir un accès sécurisé à l'informatique et au stockage des données des clients et d'autres informations sensibles, fournir des données fiables aux clients

BNP Paribas accélère sa transformation numérique pour offrir les meilleurs services dans le Cloud et renforcer la sécurité et la confidentialité des données bancaires. Pour exploiter les technologies émergentes et concevoir de nouvelles expériences clients, BNP Paribas a besoin des **tirer profit des avantages d'innovation et de rapidité d'un Cloud public toute en appliquant la haute sécurité d'un Cloud privé.**

BNP Paribas, en partenariat avec IBM Cloud, construit son propre Cloud Dédié BNP Paribas, disponible en juillet 2020

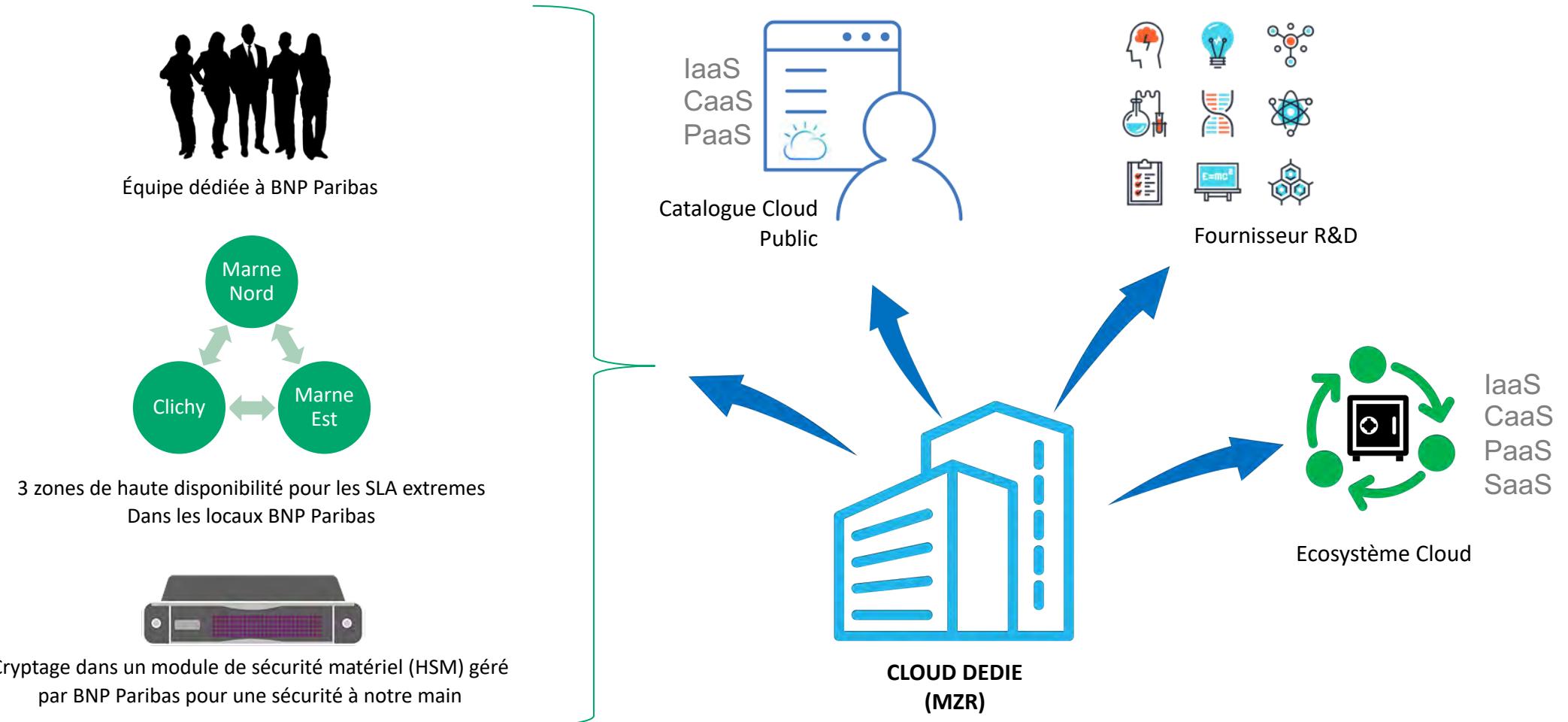


**BNP PARIBAS**

The bank for a changing world



# QU'EST CE QUE LE CLOUD DEDIEE BNP Paribas ?



## TROIS CARACTERISTIQUES UNIQUES

Une équipe dédiée, le cryptage géré par BNP Paribas, un hébergement dans nos locaux

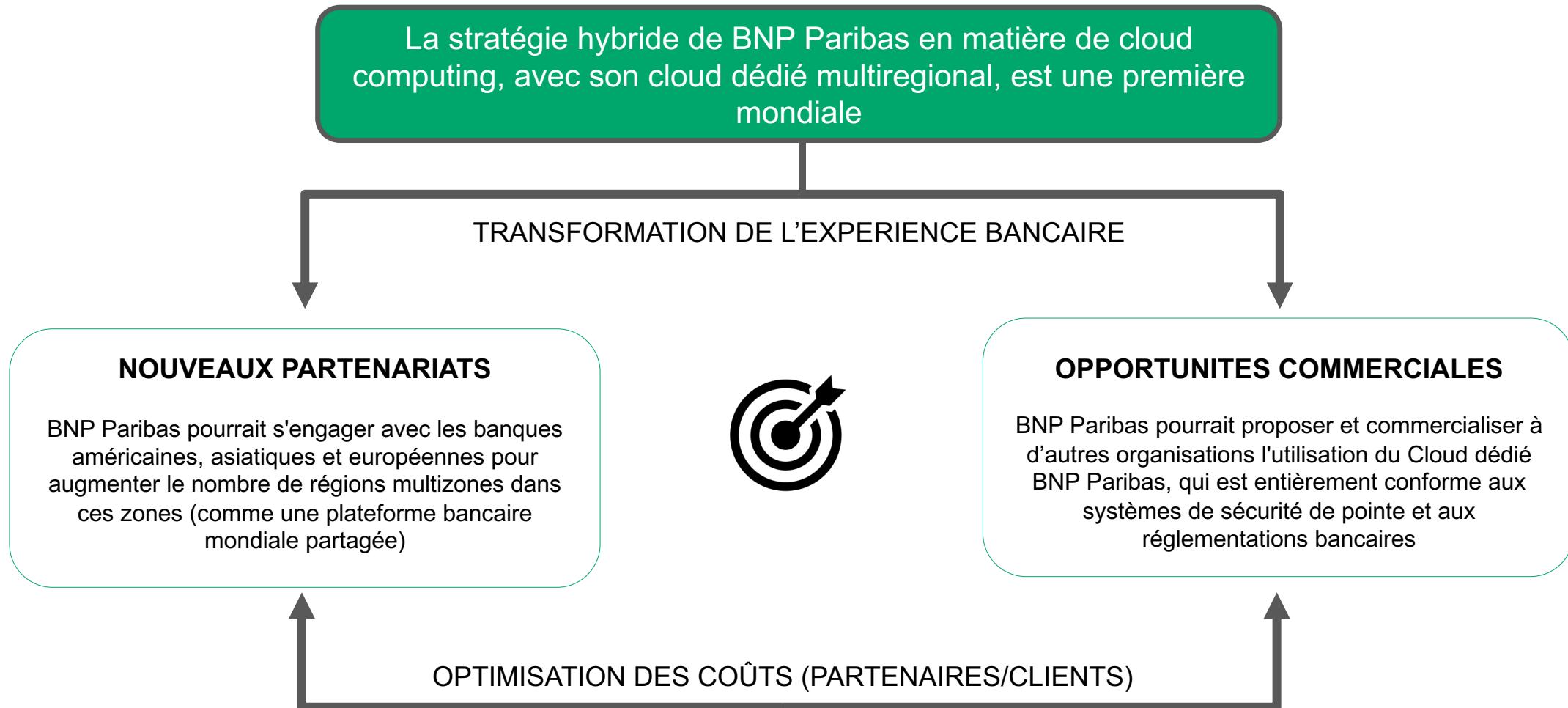


**BNP PARIBAS**

The bank for a changing world



# L'INNOVATION GRACE AU CLOUD, GÉNÉRATRICE DE VALEUR AJOUTÉE ET D'OPPORTUNITÉS COMMERCIALES



**BNP PARIBAS**

The bank for a changing world



# LES CLOUDS BNP Paribas

Découvrir les offres et modèles de déploiement  
du Cloud au sein de BNP Paribas



**BNP PARIBAS**

The bank for a changing world



# POUR RAPPEL LE “CLOUD” VIENT SOUS PLUSIEURS FORMES :

## MODELES DE SERVICE CLOUD



Note : il y a beaucoup d'autres types de XaaS, beaucoup d'entre eux sont simplement du Buzz as a Service

## MODELES DE DEPLOIEMENT CLOUD



Les services et les modèles de déploiement du cloud sont détaillés dans le Cloud Blueprint. Nous vous invitons à le consulter pour mieux comprendre l'analogie avec la voiture. Accès au Cloud Blueprint [ici](#)



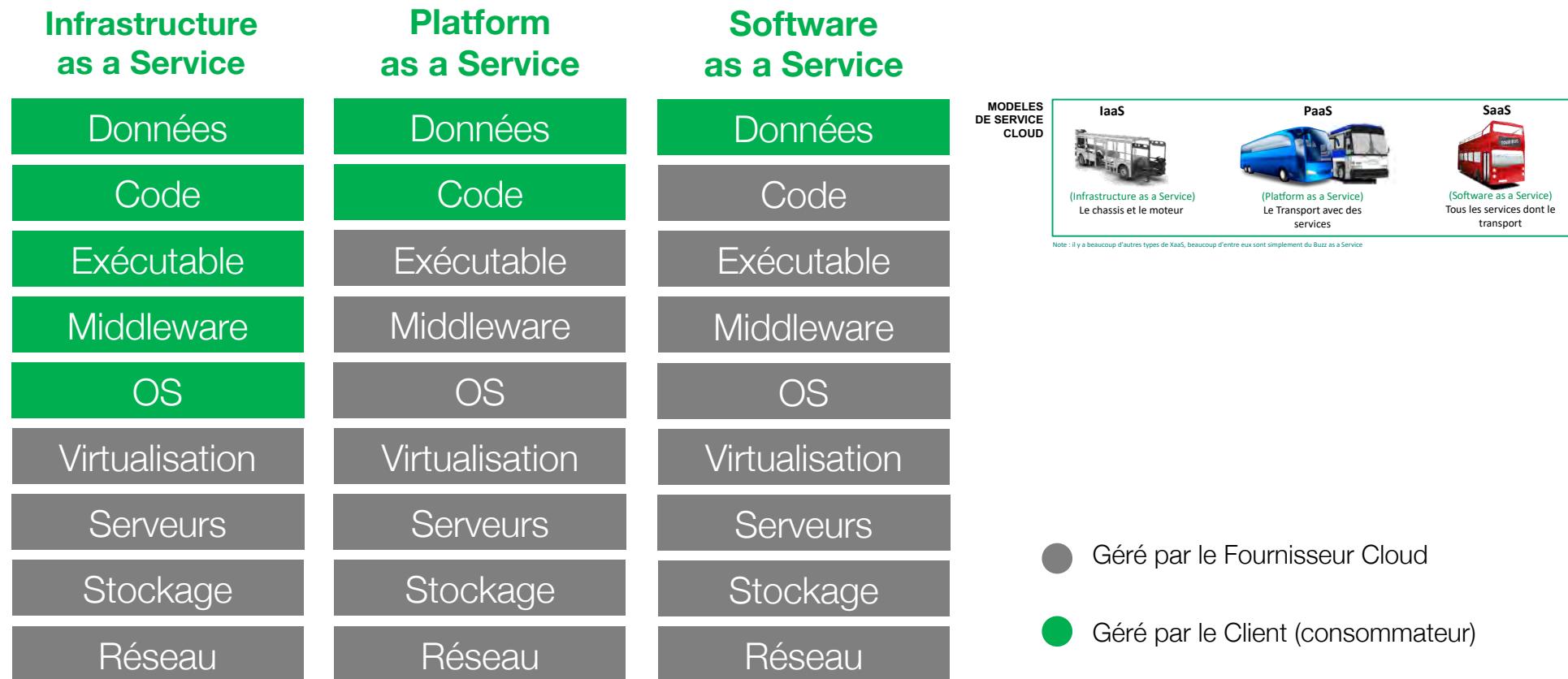
**BNP PARIBAS**

The bank for a changing world



# ZOOM SUR LES MODELES DE SERVICE CLOUD

Les responsabilités sont séparées entre ce que le fournisseur délivre et que BNP Paribas doit délivrer. A noter que vis-à-vis de nos clients, nous avons la responsabilité de bout en bout.



# MODELES DE SERVICE CLOUD: EMERGENCE DE NOUVEAUX MODELES

Depuis les 3 premiers modèles de services Cloud, un grand nombre de modèles sont apparus, voici les plus utilisés :

Baremetal as a Service	Infrastructure as a Service	Container as a Service	Platform as a Service	Software as a Service
Données	Données	Données	Données	Données
Code	Code	Code	Code	Code
Exécutable	Exécutable	Exécutable	Exécutable	Exécutable
Middleware	Middleware	Middleware	Middleware	Middleware
OS	OS	Conteneur/OS	OS	OS
Virtualisation	Virtualisation	Virtualisation	Virtualisation	Virtualisation
Serveurs	Serveurs	Serveurs	Serveurs	Serveurs
Stockage	Stockage	Stockage	Stockage	Stockage
Réseau	Réseau	Réseau	Réseau	Réseau

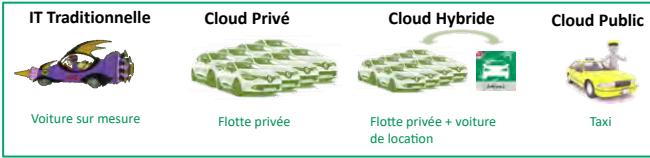


- Géré par le Fournisseur Cloud
- Géré par le Client (consommateur)

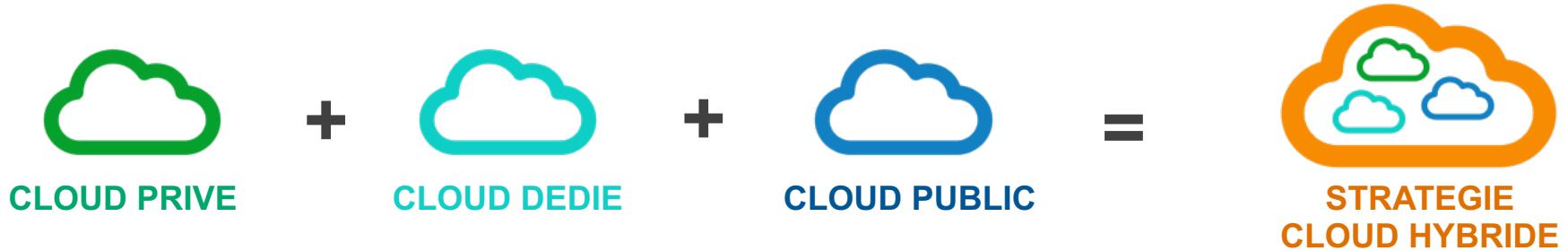


# MODELES DE DEPLOIEMENT CLOUD

## LA STRATEGIE BNP Paribas



Nous adoptons une stratégie hybride pour maximiser les capacités et tirer profit de chaque types de Clouds



### OBJECTIFS D'UNE STRATEGIE HYBRIDE



#### INNOVATION\*

Profiter des services innovants fournis par les principaux fournisseurs de services Cloud



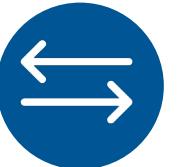
#### SECURITE\*

Conserver le contrôle des données sensibles



#### BUDGET\*

Maîtriser le budget de l'entreprise en choisissant les offres adaptées



#### SCALABILITE\*\*

Déployer les instances sans contrainte de capacité



#### PERFORMANCE\*\*

Bénéficier de la performance adaptée (réseau, traitement, etc.) en fonction des besoins de chaque cas d'utilisation

\* Aspects spécifiques à la stratégie hybride  
\*\* amélioration par rapport au Cloud privé



**BNP PARIBAS**

The bank for a changing world



# LES CLOUDS BNP PARIBAS :

## PLUSIEURS OPTIONS - PLUSIEURS MODELES OPERATIONNELS



Dans les diapositives suivantes, nous allons détailler chaque modèle de déploiement du cloud

Modèle de  
Déploiement Cloud  
(Cloud Blueprint type)

**CLOUD PRIVE**  
(Blueprint cloud type : 1)

Fournisseur:



Dispositif:

BNPP Private Clouds

Catalogue  
de services

30 Cloud services



Conçu par:



Opéré par:

**CLOUD DEDIE**  
(Blueprint cloud type : 2)



BNPP Dedicated Cloud  
(Paris' MZR)

120 Cloud services



**CLOUD PRIVE VIRTUEL**  
(adaptation du Cloud public classique avec isolement spécifique)  
(Blueprint Cloud type 4)



IBM Cloud's  
Virtual Private Cloud

200+ Cloud services



Azure, AWS, others  
VPC

200+ Cloud services



Cloud Hybride

Multi-Cloud



**BNP PARIBAS**

The bank for a changing world



# LES CLOUDS BNP PARIBAS :

## Zoom sur les Clouds Privés BNP Paribas



Modèle de  
Déploiement Cloud  
(Cloud Blueprint type)

CLOUD PRIVE  
(Blueprint cloud type : 1)

Fournisseur:

ITCLOUD IL2

Dispositif:

BNPP Private Clouds

Catalogue  
de services

30 Cloud services



Conçu par:

Opéré par:



Opérée par:

Services IaaS et PaaS de BP<sup>2I</sup> et IPS

Services IaaS et PaaS par la marketplace CIB ITO

Hébergé dans les locaux BNP Paribas

Un petit ensemble de services ont été  
développés et sont exposés

BNP Paris tire parti de la communauté open source et des  
fournisseurs de logiciels pour créer et packager des services

BNP Paribas ajoute de la valeur, de la sécurité et de la conformité à ces  
services grâce à ses propres équipes BNPP

BNP Paribas exploite tous ces services par elle-même  
ou des sous traitants

Déjà disponible

Azure, AWS, others  
VPC

200+ Cloud services



Multi-Cloud



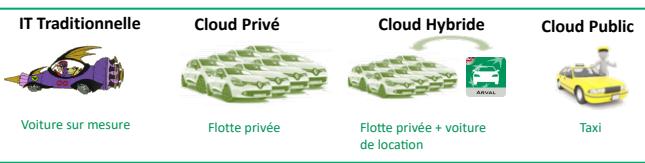
BNP PARIBAS

The bank for a changing world



# LES CLOUDS BNP PARIBAS :

## Zoom sur le Cloud dédié BNP Paribas, disponible en Juillet 2020



Modèle de Déploiement Cloud (Cloud Blueprint type)

CLOUD PRIVE  
(Blueprint cloud type : 1)



IL2

BNPP Private Clouds

30 Cloud services



Development team



Development team

Fournisseur:

Dispositif:

Catalogue de services

Conçu par:

Opéré par:

CLOUD DEDIE  
(Blueprint cloud type : 2)



IBM Cloud

BNPP Dedicated Cloud  
(Paris' MZR)

120 Cloud services



Development team



Operation team



Dedicated Operation team

Cloud Hybride

CLOUD PRIVE VIE

(adaptation du Cloud public classique à  
(Blueprint Cloud type : 3))

Disponible au 1er juillet 2020



Le cloud dédié est hébergé par  
BNP Paribas

Un sous-ensemble important du catalogue de  
services d'IBM Cloud sera disponible

L'équipe IBM Cloud qui développe tous les services à  
travers le monde fournira les services BNPP au même  
rythme

Les services publics seront exploités par une  
équipe IBM Cloud

Les services sensibles qui supportent les données  
BNP Paribas  
seront exploités par une équipe dédiée uniquement à  
BNP Paribas (BNPP, BP<sup>2</sup>I et IBM Cloud)



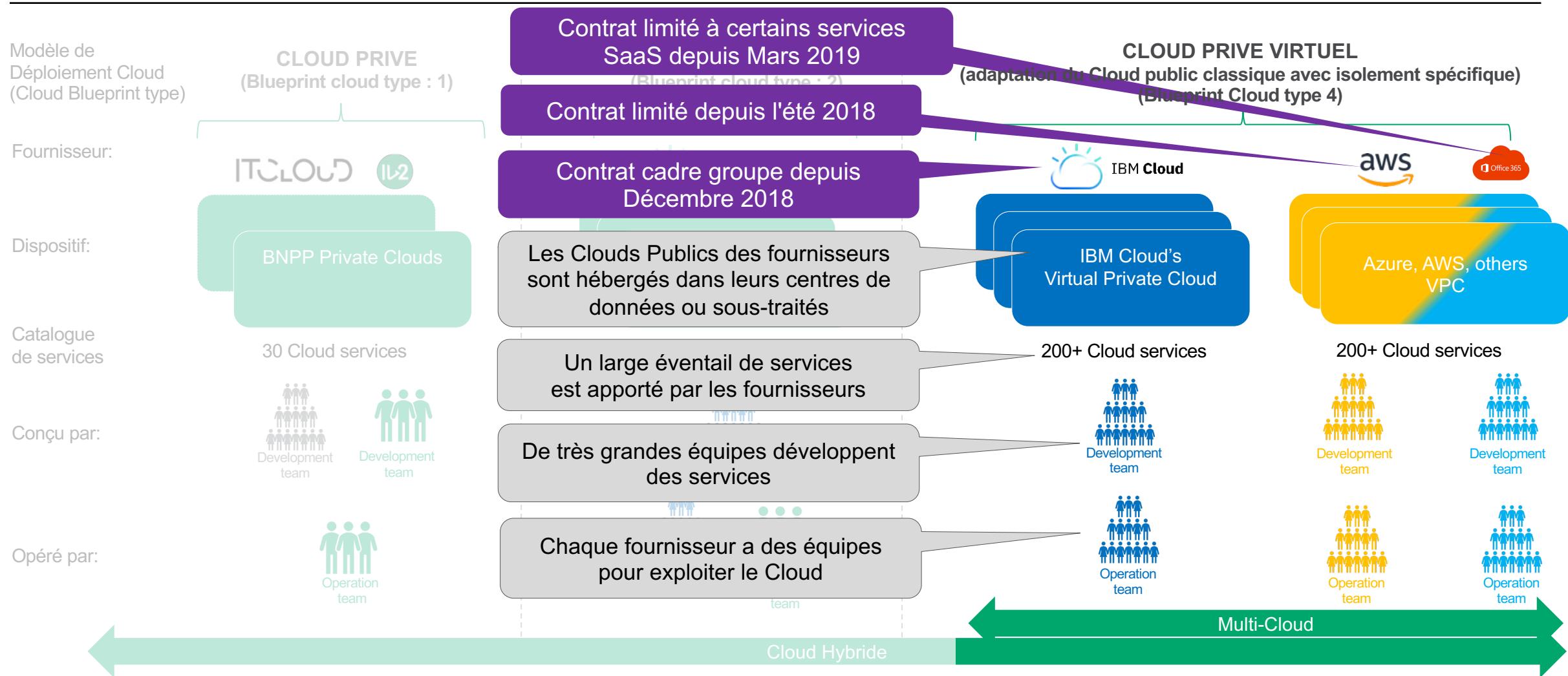
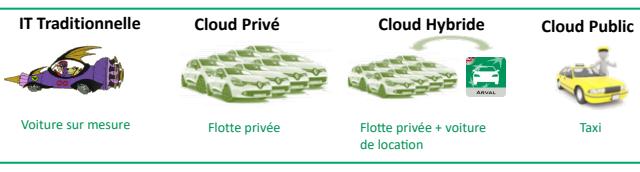
BNP PARIBAS

The bank for a changing world



# LES CLOUDS BNP PARIBAS :

# Zoom sur les Clouds privés virtuels



**BNP PARIBAS**

## The bank for a changing world



# LES CLOUDS BNP PARIBAS :

## Hybride versus multi-Cloud



Modèle de  
Déploiement Cloud  
(Cloud Blueprint type)

CLOUD PRIVE  
(Blueprint cloud type : 1)

Fournisseur:



IL2



30 Cloud services

Dispositif:

CLOUD DEDIE  
(Blueprint cloud type : 2)



120 Cloud services

Catalogue de services

Conçu par:

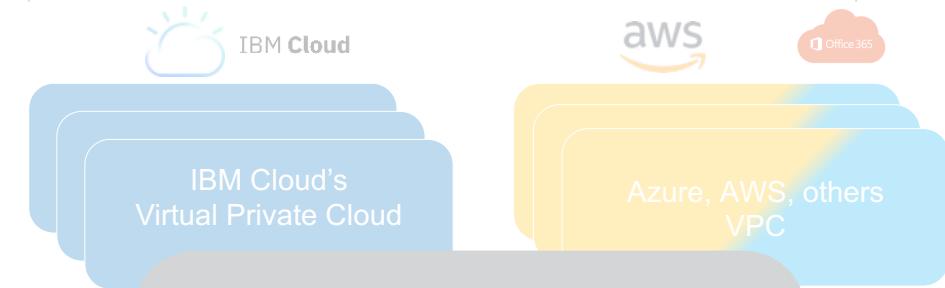
Opéré par:

**Les acteurs du Cloud définissent « Cloud hybride » comme étant l'utilisation de plusieurs Cloud de différents types.**



Cloud Hybride

CLOUD PRIVE VIRTUEL  
(adaptation du Cloud public classique avec isolement spécifique)  
(Blueprint Cloud type 4)



**Les acteurs du Cloud définissent « Multi-Cloud » comme étant l'utilisation de plusieurs clouds du même type provenant de différents fournisseurs**



BNP PARIBAS

The bank for a changing world



# LES RÈGLES D'USAGE DU CLOUD DEFINIES DANS LE CLOUD BLUEPRINT

BNPP Rules / Type of Cloud		1	2	3	4	5	6
<b>Data protection rules</b>	Masked Data	✓	✓	✓	✓	✓	✓
	Secret Data	!	!	✗	✗	✗	✗
	Sensitive personal data	!	!	✗	✗	✗	✗
	Protected strategic asset	✓	✓	✗	✗	✗	✗
	Confidential data	✓	✓	!	✗	✗	✗
	Restricted Data Personal Identifiable Data	✓	✓	!	!	!	!
<b>Service Continuity rules</b>	Process of Material Importance	✓	✓	✓	✓	✗	✓
	Other	✓	✓	✓	✓	✓	✓
<b>Premises for the Cloud</b>		On	On	Off	Off	Off	Off
<b>Cloud examples</b>		IT Cloud, CloudNg, IV2	BNPP Dedicated Cloud		IBM VPC, AWS VPC, Azure VPC	Office365, Service Now, SalesForce	

Cette matrice est un résumé des règles d'usage définies dans le Cloud Blueprint



# NOUVEAUX ROLES

Se familiariser avec les nouveaux rôles pour accompagner le déploiement du Cloud



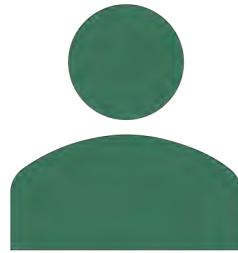
**BNP PARIBAS**

The bank for a changing world



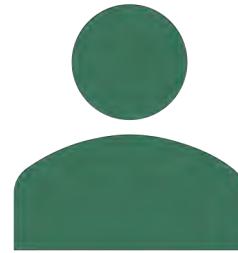
# DE NOUVEAUX ROLES POUR ACCOMPAGNER LE DEPLOIEMENT DU CLOUD

Trois nouveaux rôles émergents au sein du Groupe pour soutenir et accélérer le déploiement et l'adoption du Cloud :



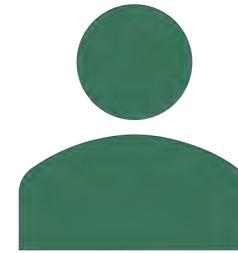
**FinOps**

FinOps fournit des conseils sur la façon d'utiliser efficacement les services Cloud. Il aide les équipes à mieux comprendre et contrôler les dépenses Cloud. Il contribue à développer une communication forte entre les équipes de DevOps et les équipes financières.



**Offering Manager**

L'Offering Manager guide les équipes crossfonctionnelles pour définir, construire et promouvoir avec succès les offres clouds BNP Paribas, conçues pour un marché d'utilisateurs. Les utilisateurs profiteront d'un expérience de bout en bout de l'offre permettant ainsi d'utiliser cette offre de façon optimale, et par conséquent, permettre à BNP Paribas de maintenir / développer le modèle commercial de l'offre.



**SRE**

Un "Service Reliability Engineer" est chargé de la disponibilité, de la qualité et de la résilience des services et des applications Clouds, et ce, pour chaque type de Clouds. Son principal objectif est d'assurer l'accord de niveau de service (SLA) de son périmètre.



**BNP PARIBAS**

The bank for a changing world



# FAQ

S'informer en consultant les questions les plus fréquemment posées



**BNP PARIBAS**

The bank for a changing world



# Foire aux questions

---

- Est-ce que la stratégie Cloud BNP Paribas va uniquement avec le Cloud IBM ?
  - Non, la stratégie est d'aller avec IBM Cloud d'abord. L'investissement pour un Cloud Dédié (type 2) nous amène à choisir le Cloud IBM comme notre premier fournisseur de Cloud pour toutes les charges de travail éligibles.
- Puis-je utiliser n'importe quelle instance publique\* d'IBM Cloud ?
  - Oui, comme pour toute charge de travail et applications qui seraient conformes au type 4 ou au type 5. Nous vous encourageons vivement à suivre le processus d'achats groupe afin d'obtenir les meilleures conditions.
- Pourquoi devrais-je d'abord utiliser le Cloud public\* IBM pour accéder à notre Cloud dédié ?
  - Notre Cloud dédié est une instance particulière d'IBM Cloud, vous obtenez donc le même contenu de part et d'autre, et vous aurez un parcours plus facile pour redéployer vos charges de travail du Cloud public vers le Cloud dédié.
- Puis-je utiliser un autre Cloud public\* qu'IBM ?
  - Oui, comme pour toute charge de travail et les applications qui seraient conformes au type 4 ou au type 5. Nous vous encourageons à suivre le processus d'approvisionnement afin d'obtenir les meilleures conditions pour consommer ces Cloud. Notez que la migration de votre application d'un autre fournisseur vers le Cloud dédié doit être prise en compte dans vos projets

\* Public or Virtual Private Cloud

---



# Foire aux questions

---

- Nous avons un contrat Cloud avec AWS, pourquoi ne pas l'utiliser ?
  - Un contrat a été signé pour le groupe avec des conditions précises, pas de la même manière qu'avec IBM Cloud. Il n'offre pas la même protection qu'IBM Cloud ou que le Cloud dédié BNPP, ni aucun moyen de migrer facilement de l'un à l'autre. Nous vous encourageons vivement à passer par le processus d'achats groupe et par IFS.Alpha/Bivwak pour être intégré correctement à AWS.
- Nous avons signé un contrat Cloud avec Microsoft, pourquoi ne pas l'utiliser ?
  - Le contrat récemment signé avec Microsoft est centré sur les outils Collaboratifs, et nous étudions comment et si cela pourrait couvrir les autres offres de Microsoft, dont Azure. Cette dernière partie est encore en cours de négociation
- Nous avons signé un contrat Cloud avec Oracle, pourquoi ne pas l'utiliser ?
  - Le contrat encore plus récent avec Oracle est utilisé pour l'évaluation des offres Oracle Cloud uniquement et limité à quelques organisations. Nous travaillons à identifier les offres et la conformité de ce Cloud à nos besoins et contraintes.
- Dois-je passer par ITG pour consommer le public IBM Cloud ou VPC ?
  - Non, le contrat cadre est défini entre le groupe et IBM Cloud. D'autre part, le contrat pour le Cloud dédié appartient à ITG. Ce serait une meilleure option, si vous avez besoin du Cloud dédié, d'obtenir toute votre consommation IBM Cloud à travers ITG.



**BNP PARIBAS**

The bank for a changing world



# Foire aux questions

---

- Le Cloud dédié BNP Paribas et le MZR sont-ils une seule et même chose ?
  - Oui, MZR (Multi Zone Region) est le nom technique de la solution IBM pour fournir le Cloud dédié de BNP Paribas. Donc "la MZR" et le Cloud dédié sont une seule et même chose. Notez qu'IBM Cloud a de multiples constructions appelées MZR à travers le monde, puis se réfère souvent à notre instance comme la MZR de BNPP. Veuillez utiliser le terme Cloud Dédié au lieu de MZR.
- Est-ce que le Cloud dédié BNPP est un "One of Kind" spécialement conçu pour BNPP ?
  - Jusqu'à présent, nous sommes le premier client d'un tel Cloud dédié à une seule organisation. Comme toute entreprise réglementée recherchant les mêmes options, nous nous attendons à ce que d'autres institutions adoptent une approche similaire. Le Programme Cloud a le devoir d'empêcher toute déviation menant à rendre le Cloud Dédié tellement unique qu'il ne puisse plus être recevoir les mises à jour de services Cloud.
- Y a-t-il une raison de garder un pur Cloud Privé vs le Cloud Dédié ?
  - Oui, il y a de multiples raisons telles que le modèle financier (par exemple prêter de la ressource par opposition à posséder la ressource pour une utilisation à long terme), notre maturité sur le IaaS (comme VMware) par opposition à celle sur le Platform-as-a-Service, bien sûr équilibrée avec l'exigence de la masse critique de compétences et volumes.



**BNP PARIBAS**

The bank for a changing world



# Foire aux questions

---

- Qu'est-ce qu'un VPC ?
  - VPC signifie Virtual Private Cloud. C'est une solution logique pour séparer les ressources entre les clients. Souvent basé sur la ségrégation du réseau et l'accès aux ressources de calcul et de stockage.
- Qu'est-ce qu'un MZR ou un SZR ?
  - MZR est l'abréviation de Multi Zone Region et SZR est l'abréviation de Single Zone Region
  - Une région dans la terminologie des Cloud se rapporte à un lieu géographique
  - Une zone dans la terminologie des Cloud est en fait une zone de disponibilité, ce qui signifie un ensemble cohérent de fonctionnalités, un accès réseau fonctionnant indépendamment d'une autre zone.
  - MZR signifie donc que dans un lieu donné, une haute disponibilité sur 3 zones ou plus (de disponibilité) est fournie, alors qu'un SZR vient sans redondance.
- Le SaaS que nous utilisons doit-il être conforme au Cloud Blueprint ?
  - Bien sûr, les offres SaaS doivent suivre les mêmes règles que IaaS et PaaS.
- N'avons nous pas aussi des contrats avec les fournisseurs de SaaS ?
  - Notre contrat le plus récent avec Microsoft porte sur la fourniture des services Office 365 au groupe.
  - Nous travaillons à l'identification de la manière d'étendre les contrats locaux avec les fournisseurs SaaS afin d'améliorer le processus d'achat ainsi que la sécurité et la conformité de ces offres.



**BNP PARIBAS**

The bank for a changing world



# FIN DU DOCUMENT



**BNP PARIBAS**

**Cloud  
Program**



RETOURNER AU SOMMAIRE  
DE LA FORMATION



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



# INTRODUCTION À LA GOUVERNANCE CLOUD : CLOUD BLUEPRINT

## Group Cloud Blueprint pour Managers



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal

# Group Cloud Blueprint

## pour Managers



Group Cloud Blueprint pour les Managers - V1b

Décembre 2019



**BNP PARIBAS**

The bank  
for a changing  
world

## **SYNTHESE**

<b>QU'EST-CE QUE LE <i>CLOUD COMPUTING</i> ?</b>	<b>2</b>
<b>LE CLOUD : SOURCE D'OPPORTUNITES</b>	<b>3</b>
<b>CLOUD PUBLIC ET NOUVELLES REGULATIONS</b>	<b>4</b>
<b>CLOUD PUBLIC ET RISQUES INFORMATIQUES</b>	<b>5</b>
<b>CONSTRAINTES D'UTILISATION DU CLOUD</b>	<b>6</b>
<b>TYPES DE DEPLOIEMENT CLOUD</b>	<b>8</b>
<b>REGLES D'UTILISATION DES CLOUDS</b>	<b>10</b>
<b>GOUVERNANCE STRATEGIQUE</b>	<b>12</b>
<b>ANNEXES</b>	<b>13</b>

**Edition :** Décembre 2019

**Sponsors :** Bernard Gavgani – Group CIO  
Christophe Boulangé – Cloud Program Director

**Editeur :** IT Group

**Contacts :** Laurent Piau, Rob Horsfall, Thierry Moineau

**Intranet :** <https://weshare.group.echonet/sites/itgcloud>

# Synthèse

## Objectifs

Ce document est une version pédagogique du ***Group Cloud Blueprint***. Il en présente les conclusions sans entrer dans des dimensions techniques.

L'objectif du *Cloud Blueprint* est de promouvoir une utilisation bénéfique et sécurisée des services Cloud au sein des Entités de BNP Paribas afin de répondre aux besoins actuels et émergents. Il présente les principes directeurs, applicables à l'ensemble du Groupe, pour la sélection des différentes solutions Cloud et décrit les organes de gouvernance destinés à accompagner l'utilisation Cloud au sein du Groupe.

Ce document, rédigé du point de vue d'un utilisateur de services Cloud, vise également à empêcher l'apparition d'une *Shadow IT* (utilisation non-encadrée de solutions Cloud en dehors de la gouvernance informatique du Groupe) en présentant les différentes opportunités au regard des contraintes et des risques liés à l'utilisation de services Cloud.

Le Cloud Blueprint a été approuvé par tous les CIO et CTO du Groupe puis formellement validé par le Comité Exécutif du Groupe et nous est donc opposable par le régulateur.

## Audience

Managers impliqués dans les décisions, projets et initiatives liés au déploiement de solutions dans le Cloud.

**Nous vous en souhaitons une lecture utile !**

Les technologies Cloud, qu'elles soient Privées, Publiques ou Hybrides, offrent d'**importantes opportunités** pour le Groupe : support à l'innovation, attraction / rétention des talents, avantages concurrentiels via l'accès à de nouvelles technologies et à de nouveaux marchés, en particulier l'Intelligence Artificielle, nécessitant une utilisation à grande échelle des données.

A moyen terme, l'**utilisation des technologies Cloud sera indispensable** pour maintenir notre compétitivité. La majorité des nouveaux traitements sera déployée avec ces technologies et les traitements existants vont être adaptés. La question est de savoir **quels seront les traitements à déployer sur quels types de solutions Clouds (privés, publics)**, en mesurant les opportunités, contraintes et risques associés.

En effet, les technologies de Cloud publics entraînent de nouvelles contraintes réglementaires, font évoluer notre profil de risques et, si utilisées de façon non maîtrisée ou inappropriée, peuvent avoir un **impact dévastateur sur la marque BNP Paribas et sur la réputation du Groupe**, voire entraîner des amendes et des révocations de licences.

Aucune des contraintes légales ou réglementaires qui s'imposent à nous, ne nous interdisent l'utilisation du Cloud public : toutes ces contraintes peuvent être gérées par des mécanismes techniques ou être garanties par de clauses contractuelles adaptées. Ces dispositifs sont définis dans nos procédures internes.

**Certaines contraintes, plus subtiles, ont en revanche des impacts plus importants.** Tout d'abord, la configuration et l'exploitation en toute sécurité de services Cloud requièrent un **niveau de maturité** important dans l'usage des technologies Cloud, en termes de compétences, d'expériences, de recommandations et de procédures de contrôle - ce qui n'est pas notre cas aujourd'hui. Deuxièmement, la **dispersion de nos données** et de nos traitements dans différents environnements de Cloud public, gérés par des acteurs potentiellement enclins à nous concurrencer, diminue notre capacité à utiliser ces données de manière corrélée et à alimenter les services d'analyse de données et d'automatisation intelligente qui seront essentiels à notre compétitivité. Cela aurait donc un **impact négatif sur notre souveraineté et pérennité** à moyen-long terme.

Par conséquent, les **déploiements dans des technologies Cloud de traitements manipulant des données hautement sensibles ou des éléments de propriétés intellectuelles sont restreints à des solutions de type Clouds privés on-prem**. (Les règles précises sont dans le document).

L'utilisation de technologies Cloud représentera rapidement une part importante de notre informatique, il est donc essentiel que le Groupe adapte progressivement sa gouvernance informatique vis à vis du Cloud. Deux structures temporaires sont mises en place à cet effet :

La *Cloud Maturity Assurance Team (CMAT)* est une équipe dédiée, mandatée au niveau Groupe et rattachée au Comité de Direction Générale de la Filière IT. Sa mission est d'accroître la maturité globale du Groupe sur les sujets Cloud et d'agir en conseil sur les décisions stratégiques concernant les technologies Cloud.

Le *Cloud Enablement Council* est composé de représentants de chaque Entité, des Fonctions Groupe et des comité transversaux concernés (par ex. Architecture Boards), pour déployer localement les responsabilités CMAT.

# Qu'est-ce que le *Cloud Computing* ?

Bien que le Cloud Computing soit devenu une technologie majeure au cours de ces dernières années, peu sont en mesure d'en donner une définition claire. En voici une (source Wikipédia) :



*« Le Cloud Computing, en français l'informatique en nuage, est un important changement de paradigme des systèmes informatiques. Un cloud (« nuage ») est un ensemble de matériels, de raccordements réseau et de logiciels fournissant des services exploitables depuis n'importe où dans le monde. Un nuage est caractérisé par sa disponibilité mondiale en libre-service, l'élasticité, l'ouverture, la mutualisation et le paiement à l'usage. Il peut permettre d'effectuer des économies, notamment grâce à la mutualisation des services. »*

L'Autorité Bancaire Européenne donne une définition similaire :



*« Services en nuage : services fournis au moyen de l'informatique en nuage (Cloud Computing), à savoir un modèle permettant d'accéder partout, aisément et à la demande, par le réseau, à des ressources informatiques configurables mutualisées (réseaux, serveurs, stockage, applications et services par exemple) qui peuvent être rapidement mobilisées et libérées avec un minimum d'effort ou d'intervention d'un prestataire de services. »*

Bien que très précises, ces définitions peuvent être difficiles à appréhender pour un non-spécialiste. Nous proposons d'utiliser une analogie avec le domaine du transport pour mieux comprendre les concepts et les conséquences des choix faits par le Groupe en matière de *Cloud Computing*.

## Une analogie

Traditionnellement dans le domaine de l'IT, chaque projet dispose de sa propre infrastructure (ordinateurs, stockages) pour déployer une application. Si nous faisons une analogie avec le monde du transport, cela s'apparente au fait de posséder une voiture : vous achetez ou faites construire une voiture, vous l'alimentez en énergie, vous assurez son entretien (maintenance et gestion de l'obsolescence technique et logicielle pour l'IT) ... et vous l'utilisez pour vos déplacements.



Le **Cloud Computing** en revanche s'apparente au fait d'utiliser **un taxi** : vous n'achetez pas le véhicule, vous n'avez pas à l'entretenir, ni à faire le plein et même pas besoin de conduire : le taxi est là, devant votre porte pour vous conduire à votre destination. Fini le temps passé à chercher une place de parking, vous ne payez que la course (c'est ce qu'on appelle "payer à l'usage") et vous pouvez vous concentrer sur d'autres activités pendant le trajet.

Cette analogie présente la version simple du Cloud, il existe de nombreuses formes de Cloud pouvant s'apparenter à la location de voitures, au crédit-bail automobile, aux services de VTC (véhicule de transport avec Chauffeur) voire même aux bus.

Dans le cadre d'une grande entreprise comme BNP Paribas, nous n'allons pas utiliser l'analogie sur une seule voiture mais considérer plutôt une flotte de véhicules. Cette flotte peut être gérée en externe par une société spécialisée : c'est un **Cloud public**. En revanche si la flotte est gérée en interne et que les employé.es n'ont pas de véhicule alloué mais peuvent utiliser un des véhicules de la flotte en fonction de leurs besoins, alors il s'agit d'un **Cloud privé**.

Il existe une autre forme de Cloud : le **Cloud hybride**. C'est un mélange de Cloud privé et de Cloud public. C'est le cas où l'entreprise possède sa propre flotte de voitures mais fait aussi appel à des sociétés externes, notamment pour gérer les situations de fortes demandes ou pour disposer de voitures spécifiques à certains types de trajets spécifiques.

Même s'ils ne sont pas différenciés dans le cadre du Cloud Blueprint, qui couvre indifféremment toutes les formes de Cloud, les notions et acronymes **IaaS**, **PaaS** et **SaaS** sont souvent utilisés et méritent d'être expliqués - vous trouverez ceci en annexe. Vous y trouverez aussi comment distinguer les services Cloud (sujet de ce document) des services Internet classiques (non soumis aux règles définies dans ce document).

# Le Cloud : source d'opportunités

L'analyse des marchés révèle une augmentation constante et significative de l'utilisation des technologies Cloud dans le domaine bancaire et financier. Cela s'explique par les opportunités engendrées par ces technologies et par les bénéfices qu'en attendent les responsables IT et les dirigeants d'entreprise.

En combinant la vision du marché avec la vision de représentants du Groupe, voici les principales opportunités identifiées, du point de vue d'un utilisateur de ces services - la plupart s'appliquant à la fois au Cloud privé et au Cloud public :

## 1. Créer un avantage compétitif :

Accéder à des technologies et à des partenaires permettant d'accompagner le développement de produits ou de services innovants et différenciants.

 *L'accès aux dernières innovations technologiques (aérodynamisme / turbo / freins) est un grand avantage lors d'une course automobile.*

## 2. - Améliorer le *time to market* :

Accéder à des plates-formes et outils permettant d'accélérer nos développements et cycles de déploiement.

 *Ne perdez plus de temps à chercher une place de parking - sautez du taxi et filez à votre rendez-vous.*

## 3. Gagner en flexibilité :

Utiliser les services Cloud pour assurer un passage rapide à l'échelle (élasticité). Passer d'un modèle financier d'investissement et d'immobilisation à un modèle de paiement à l'usage pour mieux gérer l'incertitude du succès commercial d'un service (attention : le coût par unité peut être supérieur).

 *Inutile de posséder une large gamme de véhicules pour proposer de nouveaux voyages et accueillir plus de voyageurs – si besoin, louez simplement d'autres véhicules.*

## 4. Rester compétitif :

Construire des initiatives externes via des collaborations basées sur le Cloud (par exemple Blockchain, Apprentissage et Intelligence Artificielle) et maintenir notre présence sur le marché.

 *Plus besoin de trouver la voiture universelle parfaite répondant à toutes vos situations, utilisez plutôt la voiture la plus appropriée pour chaque nouvel usage.*

A court terme, **le soutien à l'innovation** et **l'élasticité des infrastructures** sont les besoins les plus fortement exprimés par la plupart des Métiers du Groupe.

RESTER DANS  
LA COURSE

ETRE SUR  
LE PODIUM

A moyen terme, les technologies Cloud nous fourniront l'avantage stratégique de **l'utilisation étendue des données** (*Big Data*) et de **l'Intelligence Artificielle** (*Machine Learning*) pour ainsi développer une meilleure connaissance du marché et de nos clients.

## 5. Améliorer l'efficience opérationnelle :

S'appuyer sur des plates-formes et des services permettant de décharger et basculer certains traitements sur des solutions partagées plus efficientes.

 *Bénéficiez de l'expertise de professionnels de l'automobile pour un entretien plus efficace et plus économique de vos véhicules.*

## 6. Améliorer l'expérience client :

Fournir des services orientés utilisateurs (y compris des APIs) pour créer des parcours utilisateurs innovants, en intégrant des solutions alternatives de partenaires externes.

 *Invitez vos clients dans une nouvelle expérience de voyage dans un véhicule équipé des dernières innovations venant de start-ups à la pointe de la technologie.*

## 7. - Améliorer la disponibilité :

S'appuyer sur des plates-formes Cloud mondialement distribuées afin d'améliorer la disponibilité des services métiers et leur résilience face à de potentielles catastrophes (climatiques, sociales, géopolitiques, ...).

 *Ne dépendez plus de votre voiture, elle pourrait vous lâcher en cas en panne - Si un taxi tombe en panne, il suffit d'en appeler un autre.*

## 8. Attirer et retenir nos talents :

Permettre à nos talents au sein de l'entreprise d'accéder aux dernières technologies et outils. Attirer de nouveaux talents en offrant des environnements optimisés pour l'innovation et la créativité.

 *De belles voitures et de nouveaux modèles vous aideront à rester tendance et à intégrer les meilleurs clubs automobiles*

# Cloud public et nouvelles régulations

Les principaux régulateurs et législateurs dont nous dépendons ont émis des directives spécifiques pour l'utilisation de services de Cloud Computing externes. **Il est obligatoire pour toutes les entités du Groupe de garantir la conformité avec les directives et règlements applicables** de l'UE (comme par exemple le règlement RGPD), ainsi qu'avec toute autre loi nationale et internationale susceptible d'avoir une incidence sur nos activités (comme par exemple le CLOUD Act, etc.). De plus, des contraintes réglementaires supplémentaires peuvent s'appliquer à des Métiers spécifiques, comme par exemple les exigences de conformité à la loi HIPAA pour les activités d'assurance du Groupe.

**European Bank Authority** – synthèses des recommandations :

**Responsabilité** : nous sommes pleinement responsables de nos obligations envers nos clients et envers les régulateurs, quel que soit le modèle de Cloud utilisé – nous ne pouvons pas nous défausser sur le fournisseur.

**Prestation de services essentiels** : nous devons évaluer de façon formelle le risque de chaque déploiement dans le Cloud pour la continuité des services ainsi que la confidentialité et l'intégrité des données manipulées.

**Information du superviseur** : nous devons fournir à nos superviseurs les informations adéquates sur les services déployés dans un Cloud externe (en particulier pour les services importants) et tenir à jour un "Registre" de tous les déploiements dans le Cloud.

**Droit d'audit / de vérification** : nous devons avoir signés avec nos fournisseurs de services Cloud des accords permettant d'effectuer, par nous-mêmes ou par nos superviseurs, des audits complets (incluant l'accès aux locaux techniques) et nous devons effectuer ces audits conformément à l'analyse du risque associés.

**Stratégie de sortie** : nous devons, pour chaque déploiement Cloud de services essentiels, documenter et tester régulièrement un plan de sortie nous permettant soit de transférer les activités à un autre fournisseur, soit de les réintégrer dans notre organisation.

**Chaîne de sous-traitance** : Les fournisseurs de services Cloud utilisent souvent d'autres fournisseurs de services Cloud (par exemple, un fournisseur SaaS peut utiliser des services IaaS d'un autre fournisseur). Dans ces situations, les contraintes ci-dessus s'appliquent à l'ensemble de la chaîne de fournisseurs.

4

**CLOUD Act** - Clarifying Lawful Overseas Use of Data Act (le texte qui suit est un résumé de l'analyse effectuée en avril 2018 par les juristes du Groupe)

Le CLOUD Act est une loi américaine qui précise que les autorités judiciaires américaines sont, dans le cadre d'une enquête sur des crimes graves, en mesure d'avoir accès aux données détenues par des fournisseurs de services Internet même si elles se trouvent en dehors des États-Unis, et inversement, que les gouvernements étrangers, dans le cadre d'une enquête sur des crimes graves, peuvent obtenir l'accès à des données qui se trouvent aux États-Unis.

**Le CLOUD Act ne crée pas de façon immédiate de nouveaux moyens extraterritoriaux permettant aux États-Unis d'obtenir des données** (par rapport aux actuels Freedom Act, Patriot act et Foreign Intelligence Surveillance Act).

L'adoption du CLOUD Act pourra soit atténuer le risque existant ou soit créer un risque supplémentaire pour BNP Paribas - cela dépendra principalement des traités d'entraide judiciaire qui seront discutés entre les États-Unis et l'Union Européenne.

**RGPD** (Règlement Général sur la Protection des Données)

Le RGPD est un règlement législatif de l'Union Européenne sur la protection de la vie privée pour tous les individus au sein de l'Union Européenne. Il vise principalement à donner aux citoyens et aux résidents le contrôle de leurs données personnelles. Elle exige **la protection, par conception et par défaut**, de toutes les données personnelles et plus particulièrement les données sensibles.

Nous devons veiller à ce que cela soit mis en œuvre par tous les fournisseurs de services Cloud à qui nous faisons appel pour le traitement ou le stockage de ces données. En effet, outre l'effet dévastateur sur la marque et la réputation de BNP Paribas, une infraction au RGDP pourrait entraîner une amende pouvant aller jusqu'à 4% de notre chiffre d'affaires, soit actuellement **une amende d'environ 1,7 milliard d'euros**.

# Cloud public et risques informatiques

L'utilisation de services de Cloud externes modifie significativement notre profil de risque informatique, en termes juridiques, techniques et organisationnels. La liste ci-dessous, basée sur l'ENISA "Cloud Computing Risk Assessment" adaptée par nos entités Risque internes, décrit les principaux risques (risques critiques en rouge et risques majeurs en orange). Ces risques sont décrits en utilisant l'analogie ci-dessus avec le monde de transport.

## R.1 – Perte de gouvernance et impact potentiel sur la posture de conformité

 Lorsque nous mettons une voiture à disposition de nos employés ou clients, nous devons garantir la sécurité et le bon entretien de ce véhicule – et ceci doit pouvoir être contrôlé par un tiers. Lorsque nous faisons appel à un fournisseur externe, il y a un risque que la sécurité des véhicules ne soit pas au bon niveau et que ce fournisseur ne nous permette pas de vérifier la façon dont il les entretient.

## R.2 – Prise en otage (effet de verrouillage)

 En théorie, « un taxi est un taxi » et nous pouvons en changer à notre guise. Cependant, les compagnies de taxis développent des services dédiés pour faciliter la vie de leurs clients et ainsi les rendre captifs : numéro d'appel dédié, application mobile spécifique, paiement accéléré. Il est alors difficile de changer de fournisseur de taxi, même si ce dernier augmente ses prix ou si le service se dégrade.

## R.3 – Compromission du service

 Des personnes mal intentionnées peuvent avoir accès aux voitures et compromettre leur sécurité, par exemple en sabotant les freins, ou leur confidentialité, en installant des dispositifs pour écouter les conversations des passagers.

## R.4 – Non suppression ou suppression partielle des données

 La compagnie de taxis collecte des données : noms d'utilisateurs, préférences des clients, localisation, moyens de paiement etc. Comme nous avons peu de contrôle sur les traitements de données par la compagnie de taxis, il est plus difficile de garantir que ces données sont correctement effacées lorsque / si nous en faisons la demande.

## R.5 – Compromission des interfaces de gestion

 Des criminels peuvent accéder aux interfaces de gestion du service et compromettre les données comme par exemple le numéro de téléphone utilisé pour la réservation et ainsi intercepter les commandes, envoyer un faux taxi pour espionner les passagers... voire pire.

## R.6 – Menace interne

 Un employé de la compagnie de location de voiture peut saboter les freins ou installer un dispositif d'enregistrement pour écouter les conversations des passagers.

## R.7 – Défaillance du cloisonnement

 Un ancien client peut avoir installé un appareil d'enregistrement dans un véhicule de location pour espionner des utilisateurs suivants.

## R.8 – Risque systémique

 La compagnie de taxi peut ne pas être en mesure d'assurer la continuité du service, par exemple en cas de grève générale des chauffeurs ou d'une défaillance générale du service (comme un mauvais liquide de frein utilisé). Si les services de taxis sont fortement concentrés sur quelques compagnies, il sera difficile de trouver d'autres taxis en remplacement et cela pourrait impacter fortement notre capacité de déplacement.

## R.9 – Protection des données

 La société de taxis collecte de nombreuses données sur ses clients : noms, préférences, lieux, moyens de paiement, etc... Comme nous avons peu de contrôle sur les traitements de données par cette société, il est difficile d'être assuré la conformité de ces traitements avec la législation locale. C'est encore plus complexe si l'entreprise sous-traite par exemple le centre d'appel pour les réservations à un autre fournisseur dans un autre pays.

## R.10 – Risque de changement de juridiction

 La compagnie de taxi peut être originaire ou fortement dépendante d'un pays qui l'oblige à transmettre des informations à notre insu et sans notre consentement voire à nous espionner.

## R.11 – Incapacité de respecter l'obligation de signaler les incidents auprès des régulateurs

 Si un incident se produit, il peut être plus difficile de l'expliquer ou de le signaler, comme l'exige la loi, parce que l'information nécessaire est sous le contrôle du fournisseur. Par exemple, un accident peut être dû à un mauvais liquide de frein utilisé dans certaines voitures, mais l'entreprise de location peut essayer de le cacher afin de protéger son activité malgré le risque encouru pour nos employés.

# Contraintes d'utilisation du Cloud

Le sentiment que le Cloud Public est moins sécurisé qu'une solution internalisée n'est plus justifiée pour les grands fournisseurs de services Cloud. Les problèmes de sécurité avérés ayant affectés ces dernières années des clients de ces fournisseurs étaient dus à une mauvaise configuration ou à une mauvaise utilisation des services - aucune défaillance au sein de ces grands fournisseurs n'a été détectée. Ce n'est pas vraiment surprenant, car la sécurité est la clé de leur succès et ils y consacrent des moyens très importants. De plus, le mode de consommation Cloud permet d'assurer une gestion des correctifs plus rapide et plus efficace que pour les systèmes informatiques traditionnels et raccourcit ainsi fortement les durées de vulnérabilité.

Lors des ateliers menés en 2018, **le groupe de travail BNP Paribas Cloud n'a pas identifié de contraintes externes majeures nous interdisant l'utilisation d'un Cloud Public** : les contraintes légales et réglementaires peuvent toutes être adressées par des mécanismes techniques (gestion des droits d'accès, chiffrement / masquage des données, journalisation des accès, localisation des données etc.) ou encadrées par des clauses contractuelles adaptées (SLA, audit ...). Les grands fournisseurs de services Cloud souhaitent investir le marché des grandes entreprises, et notamment le secteur bancaire et financier. Ils sont donc beaucoup plus conciliants sur les contraintes contractuelles et techniques, qu'ils sont aujourd'hui disposés à discuter et accepter, comme notamment les audits de risques imposés par les régulateurs.

6

Ceci s'applique à l'ensemble de nos activités bancaires (y compris les "services essentiels") à l'exception potentielle de certaines activités encadrées par les lois de programmation militaire.

**Il existe cependant d'autres contraintes qui ont un impact important sur le choix du type de Cloud (Privé ou Public) pour le déploiement d'un traitement.**

## La maturité du Groupe dans l'usage du Cloud

De par son agilité pour la création et l'évolution rapide des services, le Cloud augmente le risque de mauvaise utilisation pouvant conduire à des failles de sécurité. De plus une application hébergée dans un Cloud public est plus exposée qu'une application profitant des protections de nos centres

## Exemples d'incident sécurité Cloud

En avril 2017, une mauvaise utilisation des services Cloud d'AWS entraîne un défaut de protection des données de l'armée - des **données "top secret" ont été exposées**. En juillet 2019, la banque américaine Capital One a annoncé que **les données de plus de 100 millions de leurs clients ont été volées** du fait d'un défaut de configuration de leurs services AWS. Bien qu'aucune violation de la sécurité des services AWS n'ait été constatée jusqu'à présent, de nombreux cas de fuites de données dues à une mauvaise configuration sécuritaire AWS ont été et sont encore régulièrement signalés. De nombreuses startups utilisent AWS pour fournir des services SaaS et on considère que bon nombre d'entre elles n'utilisent pas de configuration appropriée pour protéger les données de leurs clients.

informatiques (Data Centers) et toute faille de sécurité est plus facilement exploitable par des cybercriminels. Configurer et exploiter en toute sécurité un environnement Cloud requière donc une forte maturité vis-à-vis des technologies Cloud en général et de cet environnement en particulier.



*Reprendons notre analogie des transports et considérons le cas d'une conversation d'affaires dans un taxi. La confidentialité de cette discussion peut être préservée dans certains cas : certains taxis disposent d'une vitre séparant le conducteur des passagers et d'un système de sonorisation spécifique pour parler au conducteur si besoin. Mais pour cela nous devons savoir comment activer le dispositif : vérifier le voyant rouge/vert indiquant si le conducteur peut entendre notre conversation, avoir des indications claires pour savoir si nous pouvons nous fier aux chauffeurs de cette compagnie de taxis...*

Bien qu'il existe des noyaux d'expertise en matière d'utilisation du Cloud dans certaines Entités, il faut reconnaître que la maturité globale du Groupe sur la configuration et l'utilisation des services Cloud n'est pas au niveau requis pour éviter des incidents pouvant impacter la réputation du Groupe : il n'existe pas aujourd'hui au niveau Groupe de recommandations publiées, d'outils pratiques et de procédures de contrôle relatifs à la configuration et l'utilisation des Services Cloud.

En attendant que la maturité du Groupe dans l'utilisation des services Cloud se renforce, **il faut éviter d'utiliser des services Cloud public dans le cas où la divulgation et l'exposition des données gérées auraient un impact critique sur la pérennité ou la réputation à court terme du Groupe.**

## Disponibilité des services

La supervision de bout-en bout est essentielle pour les services inter-Métiers et inter-pays afin de garantir la qualité de services telle que requis par les Métiers, nos clients et les régulateurs.

Ceci est particulièrement important pour les solutions *mash-ups*, c'est-à-dire les solutions agrégant plusieurs services afin de fournir une nouvelle fonctionnalité (l'attrait des solutions *mash-ups* est très fort aujourd'hui puisque cela permet de réduire considérablement les délais de mise sur le marché via la réutilisation de services existants).

Lorsque les éléments constitutifs des services sont répartis entre différents fournisseurs de Cloud, avec des architectures et des outils de supervision variés et en constante évolution, il est difficile (voire impossible) de comprendre et corriger la dégradation globale d'un service causée par une mauvaise performance ou l'indisponibilité d'un composant Cloud dont nous ne maîtrisons pas le pilotage.

*En reprenant notre analogie, imaginez que vous devez organiser un important buffet d'entreprise, où chaque entité contribue en fournissant de la nourriture et du mobilier. Supposons à présent que chaque entité gère indépendamment l'acheminement de leurs contributions : que pouvez-vous faire, en tant qu'organisateur, si certaines pièces importantes n'arrivent pas à temps et si vous n'avez aucun moyen de contacter les camions pour estimer le retard ? Devriez-vous annuler le buffet ? Devriez-vous retarder le début du buffet avec une animation ? Devriez-vous préparer un plan B avec des solutions de remplacement ?*

L'industrie du Cloud s'attèle à adresser cette problématique, mais il faudra un temps certain avant que des normes et standards ne soient définis et déployés. D'ici là, **il faut éviter tout recours à des services mash-ups sur Cloud public pour nos processus critiques** (et en particuliers les activités PSE : Prestations de services essentiels).

## Compétitivité et souveraineté

Nous devons porter une attention particulière aux potentielles fuites de nos données vers les acteurs du Cloud qui pourraient être enclins à nous concurrencer. Le risque concerne non seulement les fuites de données explicites mais aussi les informations d'usages ou de comportements qu'elles peuvent révéler.

En effet les données de configuration des logiciels SaaS ou l'analyse des processus dévoilent souvent de précieuses informations sur notre savoir-faire, même si les informations relatives à notre cœur de métiers (données bancaires) sont bien protégées.

Il est par exemple impossible de masquer à nos fournisseurs Cloud les données d'usage des services (puisque elles sont nécessaires pour fournir le service en question) ; en revanche ces données d'usage sont une source d'information à forte valeur concurrentielle sur ce que nos clients utilisent ou apprécient.

 *Avec l'analogie des transports, imaginez que la majorité des voyages des employés soit gérée par une seule compagnie de taxis. Pour chaque voyage, la compagnie connaît bien-entendu les dates du voyage mais aussi les lieux de prises en charge et de destination. Ainsi, si un grand nombre de nos employés se rendent soudainement dans les locaux de l'entreprise A et de l'entreprise B, la société de taxi peut potentiellement en déduire qu'une fusion et acquisition est en jeu (de nouveaux outils d'analyse de données utilisés par les data scientists peuvent très facilement effectuer de telles corrélations et conclusions). Certes, une compagnie de taxi ne va probablement pas proposer des services bancaires et nous concurrencer – mais certains grands fournisseurs de services Cloud le peuvent, puisqu'ils possèdent déjà une licence bancaire.*

D'autre part, la dispersion de nos données et de nos traitements dans différents environnements de Cloud public réduit significativement notre propre capacité à utiliser ces données de façon corrélée et donc à alimenter les analyses de données (*Big Data*) et les services d'automatisation intelligente (*Machine Learning*), qui représentent un enjeu essentiel de compétitivité à moyen terme.

On pourrait penser qu'il sera par la suite possible de rapatrier ces données dans nos environnements d'analyse corrélée, mais l'expérience montre que les grands fournisseurs de services Cloud ne facilitent pas les démarches de récupération des données, puisqu'ils savent leur possession représenter un levier important pour le renouvellement des contrats.

Par conséquent, **il faut éviter de déployer dans un Cloud public les traitements manipulant des données hautement compétitives ou considérées comme une propriété intellectuelle**, que nous souhaitons protéger ou utiliser pour l'analyse corrélée des données (*Big Data*) et l'apprentissage profond (*Machine Learning*).

# Types de déploiement Cloud

Six types d'implémentation de services Cloud ont été identifiés afin de permettre une prise de décision équilibrant au mieux les opportunités, les risques et les contraintes (une description complète est fournie en annexe) :

Type	1 Private Internal Cloud on-prem	2 Managed Private Internal Cloud on-prem	3 Managed Private Cloud off-prem	4 Virtual Private Cloud off-prem	5 Public Cloud off-prem	6 Community Cloud off-prem
Analogie	Flotte de véhicules sur-mesure	Flotte de véhicules standards	Leasing de véhicules standards	Service de VTC (véhicules avec chauffeurs)	Transport en commun (bus, car)	Bus à accès restreint

on-prem : hébergé dans des installations immobilières et techniques à usage exclusif de BNP Paribas

off-prem (en dehors) : hébergé dans des installations partagées.



**Type 0** (non représenté dans le tableau ci-dessus) est le modèle traditionnel de déploiement informatique.



Voitures personnelles sur mesure.  
BNP Paribas attribue à chaque employé.e une voiture dédiée et sur-mesure. Seul.es les employé.es BNP Paribas peuvent disposer et conduire ces voitures. L'entretien (révisions, vidanges, réparations, ...) est effectué par des employé.es BNP Paribas dans les garages de BNP Paribas.

**Type 1** (Cloud Privé on-prem) : Cloud privé défini et construit par BNP Paribas, hébergé et administré en interne dans les centres de calcul du Groupe et mis à disposition des Métiers.



Flotte de voitures sur mesure.

BNP Paribas possède sa propre flotte de voitures construites et entretenues par des employé.es BNP Paribas dans les garages du Groupe. Les véhicules sont alloués temporairement aux employé.es en fonction de leurs besoins. Seul.es les employé.es BNP Paribas peuvent disposer et conduire ces voitures.

**Type 2** (Managed Private Internal Cloud on-prem) : Cloud dédié, défini et construit par un grand fournisseur de services Cloud, hébergés et administrés dans les centres de calcul du Groupe et mis à disposition des Métiers. L'objectif est de tirer parti des standards et des innovations d'un Cloud Public tout en profitant des propriétés d'un Cloud privé (sécurité, souveraineté, ...)

Flotte de véhicules standards.

BNP Paribas possède une flotte de voitures standards, achetées chez un constructeur automobile. Les véhicules sont alloués temporairement aux employé.es en fonction de leurs besoins du moment. Seul.es les employé.es BNP Paribas peuvent disposer et conduire ces véhicules. L'entretien des véhicules est effectué par le constructeur dans les garages de BNP Paribas.

**Type 3** (Managed Private Cloud off-prem) : Cloud dédié, défini et construit par un grand fournisseur de services Cloud, hébergés et administrés dans les centres informatiques du fournisseur et mis à disposition des Métiers. L'enjeu ici est économique : tirer profit des économies d'échelle dans la gestion d'un centre informatique via un fournisseur majeur de services Cloud, tout en conservant un certain cloisonnement physique vis-à-vis d'autres clients du fournisseur. Ces services peuvent-être utilisés en extension des services Cloud de Type 1 et 2.



Leasing (location longue durée) d'une flotte de véhicules

BNP Paribas dispose via une société de crédit-bail d'une flotte de voitures standards. Des procédures spécifiques de contrôle sont appliquées par BNP Paribas lors de l'entrée/sortie d'un véhicule de la flotte (sécurité, confidentialité, ...). Les véhicules sont temporairement alloués aux employé.es en fonction de leurs besoins du moment. Seul.es les employé.es BNP Paribas peuvent disposer des véhicules. L'entretien des véhicules est effectué par le loueur au sein de ses garages, dans un espace dédié à BNP Paribas.

**Type 4** (Cloud Privé Virtuel off-prem) : adaptation des services du Cloud Public (Type 5 ci-après), proposant à travers des techniques de virtualisation, un certain degré de cloisonnement entre les différentes ressources pour mieux adresser les besoins de ségrégation des traitements comprenant des données à protéger.



Service de voitures avec chauffeur (VTC)  
BNP Paribas contractualise avec une compagnie de voitures avec chauffeur (VTC). Les véhicules sont loués en fonction des besoins pour chaque voyage et sont conduits par les chauffeurs de la compagnie. Nous n'avons pas d'usage exclusif des véhicules (un même véhicule peut transporter successivement des passagers de différentes sociétés) et les procédures de nettoyage entre les trajets sont sous contrôle de la compagnie de VTC. L'entretien des véhicules est effectué par la compagnie de VTC dans ses garages.

**Type 5** (Cloud Public off-prem) : ensemble de ressources informatiques (serveurs, stockage, applications) mutualisées et partagées simultanément par les clients - la protection des données et des traitements étant assurée par un système logiciel de gestion des droits d'accès.



#### Transport en commun (bus)

Les employé.es de BNP Paribas utilisent les transports en commun, par exemple des bus publics. Ces bus sont gérés, conduits et entretenus par une compagnie de transport. Durant les trajets, les employé.es BNP Paribas partagent le bus avec d'autres personnes n'appartenant pas au Groupe.

**Type 6** (Community Cloud off-prem – Cloud Communautaire) : Cloud, similaire à un type 4 ou 5 suivant les cas, mais réservé à une communauté spécifique d'organisations ayant des préoccupations et contraintes communes. Cette pratique est de plus en plus courante entre des pairs du secteur bancaire, pour réduire les coûts d'activités complexes et réglementés mais n'offrant pas d'avantage concurrentiel entre les participants engagés (par exemple, le traitement des paiements en magasin).

La différence fondamentale entre les services Cloud de type 2-3 et ceux de type 4-5, est notre capacité à auditer en temps réel les activités du fournisseur (au niveau technique mais aussi contractuel, y compris par l'intermédiaire de nos régulateurs) et dans la capacité à faire le lien avec nos systèmes de sécurité afin de nous garantir un niveau supérieur de confiance.

Les principaux fournisseurs de services Cloud, historiquement opposés aux nouveaux modèles de services de types 2, 3 et 4, commencent à développer ce type d'offres et à les considérer comme un vecteur de croissance auprès des grandes entreprises ayant des besoins informatiques massifs tout en étant fortement régulées, en particulier le secteur bancaire, les services financiers et les assurances.

## Les Clouds hybrides



Nos activités sont sujettes à de fortes variations cycliques nécessitant des pics importants mais éphémères de capacité informatique. L'utilisation croissante des techniques de corrélation massive des données (*Big Data*) et d'apprentissage profond (*Machine Learning*) augmente fortement l'amplitude de ces pics. Provisionner dans nos Clouds internes (type 1-2) la capacité informatique nécessaire pour ces pics conduirait à une sous-utilisation régulière des infrastructures sous-jacentes et engendrerait donc des coûts inutiles.

Afin d'**optimiser la valeur et les coûts**, il sera nécessaire de s'appuyer sur des **Clouds hybrides**, combinant plusieurs types de Clouds dans des services structurés et fournis par les Productions Informatiques du Groupe. Cela permettra de répartir les pics d'activité entre des infrastructures de type 1, 2, 3 et 4 et de profiter du paiement à l'usage pour réduire la facture hors période de pic.

# Règles d'utilisation des Clouds

## Règle générale (Règle 0)

Tout hébergement d'une activité en dehors des infrastructures traditionnelles internes du Groupe doit être conforme aux procédures existantes de BNP Paribas telles que définies et publiées par les services responsables (Compliance, Risques, Juridiques, Achats, Informatiques, etc.), et ce à la fois à l'échelle du Groupe et au niveau local.

Ces procédures constituent un cadre général pour assurer la protection de nos actifs et le respect des lois et réglementations, comme par exemple les règles de chiffrement ou d'anonymisation des données classifiées, les prérequis juridiques en termes de localisation des données, l'audit des services, la réversibilité et la continuité des services d'importance majeure.

Tout déploiement dans un Cloud doit donc respecter ces procédures – ceci est résumé par commodité dans ce document sous le terme *Règle 0*.

## Règles spécifiques aux Clouds

Les différentes contraintes listées précédemment soulèvent deux principaux sujets d'attention : la protection des données et la continuité des services. Huit règles directrices ont été établies pour aborder ces deux sujets.

**Protection des Données** : les données sujettes aux directives réglementaires externes ou représentant une valeur compétitive pour le Groupe doivent être traitées avec précaution.

Les règles D1 à D6 ont été établies pour répondre à ce besoin. Elles utilisent une classification basée sur la procédure Groupe de niveau 1 de gestion des données, qui rappelée en annexe. Les Entités qui utilisent un autre système de classification devront assurer la correspondance pour appliquer correctement ces règles sur leur périmètre local.

Ces règles sont listées par ordre de préséance (par exemple si la règle D2 s'applique, alors les règles D3 à D6 doivent être ignorées).

10

D1 – Les traitements manipulant des données masquées (anonymisation, pseudo-anonymisation, tokenisation) peuvent être déployés sur tous les types de Cloud, sauf s'il existe un risque sur la continuité de service (voir règle C7).

D2 – Puisqu'il est impossible de garantir le zéro-défaut sécuritaire et que l'hébergement dans des Clouds externes augmente la surface d'attaque cybercriminelle en dehors du contrôle du Groupe, les traitements manipulant des données classifiées Secret devront être déployés exclusivement sur des Cloud internes (type 1 et 2).

D3 – Puisque le niveau de maturité sur les usages Cloud est globalement faible au sein du Groupe et compte tenu de l'absence de procédures de configuration sécurisée des services Cloud, les traitements manipulant des données personnelles sensibles (au sens GDPR et autres régulations similaires) devront s'effectuer exclusivement sur des Cloud internes (type 1 et 2).

D4 – Pour des raisons de protection des avantages concurrentiels stratégiques et de pérennité du Groupe, les traitements manipulant des données hautement compétitives ou considérées comme une propriété intellectuelle, que nous souhaitons protéger ou utiliser pour l'analyse corrélée des données (Big Data) et l'apprentissage profond (Machine Learning), devront être déployés exclusivement sur des Clouds internes (type 1 et 2). Des copies non opérationnelles et chiffrées de ces données (*copies mortes* non modifiables) peuvent être déployées sur des Clouds externes (type 3 à 6), sous réserve du respect des autres règles.

D5 – Compte tenu de notre faible niveau de maturité concernant l'utilisation de services Cloud, les traitements manipulant des données classifiées Confidentiel devront être déployés exclusivement sur des Clouds internes (type 1 et 2). Un déploiement sur des services Cloud Privés (de type 3) peut être envisagé si un chiffrement adéquat des données et un système de gestion des accès approprié sont mis en place.

D6 – Les traitements manipulant des données personnelles d'identification non sensibles (au sens GDPR et régulations similaires) et les traitements manipulant des données classifiées Restreint pourront être déployés sur des Cloud internes (type 1 ou 2) et aussi sur des Clouds externes (type 3 à 6) avec un chiffrement adéquat des données et un système de gestion des accès approprié.

Les traitements bancaires ne comprenant pas de valeur concurrentielle peuvent être déployés sur des Clouds Communautaires bancaires (type 6), sous réserve du respect des règles D2 à D6.

**Continuité de service :** les services essentiels au bon fonctionnement des marchés financiers et aux opérations de nos clients doivent être assurés.

#### C7 – Les traitements supportant des activités

d'importance capitale (PSE : Prestations de services essentiels) peuvent être déployés sur des Clouds de type 1, 2, 3, 4 et 6 sous réserve du respect des règles D2 à D6. Ces traitements ne devront pas être déployés sur des Cloud de type 5 puisque le cadre contractuel ne permet pas répondre aux exigences des régulateurs concernant la gestion des correctifs

(en effet, un fournisseur Cloud peut retarder le déploiement d'un correctif s'il le considère mineur pour la plupart de ses autres clients, même si ce correctif est critique pour nous).

**C8 – Les traitements liés aux activités de support** (c'est-à-dire les activités non bancaires comme la paie, les notes de frais, le collaboratif, la communication...) peuvent être déployés sur tout type de Cloud sous réserve du respect des règles D2 à D6 et C7.

L'ensemble de ces règles constitue un cadre d'application pour les utilisations des services Cloud au sein du Groupe. Les Entités peuvent être amenés à les renforcer en fonction de leur contexte local.

Ces règles sont résumées dans la matrice d'aide à la décision ci-après, qui peut être utilisée pour analyser le stock actuel ou évaluer les initiatives prévues ou à venir.

Règles		1 Private Internal Cloud on-prem	2 Managed Private Internal Cloud on-prem	3 Managed Private Cloud off-prem	4 Virtual Private Cloud off-prem	5 Public Cloud off-prem	6 Community Cloud off-prem
Protection des Données	D1 Données masquées [Enjeu de protection des données]	✓	✓	✓	✓	✓	✓
	D2 Données secrètes [Enjeu de sécurité]	!	!	✗	✗	✗	✗
	D3 Données personnelles sensibles [Enjeu de maturité BNP Paribas]	!	!	✗	✗	✗	✗
	D4 Données compétitives à protéger ou propriété intellectuelle à protéger [Enjeu de souveraineté]	✓	✓	✗	✗	✗	✗
	D5 Données confidentielles [Enjeu de maturité BNP Paribas]	✓	✓	!	✗	✗	✗
	D6 Données personnelles d'identification Données restreintes	✓	✓	!	!	!	!
Continuité de services	C7 Prestation de services essentiels (sous réserve des règles D2-D6) [Enjeu de gestion des correctifs]	✓	✓	✓	✓	✗	✓
	C8 Activités de support (sous réserve des règles D2-D6 et C7)	✓	✓	✓	✓	✓	✓
	9 Quand les règles ci-dessus ne s'appliquent pas	✓	✓	✓	✓	✓	✓

- ✓ usage autorisé sous décision locale de l'Entité.
- ! usage autorisé sous décision locale de l'Entité avec une attention particulière concernant la protection de nos actifs.
- ✗ usage interdit - dérogation nécessitant une remontée au niveau du Groupe (cf. CMAT ci-dessous).

# Gouvernance stratégique

A moyen terme, la très grande majorité des nouveaux traitements du Groupe sera déployée sur des services Cloud et une proportion importante des traitements existants sera migrée vers le Cloud pour des raisons économiques et technologiques (obsolescences de l'infrastructure sous-jacente).

Dans ce contexte, il serait inopportun de créer au sein du Groupe un organe de gouvernance Cloud parallèle aux structures de gouvernance existantes (ou pire en compétition). Il convient au contraire de **progressivement introduire les sujets Cloud au sein de la gouvernance informatique et des comités de validation existants.**

Il faut cependant constater que, bien qu'il existe des noyaux d'expertise Cloud au sein du Groupe, notre niveau général de compétences et de maturité sur l'utilisation des services Cloud est encore faible et doit être renforcé. Pour cela, deux structures sont mises en place afin de renforcer la gouvernance informatique existante :

La **Cloud Maturity Assurance Team (CMAT)** est une équipe dédiée, mandatée au niveau Groupe et rattachée au Comité de Direction Générale de la Filière IT.

La CMAT est responsable de l'évolution du Cloud Blueprint.

La CMAT apporte au niveau Groupe des éclairages sur la stratégie, les usages et les risques du Cloud. Elle intervient en support au Cloud Programme.

La CMAT surveille les usages Cloud dans le Groupe (Cloud Register) en coordination avec les fonctions Risque.

La CMAT instruit les demandes de dérogations aux règles du Cloud Blueprint (cf. ci-dessous).

Le **Coud Enablement Council** est composé de représentants des Entités, des Fonctions Groupe (Risques, Juridique, Achat, Risques IT...) et des comités transversaux (Comités d'Architectes, etc.), avec un mandat fédéral rattaché à la CMAT.

Ils agissent en délégués de la CMAT avec mandat de promouvoir le Cloud Blueprint et de renforcer la maturité de leur entité sur les sujets Cloud via des actions appropriées, ainsi que des partages d'information et d'expérience avec leurs pairs.

Ils gèrent et communiquent l'inventaires des usages Cloud de leur entité (Cloud Register).

Ils remontent auprès de la CMAT les exceptions au Cloud Blueprint pour dérogation ou remédiation.

Ces deux nouvelles structures sont temporaires (horizon 2-3 ans). Leurs compositions et mandats sont revus régulièrement pour accompagner l'évolution de la maturité du Groupe et des marchés.

Puisque le Dedicated Cloud BNP Paribas (type 2) est en cours de construction et n'offre pas aujourd'hui l'ensemble des capacités dont on peut bénéficier avec certains Clouds publics, les Entités, à travers leurs organes de gouvernance existants, pourront décider d'utiliser différentes solutions Cloud, en fonction de la valeur, des risques et contraintes présentés dans ce document mais aussi en fonction de l'adéquation des différents services Cloud avec les besoins techniques et métiers.

En complément de la gouvernance existante, un nouveau dispositif est donc mis en place à l'échelle du Groupe via la CMAT pour accompagner cette prise de décision. **Les demandes de dérogation sont à adresser à la CMAT** qui apporte un avis consultatif à intégrer dans le comité de validation IT de l'entité.

L'avis de la CMAT s'inscrit dans un cadre de positionnement stratégique du Groupe sur des domaines intimement liés au Cloud (par exemple les *Blockchains*, le *Machine Learning* ou l'*Open Banking*) et/ou d'augmentation de maturité du Groupe par expérimentation ciblée.

Les **Comités de Validation IT (CVIT) conservent leurs prérogatives actuelles**, en termes de respect des règles et principes du Groupe, d'analyse des risques et de prise de décisions (y compris les sujets de Shadow IT). Les cas de divergence de points de vue entre une Entité et la CMAT seront remontés au niveau du *Comité de Direction Générale de la Filière IT*.



## Annexes

1. DEFINITION  
IAAS, PAAS, SAAS  
CLASSIFICATION DES DONNEES  
PROTECTION DES DONNEES
2. ANALYSE DU MARCHE
3. TYPES DE DEPLOIEMENT CLOUD
4. PRINCIPALES CONTRAINTES A L'UTILISATION DU CLOUD PUBLIC

# 1 Définitions

## IaaS, PaaS and SaaS

Même s'ils ne sont pas essentiels pour la compréhension du Cloud Blueprint, les notions et acronymes IaaS, PaaS et SaaS sont souvent utilisés et mérités d'être expliqués, en suivant l'analogie du transport.



IaaS, **Infrastructure as a Service**, peut être comparée à la structure d'un bus (châssis, roues, moteur, freins, ...), qui doit être aménagée et équipée en fonction des besoins. Le fournisseur de services livre la structure, en assure l'entretien. Le client loue la structure, sélectionne, installe et assure la maintenance des différents équipements (par exemple les sièges : de base ou de luxe, avec ou sans écran TV etc.) et assure ensuite le fonctionnement du service de transport pour les passagers.



PaaS, **Platform as a Service**, correspond à un bus pré-équipé pour un usage précis. Il existe de nombreux types de PaaS : bus urbains, bus classiques assurant des trajets courts, cars couchettes pour les trajets longs. Le fournisseur de services livre et entretient le bus : structure et équipements. Le client loue le bus, choisit la décoration extérieure (par exemple le logo d'entreprise) et assure ensuite le fonctionnement du service de transport aux passagers.



SaaS, **Software as a Service**, s'apparente à un service de visite guidée en bus. Le fournisseur de services livre, exploite et conduit le bus et permet à son client (le tour-opérateur) de délivrer un service à valeur ajoutée (visite guidée) au client final (le touriste). Le tour-opérateur fournit leur itinéraire aux chauffeurs du bus et peut se concentrer sur son activité principale : fournir à ses clients une visite guidée, des descriptions et des anecdotes sur les différentes attractions locales.

Le SaaS permet à une entreprise de se concentrer sur son cœur de métier sans avoir à se soucier des complexités informatiques (du moins c'est l'affirmation des fournisseurs SaaS - la réalité est un peu différente). *Saleforce.com* est un exemple bien connu de services SaaS : l'entreprise propose des solutions performantes de gestion de la relation clients sans que le client ait besoin d'installer et d'administrer un système informatique.

Les services SaaS peuvent être déployés par le fournisseur de services Cloud sur des infrastructures dédiées ou sur des infrastructures Cloud (la plupart des petits fournisseurs SaaS utilisent les solutions PaaS ou IaaS de grands fournisseurs Cloud comme AWS, Microsoft Azure, Google Cloud ou IBM Cloud).

## Service Cloud ou Service Internet ?

Les services Cloud et les services Internet sont très étroitement liés : l'omniprésence d'Internet a fortement favorisé l'essor du Cloud et les services de Cloud publics les plus connus sont accessibles via Internet.

14

Cependant, de nombreuses grandes entreprises contournent Internet en déployant, pour des raisons de sécurité et de performance, des connexions télécoms dédiées vers les infrastructures de leurs fournisseurs de services Cloud. D'autre part, les Clouds privés sont généralement accessibles depuis le réseau interne de l'entreprise mais il est courant pour une entreprise d'exposer une partie de son Cloud privé sur Internet pour fournir des services à ses utilisateurs mobiles.

Tout ceci peut prêter à confusion. Retenons que **si internet représente un point d'accès majeur pour les services Cloud, ce n'est pas le seul**, surtout pour les grandes entreprises comme BNP Paribas.

Il est également parfois difficile de **distinguer entre services externes accessibles via Internet et services Cloud**.



Poursuivons avec l'analogie du transport : lorsqu'un employé utilise *Google Maps* pour localiser le lieu de son prochain rendez-vous, il utilise tout simplement un service externe depuis Internet.

Lorsqu'une entreprise de livraison utilise la plate-forme *Google Maps* pour suivre en temps réel le mouvement de ses véhicules et optimiser leurs trajets (eh oui c'est un service que *Google Maps* propose aussi), elle utilise dans ce cas les services Cloud, puisque les données de l'entreprise sont stockées et traitées par Google pour fournir le service.

## CLASSIFICATION DES DONNEES

Les définitions suivantes, basées sur les procédures Groupe de niveau 1, sont celles qui s'appliquent sur l'ensemble du Cloud Blueprint. Les Entités qui utilisent un autre système de classification devront assurer la correspondance pour appliquer correctement les règles du Cloud Blueprint sur leur périmètre local.

**Donnée secrète** : données dont la divulgation s'avérerait létale pour la pérennité à court terme du Groupe.

**Donnée confidentielle** : données dont la divulgation aurait un impact négatif fort sur la réputation du Groupe et ses résultats financiers à court-moyen terme.

**Données Personnelles Sensibles** : données définies comme telles par la réglementation RGPD en Europe et par les règlements similaires dans les autres pays (par ex. CCPA en Californie) – en général : origine ethnique, religion, préférences sexuelles, informations médicales, etc.

**Données restreintes** : données qui ne sont ni secrètes ni confidentielles, mais qui ne sont pas non plus destinées à être diffusées publiquement.

**Données publiques** : données librement ou légalement accessibles en dehors du Groupe.

## PROTECTION DES DONNEES

**Chiffrement** : processus de cryptage d'un message ou d'une information consistant à restreindre son accès uniquement aux personnes autorisées.

L'information ou le message est chiffré par un algorithme de cryptage. A l'issue du chiffrement, un message encodé est généré et il ne peut être compréhensible que si décodé. Le dispositif de chiffrement utilise une clé secrète. Un destinataire autorisé peut facilement déchiffrer le message avec la clé fournie par l'expéditeur, mais pas les utilisateurs non autorisés. Il est en théorie possible de décrypter un message sans posséder la clé de cryptage, mais si le système de chiffrement est bien conçu, ceci nécessite des ressources et des compétences informatiques considérables.

**Masquage des données** : processus consistant à empêcher l'utilisation abusive des données en donnant aux utilisateurs un accès à des données réalistes mais fictives (ou à un mélange entre des données réelles et fictives), au lieu des données réelles.

Trois méthodes sont généralement utilisées :

L'**anonymisation** est un processus consistant à masquer de manière irréversible les données originales (brouillage, floutage, etc.). Anonymiser des données tout en en permettant un traitement utile est souvent complexe voire impossible.

La **pseudo-anonymisation** visent à substituer un élément de données sensibles par un pseudonyme, n'ayant aucune valeur extrinsèque ou exploitable directement (imaginez le nom de code d'un agent secret). Cette méthode utilise des traitements qui rendent impossible le retour en arrière en l'absence d'informations supplémentaires. Un même pseudonyme remplace toutes les valeurs d'origine, ce qui permet la corrélation des données (ce qui est désirable ou non suivant les cas).

La **tokenisation** est un renforcement de la pseudo-anonymisation qui impose l'attribution d'une nouvelle valeur aléatoire, appelé jeton, à chaque utilisation de la donnée d'origine. Cette méthode rend impossible la corrélation des données.

## 2 Analyse du marché

L'une des principales questions auxquelles les analystes sont confrontés sur l'utilisation de Cloud au sein des banques est : "Que font les autres industries ... et les autres banques ?".

### *Le Cloud n'est pas un phénomène de mode...*

Les analystes estiment que d'ici fin 2020, 35% des traitements informatiques des entreprises seront opérés depuis un Cloud hybride, dont 11% sur unxx Cloud public, et additionnellement 12% des traitements auront été migrés sur des solutions SaaS (source ISG © 2018).

L'industrie des services bancaires, financiers et d'assurance (BFSI) traditionnellement réticente à l'égard de l'utilisation les services Cloud pour des raisons de sécurité et de réglementation, commence à les adopter et les analystes prévoient des ratios d'utilisation similaires.

### *... pour différents types d'activités ...*

Les analystes (source © Gartner 2017) notent les propensions suivantes des banques pour le Cloud public :

- intérêt prononcé pour les activités de sécurité et conformité, de développement et de tests, les activités de vente et d'après-vente et pour les activités de paiement (impact SEPA)
- intérêt plus mitigé pour les activités de distribution, de reporting analytique, de gestion de contenus documentaires (Enterprise Content Management) et pour les outils collaboratifs
- faible intérêt pour la comptabilité générale, la trésorerie, la gestion des données clients, les activités de recouvrement, de commerce et de gestion de patrimoine (mais forte progression pour le Core Banking chez les banques de petite/moyenne taille).

### *.... et de nombreuses banques dans le monde ....*

De nombreuses grandes banques ont fait ces dernières années des annonces sur leur stratégie d'utilisation du Cloud, par exemple :

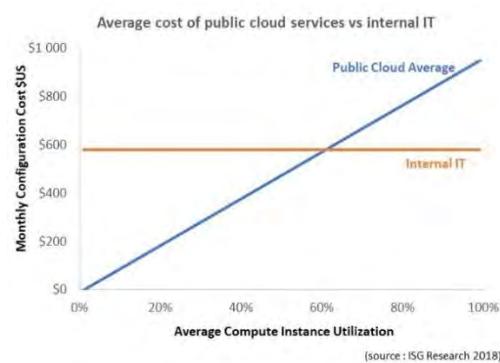
**Capital One** (2016) : l'une des 10 premières banques américaines, utilise AWS comme élément central de sa stratégie technologique.

**HSBC** (Juillet 2018) : La banque mondiale a signé un partenariat stratégique avec Google Cloud dans le cadre de sa « Cloud first Strategy ».

**TD Bank**, l'une des 10 premières banques nord-américaines (oct 2017) et la banque danoise **Saxo** (avril 2018) ont annoncé un partenariat stratégique avec Microsoft pour déployer leurs socles technologiques dans le Cloud Microsoft Azure.

**Bank of America** (nov 2019) : le seconde banque américaine a annoncé le développement, au-dessus du Cloud IBM, de leur plateforme bancaire - plateforme qu'il mettront aussi à disposition des fintechs.

## 16 ... le coût n'est pas nécessairement le vecteur principal ...

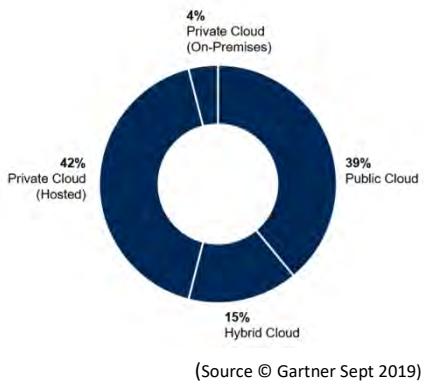


Les grandes banques ont déjà réalisé déjà d'importantes économies d'échelle grâce à leurs propres infrastructures et ne considèrent pas forcément le Cloud, sur un périmètre comparable, comme une opportunité de réduction massive des coûts, notamment lorsqu'elles prennent en considération au niveau corporate l'ensemble des coûts associés, comme le coût total de possession (TCO) ou les coûts d'ingénierie et de main-d'œuvre.

De nombreuses entreprises ont également remarqué que le paiement à l'usage peut entraîner une augmentation forte des coûts et des dépassements significatifs de budget.

Une nouvelle fonction émerge actuellement comme un standard de fait pour assurer le contrôle en temps réel des coûts : **FinOps** (contraction de Finance et de Opérations)

... et le multi-Cloud est le modèle prédominant



Les grandes entreprises s'orientent toutes vers un modèle multi-Cloud, mélangeant des services Cloud privés (en interne ou hébergé) et des services Cloud publics tiers, pour tirer parti des capacités informatiques internes de l'entreprise et de l'élasticité des Cloud externes.

Les usages SaaS continuent d'être prépondérants avec presque 70% des déploiements, aussi bien en mode privé on-prem que hébergé ou public.

Les fonctions en charge des activités d'exploitation informatique, opérant traditionnellement comme constructeur et fournisseur de services informatiques, se transforment en **agrégateur et courtier** de services provenant de plusieurs fournisseurs (informatique traditionnelle virtualisée, Cloud privé, Cloud public, etc.).

## 3 Types de déploiement Cloud

Six types d'implémentation de services Cloud ont été identifiés afin de permettre une prise de décision équilibrant au mieux les opportunités, les risques et les contraintes. Ces six types sont présentés ci-dessous avec leurs caractéristiques technique et leurs modes d'utilisation et de gestion.

Type	1 Private Internal Cloud on-prem	2 Managed Private Internal Cloud on-prem	3 Managed Private Cloud off-prem	4 Virtual Private Cloud off-prem	5 Public Cloud off-prem	6 Community Cloud off-prem
Utilisation <sup>(1)</sup>	Single-Tenant	Single-Tenant	Single-Tenant	Single-Tenant	Multi-Tenant	Multi-Tenant / Communauté
Hébergement <sup>(2)</sup>	Exclusif BNPP	Exclusif BNPP	Exclusif BNPP	Public	Public	Groupe restreint
Ségrégation des ressources	Physique	Physique	Physique	Logique	Logicielle	Logicielle
Localisation des données et des traitements	Connue	Connue	Connue	Connue	Connue	Connue
Solution conçue et gérée par	BNPP <sup>(3)</sup> Fournisseur	Fournisseur	Fournisseur	Fournisseur	Fournisseur	Fournisseur
Solution opérée par	BNPP <sup>(3)</sup> Fournisseur	Fournisseur	Fournisseur	Fournisseur	Fournisseur	Fournisseur
Localisation des administrateurs	Connue	Connue	Connue	Non définie	Non définie	Connue
Analogie	Flotte de véhicules sur-mesure	Flotte de véhicules standards	Leasing de véhicules standards	Service de VTC (véhicules avec chauffeurs)	Transport en commun (bus, car)	Bus à accès restreint

(1) *Single-tenant* signifie que les services sont dédiés à BNP Paribas (une ou plusieurs entités). *Multi-tenant* signifie qu'une instance de la solution fournit en même temps le service à plusieurs clients.

(2) Exclusif signifie que l'infrastructure héberge uniquement des services BNP Paribas (la localisation dans un espace dédié et d'accès restreint d'un centre informatique n'appartenant pas à BNP Paribas peut être considérée comme un hébergement exclusif, sous réserve d'un contrat approprié et d'un dispositif adéquat de sécurité physique).

(3) ou un partenaire stratégique comme BP<sup>21</sup>

## 4

## Principales contraintes à l'utilisation du Cloud public

Les institutions financières doivent être particulièrement vigilantes dans leur usage du Cloud public et choisir la solution la plus appropriée à leur problématique de sécurité et de conformité.

Les défis majeurs d'une migration vers des services Cloud sont listés ci-dessous.

- **Sécurité** : Compte tenu de l'augmentation actuelle des cyberattaques et des fuites de données, il est primordial d'assurer la sécurité des données et des applications. En plus des prérequis en termes de sécurité et de continuité de services, les services Cloud doivent être en conformité avec la politique de gestion des données clients BNP Paribas, notamment concernant le chiffrement (à la fois en transit et au stockage), la suppression des données, la ségrégation des données et la bonne gestion des habilitations pour les traitements.
- **Conformité avec la législation et la réglementation** : De nombreux régulateurs bancaires exigent que les données bancaires des clients soient hébergées localement. D'autres règles de conformité exigent que les données bancaires ne soient pas mélangées avec d'autres données, notamment au sein de serveurs ou des bases de données partagés, et qu'elles ne soient pas transférées vers un autre lieu sans le consentement du client. Les directives et règlements de l'UE applicables, tels que le RGDP, doivent être respectés, tout comme l'ensemble des lois nationales et internationales susceptibles d'avoir une incidence sur les activités de l'entreprise. De plus, des contraintes réglementaires supplémentaires peuvent s'appliquer spécifiquement à certains Métiers, comme par exemple la loi HIPAA pour les activités d'assurance du Groupe BNP Paribas
- **Auditabilité - Reporting** : L'audibilité a une importance majeure dans le secteur bancaire et doit être traitée de façon spécifique. A minima, le fournisseur Cloud doit être en mesure de prouver le respect et l'application des exigences sécuritaires, juridiques et réglementaires des régulateurs. De plus, la conception technique, le déploiement et l'administration des services Cloud doit pouvoir être auditee par un auditeur externe.

- **Interopérabilité** : Les interfaces et flux fournis par la solution Cloud doivent permettre l'interopérabilité entre les systèmes internes et les services Cloud.
- **Performance des applications** : Les exigences de niveau de services relatives à la performance ne sont généralement pas négociables dans un Cloud Public. Si cela représente un obstacle majeur pour l'application, alors d'autres modes de déploiement doivent être considérés.
- **Engagement commercial / contractuel** : Avant de s'engager commercialement / contractuellement, il est important de formaliser une vision claire sur les risques et points d'attention suivants :
  - définir une **stratégie de sortie et de résiliation** de services Cloud en fonction des différents cas (en cas de force majeure, pour éviter un effet de verrouillage commercial, etc.) et les services d'assistance associés (par exemple : récupération des données/code, portabilité de la solution, etc.) ;
  - clarifier l'**écosystème du fournisseur**, en incluant les sous-traitants et les externalisations et en anticipant tout changement qui pourrait survenir dans cet écosystème ;
  - définir des clauses précises sur les **droits de propriété intellectuelle** pour nos algorithmes et les données associées, notamment en cas de co-création aussi bien avec un fournisseur Cloud qu'une Fintech.
- **Licences logicielles** : Une évaluation précise est nécessaire des risques techniques et commerciaux encourus lors de la migration vers le Cloud des licences logicielles de nos autres fournisseurs.
- **Modèle opérationnel** : Il faut évaluer les outils mis à disposition par le fournisseur Cloud pour administrer les services (self-service, niveau d'automatisation, etc.).
- **Modèle tarifaire à l'usage** : Il faut évaluer la complétude des données d'usage permettant de vérifier la consommation, la facturation à l'usage et la refacturation en interne.



[RETOURNER AU SOMMAIRE  
DE LA FORMATION](#)



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal

## LE CLOUD EN ACTION



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



# INTRODUCTION AUX CONTENEURS

*La vidéo précédemment utilisée ayant été mise hors ligne, nous l'avons remplacée par un article au contenu équivalent.*

## LIEN VERS L'ARTICLE

<https://www.lebigdata.fr/docker-definition>



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



[RETOURNER AU SOMMAIRE  
DE LA FORMATION](#)



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



# DOCKER 101 : CONCEPTS CLÉS

**LIEN YOUTUBE :**

<https://youtu.be/XgKOC6X8W28>

**Comment retrouver la vidéo via la barre de recherche Youtube :**

The screenshot shows a YouTube search result for a video titled "Tutoriel Docker : Présentation de Docker" by "Grafikart.fr". The video has 181k views and was uploaded 4 years ago. It includes a thumbnail of a blue whale carrying shipping containers, a duration of 23:03, and a link to an article: <https://grafikart.fr/tutoriels/docker-intro-634>. There is also a link to subscribe: <https://bit.ly/GrafikartSubscribe>.



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



RETOURNER AU SOMMAIRE  
DE LA FORMATION



**BNP PARIBAS**

La banque d'un monde qui change



30

BNPP Classification : Internal



# DOCKER 101 : COMMANDES PRINCIPALES

Docker est maintenant utilisé avec énormément de technologies, et vous pourriez avoir besoin d'apprendre vite ou de raviver de vieux souvenir. Voici une liste des commandes fondamentales à connaître pour utiliser Docker et Docker-Compose.

## Sommaire

1. Un peu de contexte
2. Commandes de monitoring
3. Commandes de runtime
4. Commandes de suppression
5. Commandes de logs



**BNP PARIBAS**

La banque d'un monde qui change



31

BNPP Classification : Internal



# DOCKER 101 : COMMANDES PRINCIPALES

## LIEN :

<https://www.padok.fr/blog/docker-docker-compose-commandes-connaître>

## 1. UN PEU DE CONTEXTE

Un conteneur est assez semblable à une VM.

Alors que la VM est une machine entièrement nouvelle (d'un point de vue software) construite sur une machine physique, un conteneur n'a de son côté pas tous les composants habituels d'une machine à habituellement. Pour être plus précis, il n'a pas d'OS entier, mais seulement ce qui est nécessaire pour faire tourner ses applications. Il est construit à partir d'une image, qui correspond à sa configuration.

Vous avez peut-être entendu parler de Docker-compose.

La différence entre Docker et Docker-compose est simple: les commandes Docker ne concernent qu'un seul conteneur (ou image) à la fois, alors que Docker-compose gère plusieurs conteneurs Docker.



**BNP PARIBAS**

La banque d'un monde qui change



32

BNPP Classification : Internal



# DOCKER 101 : COMMANDES PRINCIPALES

## 2. COMMANDES DE MONITORING

Les commandes suivantes sont les premières que vous avez besoin de connaître quand vous utilisez Docker.

**docker ps (-a)**

docker ps vous affiche toutes les instances de docker qui tournent actuellement sur votre environnement. Si vous ajoutez l'option -a, alors vous verrez même les containers stoppés.

**docker images (-a)**

Cette commande vous montre les images que vous avez construites, et le -a vous montre les images intermédiaires.

**docker network ls**

**docker-compose ps**

La commande docker network ls liste les différents réseaux et docker-compose ps affiche tous les containers qui ont été lancés par docker-compose (qu'ils tournent actuellement ou non).



**BNP PARIBAS**

La banque d'un monde qui change



33

BNPP Classification : Internal



# DOCKER 101 : COMMANDES PRINCIPALES

## 3. COMMANDES DE RUNTIME (1/2)

Vous avez maintenant besoin d'images et de conteneurs pour tester les commandes précédentes.

```
docker-compose up (-d) (--build)  
docker-compose stop
```

La docker-compose est la plus simple car vous n'avez besoin que de 2 commandes : up et stop. stop est assez explicite et stop (mais ne supprime pas) vos conteneurs, mais up nécessite plus d'explications : cela va construire vos images si elles ne le sont pas déjà, et va démarrer vos dockers. Si vous voulez re-build vos images, utilisez l'option --build (vous pouvez aussi utiliser la commande docker-compose build pour uniquement construire des images). L'option -d, qui signifie "detach" fait tourner les conteneurs en tâche de fond.

```
docker build (-t <NAME>) <PATH>/<URL>
```

Avec Docker, vous avez besoin d'une commande séparée pour construire votre image, où vous pouvez spécifier le nom de votre image et vous devez spécifier le PATH ou URL selon votre contexte (cela peut être un repo git).



**BNP PARIBAS**

La banque d'un monde qui change





# DOCKER 101 : COMMANDES PRINCIPALES

## 3. COMMANDES DE RUNTIME (2/2)

```
docker run (-d) (-p <hostPort>:<containerPort>) (--name <NAME>) <IMGNAME>/<IMGID>
```

run crée le conteneur en utilisant l'image que vous indiquez. Vous pouvez spécifier de nombreux paramètres. Nous vous recommandons d'ajouter un nom à votre conteneur et vous pourriez avoir besoin de spécifier quelques ports à exposer. Comme pour docker-compose, le -d lance le conteneur en tâche de fond.

```
docker start <ID>/<NAME>
```

```
docker stop <ID>/<NAME>
```

Le start and stop ne devraient pas être trop compliqués à comprendre, mais il faut noter que vous pouvez "start" uniquement des conteneurs qui sont déjà arrêtés, donc déjà build avec la commande run.

```
docker exec -it <NAME>/<ID> <"sh">/<"/bin/bash">
```

Cette commande vous permet de lancer un shell sur votre container. Je préfère utiliser "/bin/bash" mais votre conteneur peut ne pas avoir bash d'installé, et seulement "sh" qui est plus courant (surtout sur les alpines). Si vous avez des configurations spéciales dans votre conteneur, vous aurez peut-être besoin d'utiliser des arguments supplémentaires pour vous y connecter. Cette commande peut vous permettre de faire bien plus, je vous recommande donc de lire cette [doc](#) pour trouver des informations supplémentaires..





# DOCKER 101 : COMMANDES PRINCIPALES

## 4. COMMANDE DE SUPPRESSION

Ces commandes permettent de supprimer vos conteneurs et vos images. Vous en aurez probablement besoin pour libérer de l'espace disque.

```
docker rm <ID>/<NAME>  
docker-compose rm
```

Le docker rm supprime seulement un conteneur alors que docker-compose rm supprime tous les conteneurs démarrés avec une commande docker-compose.

```
docker rmi <ID>/<NAME>
```

Docker rmi supprime l'image que vous passez en paramètre et récursivement toutes les images intermédiaires utilisées pour la construire.





# DOCKER 101 : COMMANDES PRINCIPALES

## 5. COMMANDE DE LOGS

Les commandes suivantes sont utiles quand vous devez débugger certains de vos conteneurs (ou, plus souvent, l'application que vous déployez à l'intérieur).

**docker logs <ID>/<NAME> (-f --tail <NBLINE>)**

Cette commande affiche les logs du container passé en paramètre. Si vous utilisez l'option -f --tail <NBLINE> vous pouvez suivre en live le flux de vos logs (<NBLINE> est le nombre de lignes que vous souhaitez afficher). Gardez à l'esprit de choisir un nombre de lignes que vous serez capable de gérer, pour ne pas être dépassé par vos logs.

**docker-compose logs (<ID>/<NAME>)**

L'option (<ID>/<NAME>) avec docker-compose logs vous permet de voir les logs d'un conteneur uniquement, au lieu de voir tous les logs. L'astuce ici est que si vous n'utilisez pas l'option -d quand vous utilisez docker run ou docker-compose up vous verrez vos logs directement (mais vous aurez besoin d'arrêter le conteneur pour quitter la vue). Cela peut toujours être utile pour débugger des applications au démarrage.

Voici les commandes de base pour Docker et Docker-compose.



**BNP PARIBAS**

La banque d'un monde qui change



37

BNPP Classification : Internal



RETOURNER AU SOMMAIRE  
DE LA FORMATION



**BNP PARIBAS**

La banque d'un monde qui change



38

BNPP Classification : Internal

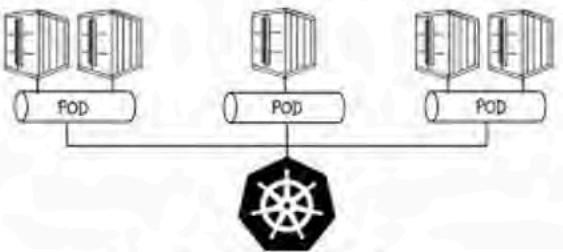


# INTRODUCTION À KUBERNETES

## LIEN YOUTUBE :

<https://youtu.be/NChhdOZV4sY>

## Comment retrouver la vidéo via la barre de recherche Youtube :



**Kubernetes : l'essentiel en 7 minutes**  
Cookie connecté • 78 k vues • il y a 2 ans  
Dans cette vidéo, je vous explique l'essentiel à retenir sur Kubernetes : - Qu'est ce que Kubernetes? - A quoi sert Kubernetes ...  
Sous-titres

**Kubernetes** 7:21



**BNP PARIBAS**

La banque d'un monde qui change



39

BNPP Classification : Internal



RETOURNER AU SOMMAIRE  
DE LA FORMATION



**BNP PARIBAS**

La banque d'un monde qui change



40

BNPP Classification : Internal



# INTRODUCTION À L'APPROCHE CLOUD NATIVE

**LIEN :**

<https://tanzu.vmware.com/fr/cloud-native>

## Qu'est-ce qu'une application cloud native ?

L'approche cloud native vise à développer et exécuter des applications capables d'exploiter tous les avantages du cloud. Ces dernières années, le cloud a bouleversé l'ordre établi dans presque tous les secteurs.

Et la raison est simple. Grâce à lui, les entreprises ont pu réduire les investissements consacrés à leurs data centers internes au profit de ressources de calcul illimitées, disponibles à la demande et facturées à l'utilisation. De fait, la réduction des coûts informatiques a fait tomber les barrières à l'entrée.

Désormais, la compétitivité d'une entreprise dépend directement de sa capacité à concrétiser rapidement de nouvelles idées. D'où la montée en puissance des logiciels. Les start-ups l'ont bien compris, c'est pourquoi elles misent sur les approches cloud natives pour disrupter les secteurs traditionnels.



**BNP PARIBAS**

La banque d'un monde qui change

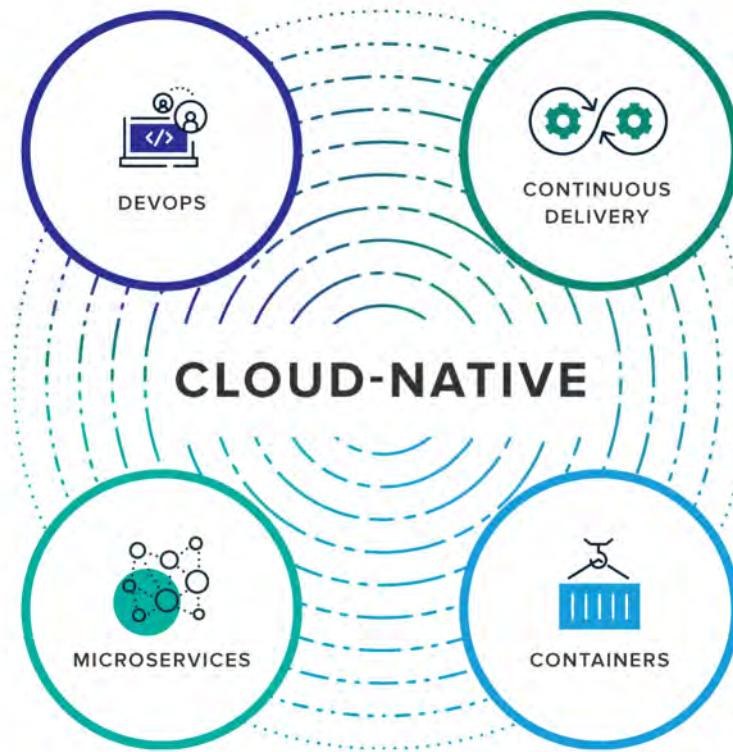


BNPP Classification : Internal



# INTRODUCTION À L'APPROCHE CLOUD NATIVE

Pour se mettre à l'heure du Cloud Native, les entreprises ont besoin d'une plateforme de création et d'exploitation dédiée, capable d'automatiser et d'intégrer les nouveaux concepts du développement logiciel – du DevOps aux conteneurs, en passant par le déploiement continu et les microservices :





# INTRODUCTION À L'APPROCHE CLOUD NATIVE

Dans une approche DevOps, développeurs et opérations IT travaillent main dans la main pour automatiser le processus de déploiement logiciel et les modifications d'infrastructure. Cette approche instaure une culture et un cadre propices pour des développements, tests et lancements plus rapides, plus fiables et plus fréquents.

Dans un modèle de déploiement continu, chaque modification applicative est mise en production dès sa finalisation. Nul besoin d'attendre la sortie d'une nouvelle version (au terme de l'intégration de multiples modifications), ni même de planifier une fenêtre de maintenance. Ainsi, chaque lancement devient un « non-événement ». Les équipes déploient des modifications de manière fiable, plus fréquente et moins risquée, tout en raccourcissant drastiquement la boucle de feedback. L'enjeu : intégrer les déploiements au cœur du processus métier et de la compétitivité de l'entreprise.

Les microservices désignent un type d'architecture où une application est développée sous la forme d'une collection de mini-services. Chaque service implémente des fonctionnalités métiers spécifiques, s'exécute dans son propre processus et communique via une API HTTP. Vous pouvez déployer, modifier, monter en capacités et redémarrer chaque microservice de façon indépendante, généralement à partir d'un système automatisé permettant des mises à jour fréquentes en production, sans aucun impact sur le client.





# INTRODUCTION À L'APPROCHE CLOUD NATIVE

Par rapport aux machines virtuelles (VM) standards, les conteneurs offrent à la fois des gains d'efficacité et de rapidité. Grâce à la virtualisation au niveau du système d'exploitation (OS), vous pouvez diviser une instance d'OS de façon dynamique en plusieurs conteneurs isolés, chacun possédant son propre système de fichiers en écriture et quota de ressources. Le faible impact de la création et suppression des conteneurs, combiné à la haute densité d'une VM unique, font des conteneurs un vecteur idéal pour le déploiement de microservices individuels.

« Ce que nous avons appris, c'est que le marché ne nous attend pas. Peu importe la qualité de l'ingénierie, du développement, du déploiement ou de la formation des équipes. Pour faire mouche, un produit doit sortir au bon moment. Après l'heure, c'est plus l'heure. »

James McGlennon, Vice-président exécutif et DSI, Liberty Mutual Insurance Group



**BNP PARIBAS**

La banque d'un monde qui change





# INTRODUCTION À L'APPROCHE CLOUD NATIVE

## Les avantages des applications cloud natives

Les applications cloud natives sont spécialement conçues pour le cloud. Le principe ? De petites équipes dédiées créent et déploient ces applications à partir d'une plateforme facilement scalable et découplée du matériel. À la clé, les entreprises disposent d'applications hautement agiles, résilientes et déployables dans divers formats de cloud.

### COMPÉTITIVITÉ

L'approche cloud native implique un revirement des objectifs : d'un simple outil de réduction des coûts informatiques, le cloud se transforme en moteur de votre croissance. À l'ère du logiciel, les grandes gagnantes seront les entreprises capables de développer et déployer rapidement des applications en réponse aux besoins de leurs clients. Une fois déployées, les applications doivent s'exécuter sous forme de services scalables et disponibles en continu.

### FLEXIBILITÉ

Les entreprises peuvent créer des applications qui s'exécuteront sur n'importe quel cloud, sans aucune modification. Leurs équipes ont ainsi la possibilité de migrer ou distribuer leurs applications entre divers clouds publics et privés pour satisfaire leurs priorités et réduire leurs coûts.

### DÉVELOPPEMENT OPTIMAL

Avec l'approche cloud native, les développeurs n'ont plus à tenir compte des contraintes d'exécution et de montée en charge sur une diversité d'infrastructures cloud. Ils se recentrent ainsi sur l'écriture de code à plus forte valeur ajoutée. Les applications de type « twelve-factor », utilisant des services courants dans des environnements de développement standardisés, suivent un modèle de « contrat » garantissant l'exploitation optimale de la plateforme cloud native sous-jacente.

### ALIGNEMENT DES OPÉRATIONS SUR LES MÉTIERS

À travers des processus automatisés, les opérations IT peuvent adopter une approche lean et se mettre au diapason des priorités métiers. Plutôt que de se concentrer sur les tâches d'administration ordinaires, elles peuvent se consacrer à l'amélioration des processus tout en supprimant les risques liés aux erreurs humaines. Enfin, grâce à des corrections et montées de version automatiques à tous les niveaux, elles peuvent éliminer les interruptions de service et l'intervention de techniciens chevronnés.



**BNP PARIBAS**

La banque d'un monde qui change





# INTRODUCTION À L'APPROCHE CLOUD NATIVE

## Comparatif : Applications cloud natives vs. Applications traditionnelles

### APPLICATIONS CLOUD NATIVES

**Prévisibilité.** Les applications cloud natives suivent un cadre ou « contrat » spécifique conçu pour maximiser leur résilience par la description de comportements prévisibles. L'infrastructure orientée conteneurs et hautement automatisée des plateformes cloud conditionne le mode d'écriture logicielle. Les 12 principes qui composent la méthodologie applicative à douze facteurs illustrent bien un tel « contrat ».

**Abstraction de l'OS.** Dans une architecture applicative cloud native, les développeurs utilisent une plateforme comme moyen d'abstraction des dépendances sous-jacentes de l'infrastructure, ce qui simplifie les migrations et montées en charge. La solution d'abstraction la plus efficace ? Une plateforme formalisée, VMware Tanzu par exemple, idéale pour des opérations sur une infrastructure cloud comme Google Cloud Platform (GCP), Microsoft Azure ou Amazon Web Services (AWS).

**Capacités sur mesure.** Une plateforme d'applications cloud natives automatise le provisionnement et la configuration de l'infrastructure, permettant ainsi une allocation dynamique de vos ressources selon vos besoins applicatifs. En vous appuyant sur une exécution cloud native, vous optimisez la gestion du cycle applicatif dans sa globalité : des montées en charge jusqu'aux opérations de restauration, en passant par l'utilisation et l'orchestration des ressources disponibles.

### APPLICATIONS D'ENTREPRISE TRADITIONNELLES

**Imprévisibilité.** Intrinsèquement, l'architecture et le modèle de développement des applications traditionnelles les empêchent d'exploiter tout le potentiel des plateformes cloud natives. Ces applications se déclinent dans des versions plus lourdes, plus longues à développer, peu scalables et sujettes à de nombreux points de défaillance uniques.

**Dépendance OS.** L'architecture applicative traditionnelle permet aux développeurs de créer des liens de dépendance étroits entre l'application et le système d'exploitation, les matériels, le stockage et autres services sous-jacents. Or, ces dépendances rendent complexe et périlleuse toute migration ou montée en charge des applications vers de nouvelles infrastructures, ce qui ne favorise pas la transition vers un modèle cloud.

**Capacités surdimensionnées.** Pour chaque application, l'approche informatique traditionnelle consiste à concevoir une solution d'infrastructure dédiée et sur mesure (on parle de « snowflakes » en anglais), ce qui allonge les délais de déploiement. Résultat : l'infrastructure est dimensionnée en fonction des estimations de pics de charge, ce qui la laisse le plus souvent en surcapacité sans pour autant pouvoir évoluer au-delà du seuil maximal défini.



# INTRODUCTION À L'APPROCHE CLOUD NATIVE

## Comparatif : Applications cloud natives vs. Applications traditionnelles

### APPLICATIONS CLOUD NATIVES

**Collaboration.** L'approche cloud native favorise l'adoption du DevOps. Outre une savante combinaison de talents, de processus et d'outils, vous instaurez une collaboration plus étroite entre vos développeurs et vos opérations IT, avec à la clé l'envoi plus rapide et plus fluide du code applicatif en production.

**Déploiement continu.** Les équipes informatiques déploient chaque mise à jour logicielle dès sa finalisation. Résultat : elles raccourcissent leur boucle de feedback et restent ainsi au plus proche des besoins de leurs clients. Le déploiement continu fonctionne encore mieux en conjonction avec d'autres approches, comme le développement centré sur les tests ou l'intégration continue.

**Indépendance.** Une architecture de microservices décompose les applications en une série de mini-services indépendants et faiblement couplés. Ces services sont eux-mêmes rattachés à des équipes de développement autonomes et de petite taille. Cette configuration permet des mises à jour fréquentes et indépendantes, ainsi que des montées en charge et des basculements/redémarrages sans impact sur les autres services.

### APPLICATIONS D'ENTREPRISE TRADITIONNELLES

**Cloisonnement.** Dans une approche traditionnelle, le code applicatif fini passe sans transition des développeurs aux opérations, dont la mission est de mettre ce code en production. La politique interne prend alors le pas sur le client. On assiste à des conflits et renvois de responsabilités qui ralentissent les déploiements et démoralisent les collaborateurs.

**Développement en cascade.** Traditionnellement, les nouvelles versions de logiciels sortent de façon régulière, généralement à des semaines voire des mois d'intervalle, une fois tout le code incorporé dans la version. Pourtant, de nombreux composants sont prêts avant l'heure et n'ont d'autre dépendance que le véhicule artificiel de cette version. Pendant ce temps, les fonctionnalités que les clients demandent, voire exigent, tardent à venir. Si bien que l'entreprise manque de nombreuses occasions de se démarquer, de conquérir de nouveaux clients et d'accroître son chiffre d'affaires.

**Dépendance.** Les architectures monolithiques regroupent de nombreux services disparates dans un seul et même pack de déploiement, avec pour conséquences des dépendances inutiles entre les services, ainsi qu'une perte d'agilité au cours du développement et des déploiements.



# INTRODUCTION À L'APPROCHE CLOUD NATIVE

## Comparatif : Applications cloud natives vs. Applications traditionnelles

### APPLICATIONS CLOUD NATIVES

**Scalabilité automatique.** L'automatisation à grande échelle permet d'appliquer un ensemble de règles cohérentes à des environnements et déploiements de toutes tailles. Résultat : vous éliminez les interruptions de service liées aux erreurs humaines. L'approche cloud native va au-delà d'une automatisation ad hoc, cas classique dans l'orchestration traditionnelle orientée virtualisation. De fait, dans une architecture cloud native, l'automatisation et l'orchestration travaillent pour les équipes de manière homogène, plutôt que de contraindre ces dernières à coder de tels processus au cas par cas, pour chaque application. En d'autres termes, l'automatisation simplifie le développement et l'exécution d'applications faciles à gérer.

**Restauration accélérée.** L'environnement d'exécution et l'orchestrateur de conteneurs ajoutent une couche de virtualisation dynamique à haute densité à vos VM. L'orchestration gère le placement des conteneurs de façon dynamique à travers un cluster de VM. L'objectif est double : assurer à la fois une scalabilité élastique et une reprise/un redémarrage rapide en cas de panne.

### APPLICATIONS D'ENTREPRISE TRADITIONNELLES

**Évolutivité manuelle.** Une infrastructure manuelle repose sur des opérateurs humains qui définissent et gèrent les configurations serveurs, réseau et de stockage. Compte tenu du degré de complexité, les opérateurs mettent énormément de temps à diagnostiquer les problèmes et ne parviennent pas à faire évoluer leurs environnements à grande échelle. Les solutions d'automatisation créées manuellement risquent de coder en dur les erreurs humaines dans l'infrastructure.

**Reprise lente.** Une infrastructure basée sur les VM est conceptuellement inadaptée aux impératifs de rapidité et d'efficacité des microservices. Longues à démarrer et à stopper, les VM individuelles pèsent sur l'infrastructure avant même le déploiement du code applicatif.



# INTRODUCTION À L'APPROCHE CLOUD NATIVE

**Les applications cloud natives vous intéressent ? Voici les points à retenir :**

## Transformation des opérations IT

De simple garante du statu quo, votre équipe opérationnelle se transformera en championne de l'amélioration et de l'automatisation des processus pour offrir plus de valeur aux différents métiers. Fini les interventions manuelles. Avec une plateforme cloud native, votre équipe déploie et exploite ses applications tout en profitant de fonctionnalités automatiques de monitoring et de résolution des problèmes.

## Priorisation des workloads

Attention, l'approche cloud native ne convient pas à tous les workloads. Ensemble, les fonctions IT et métiers doivent se concerter pour définir les priorités des workloads existants et nouveaux. Pour chacun, l'objectif est de déterminer la faisabilité technique, l'importance stratégique et le ROI d'une exécution cloud native. Outre des développements entièrement nouveaux, divers modèles de « replatforming » peuvent vous accompagner dans cette évaluation.

## Adoption de directives claires pour les développeurs

Pour exploiter tous les avantages d'une plateforme cloud native, vos développeurs doivent s'en tenir aux principes des 12 facteurs et utiliser des plateformes et services standardisés. Certains développeurs se sentiront peut-être les mains liées mais en définitive, les avantages offerts par la plateforme cloud native devraient avoir raison de leurs réticences.



**BNP PARIBAS**

La banque d'un monde qui change



49

BNPP Classification : Internal



# INTRODUCTION À L'APPROCHE CLOUD NATIVE

## Approche « build » ou « buy » ?

De nombreuses équipes envisagent le développement de leur propre plateforme à partir d'une combinaison de technologies open-source d'automatisation et de conteneurs. Toutefois, elles découvrent rapidement qu'il leur faut plus de composants que prévus. Elles doivent également déployer des efforts conséquents pour intégrer tous ces éléments, ce qui retarde évidemment le démarrage du développement d'applications. Une fois qu'elles disposent d'une telle plateforme, elles doivent ensuite en effectuer la maintenance. À l'inverse, avec une plateforme intégrée et éprouvée comme VMware Tanzu, les équipes peuvent se concentrer dès le premier jour sur la création d'applications porteuses de valeur pour les métiers, sachant que la plateforme couvre toutes les questions opérationnelles et d'infrastructure.

## Inutile de faire cavalier seul.

Comme souvent, l'apprentissage « en immersion » reste la meilleure solution. Au contact des équipes Pivotal Labs, vos développeurs pourront s'imprégner des pratiques de développement agile (DevOps, déploiement continu, etc.) et développer de nouveaux réflexes de programmation. On trouve une pléthore d'informations sur ce modèle : faites-en l'expérience et jugez par vous-même ! Aujourd'hui, 75 % des équipes pensent que leur entreprise manque d'agilité. Si vous en faites partie, c'est l'occasion idéale d'oser quelque chose de nouveau.



**BNP PARIBAS**

La banque d'un monde qui change





[RETOURNER AU SOMMAIRE  
DE LA FORMATION](#)



**BNP PARIBAS**

La banque d'un monde qui change



51  
BNPP Classification : Internal



## LIEN YOUTUBE :

<https://youtu.be/ucHwp1jUS2w>

## Comment retrouver la vidéo via la barre de recherche Youtube :

Comprendre les microservices en 6 minutes

Cookie connecté • 30 k vues • il y a 1 an

Dans cette vidéo, je vous explique l'essentiel à retenir des microservices : - Qu'est que l'architecture en microservices ...

Sous-titres

**Microservices** 6:32





[RETOURNER AU SOMMAIRE  
DE LA FORMATION](#)



**BNP PARIBAS**

La banque d'un monde qui change



53

BNPP Classification : Internal



# DEVOPS : UN ACCÉLÉRATEUR DU MOVE TO CLOUD

## LIEN :

<https://www.padok.fr/blog/cloud-devops-complementaires>

## LE CLOUD ET LE DEVOPS SONT-ILS COMPLÉMENTAIRES ?

Petit rappel sur la culture DevOps : La méthodologie DevOps consiste à lisser les relations entre les équipes de développeurs et les Ops afin de faire des mises en production plus rapides et de meilleure qualité. Toujours dans un but de compétitivité lié à l'environnement actuel.

Le Cloud et le DevOps sont indépendants et pourtant fonctionnent difficilement l'un sans l'autre. Vous allez me dire que l'on peut faire du DevOps sans Cloud et inversement. Vous avez raison... mais le Cloud vient booster le DevOps. Ce combo gagnant Cloud et DevOps comporte plusieurs avantages.

### Une amélioration continue...

Pour réussir à offrir des améliorations constantes aux utilisateurs finaux, il faut réduire les cycles de production. Pour cela, la culture DevOps a besoin d'outils qui lui permettent cette souplesse et rapidité d'exécution. Les fournisseurs Cloud tels que AWS, Google Cloud Platform (GCP), OVH et Azure proposent notamment des outils DevOps directement intégrés à leurs services (gestionnaires de code source, de chaînes d'intégration, ...).

### ... grâce à l'intégration continue

L'intégration continue est un des principaux concepts du DevOps. C'est un ensemble de pratiques qui consistent à tester de manière automatisée chaque révision de code avant de le déployer en production. Cela permet donc d'accélérer les développements et les mises en production.



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



# DEVOPS : UN ACCÉLÉRATEUR DU MOVE TO CLOUD

## Le Cloud, une solution de flexibilité

En SaaS, le logiciel est accessible partout, à tout moment, il suffit d'une connexion internet. Vos équipes peuvent ainsi travailler de n'importe où. Avec la démocratisation du Remote, c'est un facteur à prendre en compte.

Le Cloud c'est aussi un service qui évolue facilement et rapidement en fonction de votre croissance et du nombre de collaborateurs. Une solution On Premise par opposition est beaucoup plus figée. Ajouter de la puissance aux serveurs ne se fait pas en quelques minutes par exemple. Vous gagnez par ailleurs du temps car vous ne vous occupez plus des mises à jour. Le fournisseur s'en occupe pour vous. Votre service informatique peut se concentrer sur d'autres tâches.

Les Ops ont aussi accès, grâce au Cloud, à un service qui leur permet une grande flexibilité de volume, de stockage et qui intègre directement tous les outils DevOps dont ils ont besoin pour être productifs. Ce qui permet aux équipes opérationnelles de se concentrer sur la mise en production et l'analyse du besoin des développeurs, sans penser à la coupure de serveurs physiques, à la maintenance, aux capacités, etc.

## Le Cloud, une solution moins coûteuse

Historiquement, les serveurs étaient stockés dans les entreprises et demandaient une maintenance lourde et fastidieuse. Les coûts fixes de l'installation d'un logiciel sur un serveur physique d'une entreprise sont plus élevés que les coûts variables d'un abonnement Cloud utilisateur mensuel. En effet pour un serveur en propre, il faut prendre en compte le prix des licences d'utilisation, les coûts de maintenance ainsi que les coûts liés aux problématiques de redondance, de résilience, etc. Le Cloud est donc une solution économique qui permet de payer à la consommation réelle et qui est accessible au plus grand nombre. Notamment pour les startups qui n'ont pas une forte capacité d'investissement.





# DEVOPS : UN ACCÉLÉRATEUR DU MOVE TO CLOUD

## Une équipe DevOps et une entreprise plus sereines

La combinaison DevOps et Cloud a profité aux entreprises européennes. En effet, selon une étude de CA Technologies, elles enregistrent une hausse de 129% de leur performance de déploiement. Elles notent aussi une amélioration de leur expérience client de 108% par rapport aux modèles de déploiement traditionnels. Elles annoncent avoir un meilleur contrôle des coûts et des ressources utilisées par les équipes DevOps. Des chercheurs ont par ailleurs constaté que l'association Cloud et DevOps réduit les tensions dans le processus de développement et de déploiement. Ce qui a un impact direct sur la compétitivité de l'entreprise.

Vous l'aurez compris, l'environnement actuel étant ultra concurrentiel, les entreprises doivent être capable de s'adapter rapidement aux évolutions du marché et aux exigences toujours plus importantes des utilisateurs. C'est pour cette raison que les sociétés se tournent de plus en plus vers le Cloud. Mais certaines activités nécessitant une haute confidentialité des données (les sociétés publiques telles que la défense par exemple) ont des réticences à opter pour un hébergement en mode SaaS. Comme mentionné précédemment, il n'existe pas encore de lois internationales qui régissent cette nouvelle pratique qui consiste à stocker des données en dehors de sa propriété, voire en dehors du pays où l'entreprise exerce. La raison principale pour un hébergement On Premise reste donc bien souvent la sécurité des données. Il est donc important de se poser les bonnes questions avant d'adopter le duo Cloud et DevOps.





# DEVOPS : UN ACCÉLÉRATEUR DU MOVE TO CLOUD

## COMMENT ADOPTER CE DUO GAGNANT CLOUD & DEVOPS ?

Pour mettre en place le duo gagnant Cloud et DevOps en toute sérénité dans votre entreprise, suivez les étapes suivantes :

1. Établir un cahier des charges pour bien cerner vos besoins et définir un budget.
2. Choisir un modèle IaaS, PaaS ou SaaS. Cette partie concerne vos ressources internes. Avez-vous suffisamment de salariés dans votre service informatique pour s'occuper l'infrastructure matérielle ? Avez-vous la place d'accueillir des serveurs ? Etc.
3. Choisir un modèle de déploiement privé, public ou hybride. Ici, la question tourne autour de votre solution. Son besoin de puissance évolue-t-il ? Utilise-t-elle des données sensibles (attention aux règles du RGPD) ? Etc.
4. Définir les outils dont vos équipes de développement et opérationnelle ont besoin. Un point d'attention, il existe un très grand nombre d'outils intégrés dans le Cloud. Il est très facile de s'y perdre et d'avoir une mauvaise surprise sur la facturation. Même si le Cloud coûte de base moins cher que le On Premise, si vous ajoutez une multitude d'outils, la facture peut rapidement monter. Il est donc important de faire un benchmark avant de se lancer pour comprendre quels outils correspondent à vos besoins.
5. En fonction de la sélection des outils, vous pourrez faire le choix de votre fournisseur Cloud (AWS, GCP, OVH ou Azure).



**BNP PARIBAS**

La banque d'un monde qui change





RETOURNER AU SOMMAIRE  
DE LA FORMATION



**BNP PARIBAS**

La banque d'un monde qui change



58

BNPP Classification : Internal

# DÉCOUVRIR LE CLOUD PUBLIC IBM



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



# INFRASTRUCTURE DU CLOUD PUBLIC IBM

## AU SERVICE DE LA RÉSILIENCE, PORTABILITÉ ET SÉCURITÉ DES TRAITEMENTS INFORMATIQUES

### Les avantages d'une infrastructure Cloud Public

La technologie Cloud permet de transformer « l'endroit » où l'informatique crée de la valeur pour les utilisateurs. L'utilisation du Cloud continue de se diffuser chez la plupart des entreprises, quels que soient leurs niveaux d'adhésion ou maturité.

L'utilisation du Cloud se traduit par le recours à des services d'infrastructure clés, comme les réseaux, les capacités de calcul ou de stockage, la sécurité et le management, afin d'assurer la scalabilité, sécurité et résilience des traitements informatiques. les services Cloud offrent une réelle valeur ajoutée aux entreprises, puisqu'ils offrent un accès à des services de paiement à l'utilisation, à aux offres en libre-service et à une scalabilité à la demande, sans avoir à en assumer les coûts d'exploitation

Les services d'infrastructure IBM Cloud permettent aux entreprises d'accéder aux capacités du Cloud Public, tout en assurant la sécurité des applications et l'isolation des données.

*« Les entreprises qui basculeront sur le Cloud exploiteront une variété de services d'infrastructure pour faire tourner à la fois leurs anciennes applications, compatibles avec le cloud et les applications cloud natives. Les services d'infrastructure d'un cloud public fournissent aux entreprises des capacités en termes d'évolutivité, de sécurité, d'intégration et de résilience. DevOps permet également à l'entreprise de déployer, valider et gérer ses infrastructures comme des services (Infrastructure as a Service - IaaS) »*

Paul Bahrs,  
Distinguished Engineer, IBM Cloud and Cognitive Software



**BNP PARIBAS**

La banque d'un monde qui change



60

BNPP Classification : Internal



# INFRASTRUCTURE DU CLOUD PUBLIC IBM

## LES PRINCIPAUX COMPOSANTS

Lors d'une transition vers une infrastructure Cloud, les entreprises ont tendance à construire leurs solutions en utilisant des briques d'architectures communes et reproductibles. Ces briques permettent d'exploiter rapidement une nouvelle plate-forme ou service et peuvent être utilisées comme points de départ pour créer une solution sur-mesure. Ces schémas d'architecture s'appuient sur plusieurs services essentiels Cloud :

### RÉSEAU

Il est possible de connecter des centres de données « on-prem » avec le Cloud IBM pour intégrer l'exploitation, la supervision et la gestion des traitements. L'architecture de réseau permet de communiquer entre les services et les utilisateurs, dans un dispositif privé ou public.

Un Cloud privé virtuel (VPC) est un type de Cloud permettant de fournir (via un firewall) un certain niveau d'isolement entre les différentes organisations qui utilisent les ressources Cloud. Certaines offres proposent des fonctionnalités automatisées qui nécessitent une intervention minimale. Contrairement à un type de Cloud public traditionnel, ici le fournisseur Cloud destine une partie de son infrastructure à un seul utilisateur.

### SECURITÉ

Il est possible d'exploiter des services Cloud servant uniquement un client ou plusieurs organisations clientes pour gérer les traitements. Il est possible d'appliquer des contrôles d'accès entre les comptes et les organisations, et d'autoriser ou limiter les communications entre les différents réseaux et dispositifs de calcul. Les fournisseurs de Cloud proposent également services de gestion des chiffrements, des SSH et des IP pour automatiser la gestion et l'utilisation de ces ressources

### CAPACITÉ DE CALCUL

Il est possible de fournir l'infrastructure brute sous forme de service (IaaS) pour les traitements gourmands en puissance de calcul et en E/S. Les serveurs virtuels permettent de répondre au besoin d'allouer rapidement des ressources supplémentaires.

Les services spécialisés disposent des certifications VMware, Power et SAP. Le GPU NVIDIA permet de gérer les traitements complexes et gourmands en puissance de calcul. Les serveurs Bare-metal peuvent également fournir les performances nécessaires pour faire face aux applications exigeantes (consommation de processeurs et E/S importante)

### STOCKAGE

Il est possible d'utiliser le stockage cloud comme moyen de stockage indépendant ou complémentaire, comme une solution de stockage standard ou comme un ensemble de composants utilisés pour construire une solution propre.

Les services de stockage Cloud IBM proposent l'ObjectStorage, le stockage de fichiers, de blocs ou de SSD, chaque service étant conçu pour répondre à différentes exigences des traitements.



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal

## USERS & OTHER SERVICES

## IBM CLOUD

### Platform Management



### Asset Services



### Cloud Management



LOGGING



CLOUD MESSAGING



MONITORING

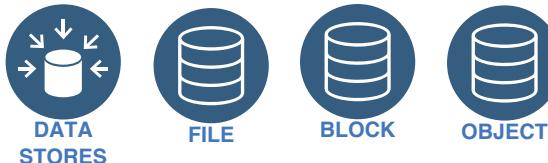


NOTIFICATION



BACKUP/ DR

### Storage & Data



### Runtime Management



### Compute & Run Time



### Connectivity



### Security



TRANSPORT SECURITY



IDENTITY &  
ACCESS  
MANAGEMENT



DATA SECURITY



NETWORK SECURITY



APPLICATION SECURITY



SECURITY  
VISIBILITY

## ENTERPRISE



END  
USER



EDGE  
SERVICES



OTHER  
CLOUD  
SERVICES



END  
USER



ENTERPRISE  
DATA



TRANSFORMATION &  
CONNECTIVITY



ENTERPRISE  
SERVICES



EXISTING  
ENTERPRISE  
SYSTEMS

### LEGEND

- █ Users
- █ Application component
- █ Infrastructure services
- █ Management
- █ Data store
- █ Analytics
- █ Security



# INFRASTRUCTURE DU CLOUD PUBLIC IBM

POUR EN SAVOIR PLUS SUR LE CLOUD PUBLIC IBM:

<https://www.ibm.com/cloud/garage/architectures/public-cloud>



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



[RETOURNER AU SOMMAIRE  
DE LA FORMATION](#)



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal



# CATALOGUE DU CLOUD PUBLIC IBM

**LIEN :**

<https://www.ibm.com/fr-fr/cloud/products>

## Produits IBM Cloud

Explorez un vaste portefeuille de produits cloud - comprenant l'infrastructure, les outils et les services pour développeurs



**BNP PARIBAS**

La banque d'un monde qui change



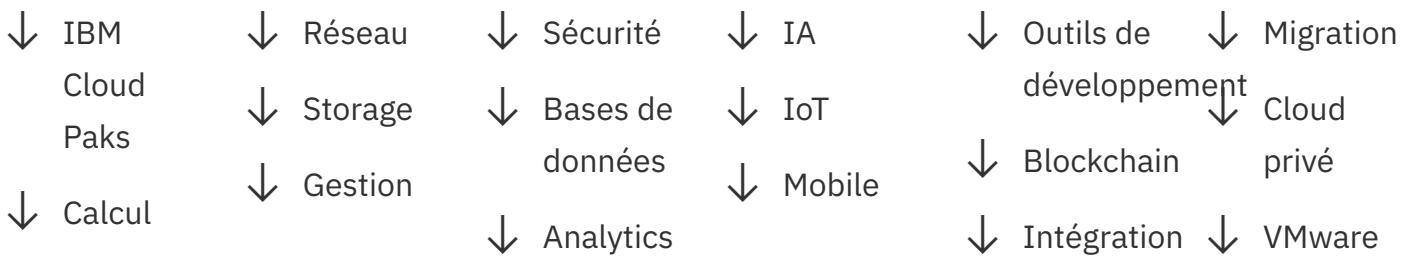
BNPP Classification : Internal

# Produits IBM Cloud

Explorez un vaste portefeuille de produits cloud - comprenant l'infrastructure, les outils et les services pour développeurs

Site feedback

[En savoir plus sur le niveau gratuit](#)



## IBM Cloud Paks

Un moyen plus rapide et plus fiable de se moderniser et de migrer vers le cloud. [En savoir plus](#)

### [IBM Cloud Pak for Data](#)

Accélérez votre modernisation par l'IA avec une plateforme de données native du Cloud

### [IBM Cloud Pak for Multicloud Management](#)

Augmentez l'efficacité opérationnelle grâce à une analyse intelligente des données et des signaux prédictifs majeurs, et obtenez un support intégré pour la gestion de la conformité

### [IBM Cloud Pak for Security](#)

Discutons

Intégrez des outils de sécurité pour mieux comprendre les menaces dans les environnements multicloud hybrides

### IBM Cloud Pak System

Créez, déployez et gérez des applications conteneurisées et des charges de travail Kubernetes - sur site, à la périphérie ou sur n'importe quel Cloud

### IBM Cloud Pak for Applications

Passez d'une architecture monolithique aux microservices via des méthodologies Devops et des kits d'outils de modernization

### IBM Cloud Pak for Integration

Propulsez votre transformation digitale avec une solution simple et complète pour adopter une approche moderne de l'intégration

### IBM Cloud Pak for Automation

Créez et exécutez des applications d'automatisation partout, sur le cloud de votre choix

Site feedback

## Calcul

Depuis les serveurs bare metal jusqu'aux calculs sans serveur, IBM offre des ressources pour tous les types de charge de travail. [En savoir plus](#)

### IBM Cloud for VMware Solutions

Déplacer les charges de travail VMware depuis le site local vers IBM Cloud

#### Serveurs bare metal

Serveurs cloud hautes performances avec configurations à l'heure ou au mois

#### Serveurs virtuels Cloud

Discutons

## Serveurs virtuels publics et dédiés avec provisionnement et extension à la demande

### Serveurs de stockage de masse

Gérez votre propre serveur bare metal de stockage de masse avec le système d'exploitation de votre choix, ou déployez une appliance clés en main et faites une demande de placement

### Infrastructure certifiée SAP

Exécutez et gérez vos applications SAP dans le cloud sur des serveurs bare metal

### Registre des conteneurs

Stockez et distribuez des images Docker dans un registre privé géré

### Service IBM Cloud Kubernetes

Orchestrez une planification intelligente, une réparation spontanée et une mise à l'échelle horizontale

### Cloud foundry

Déployez et faites évoluer vos applications sans configurer ni gérer vos serveurs manuellement

### IBM Cloud Functions

Une plateforme de programmation polyglotte de fonctions sous forme de service (FaaS) basée sur Apache OpenWhisk

### IBM WebSphere Application Server on Cloud

Lancez des applications Java nouvelles ou existantes dans le cloud, avec des options uniques et à service partagé

### Mise à l'échelle automatique

Discutons

Développez ou réduisez automatiquement votre environnement cloud en fonction de la

## Logiciels du serveur

Une gamme complète d'options logicielles pour simplifier l'administration de l'infrastructure

### HPCaaS depuis Rescale

Accélérez la résolution des problèmes à l'aide d'une plateforme de calculs haute performance (HPC) clé en main sous forme de service, avec automatisation intégrée et s'exécutant sur IBM Cloud

Site feedback

# Réseau

Gérer de très performants et rentables réseaux publics, privés et de gestion. [En savoir plus](#)

### Dispositifs réseau

Gérez les réseaux physiques et virtuels avec des routeurs, des pare-feux, des tunnels VPN et des équilibriseurs de charge

### Content Delivery Network (CDN)

Évitez les embouteillages réseau et diminuez le temps d'attente en maintenant les données plus près des utilisateurs

### Lien direct

Sécurisez et accélérez le transfert de données entre l'infrastructure privée et IBM Cloud

### Services de noms de domaine

Service complet d'enregistrement et d'administration de domaines

### Équilibrer de charge

Discutons

Équilibrer le trafic entre les serveurs pour améliorer le temps de disponibilité et les performances

## Sécurité réseau

Les pare-feu et les groupes de sécurité aident à protéger les serveurs et les utilisateurs finaux des activités malveillantes

Site feedback

## IBM Cloud Internet Services

Un guichet unique alliant sécurité et performance conçu pour protéger les contenu et les applications Web publics avant qu'ils n'atteignent le cloud

# Storage

Choisissez dans un ensemble de services de stockage d'objets, de blocs et de fichiers, tous robustes et durables. [En savoir plus](#)

## Stockage d'objets

Un service de stockage pour les données non structurées, conçu pour la durabilité, la résilience et la sécurité

## Stockage par blocs

Performances de disque local avec support flash et persistance et durabilité d'un réseau de stockage

## Stockage de fichiers

Stockage de fichiers NFS avec support flash durable, rapide et flexible

## IBM Cloud Backup

Solution de sauvegarde et de récupération de niveau entreprise avec automatisé Discutons évolutivité, intégrations tierces, chiffrement et capacités « multivaulting »

# Gestion

Améliorez la gestion des infrastructures, des applications, des processus et des environnements de cloud complets. [En savoir plus](#)

Site feedback

## Availability Monitoring

Exécutez des tests synthétiques pour détecter et corriger les problèmes de performance avant qu'ils n'impactent les utilisateurs

## IBM Cloud Automation Manager

Permet au département informatique de déployer, automatiser et gérer des environnements multi-cloud

## IBM Cloud Event Management

Corrélation, hiérarchisation et résolution des événements opérationnels et des incidents

## Planificateur de charge de travail

Allez au-delà de la commande Cron et créez des workflows qui fonctionnent à des moments précis, ou sur une base régulière ou encore par événement

## IBM Log Analysis avec LogDNA

Fonction de collecte de journaux et de recherche qui collecte automatiquement les données des applications et des services

## IBM Cloud Monitoring avec Sysdig

Surveillance en temps réel et alerte pour la visibilité opérationnelle dans les applications, plateformes et services basés sur Kubernetes

## Des règles métier

Discutons

## Automatisez et gérez la logique et les décisions métier en dehors des applications

### Istio

Exécutez Istio sur IBM Cloud Kubernetes Service pour connecter, gérer et sécuriser les microservices à grande échelle

Site feedback

## Sécurité

Intégrez la sécurité dans les applications, les services et l'infrastructure grâce à des outils d'authentification, de sécurité réseau et de surveillance. [En savoir plus](#)

### IBM Cloud Activity Tracker

Affichez, gérez et vérifiez l'activité dans le cloud

### App ID

Ajoutez une fonction d'authentification à vos applications Web et mobiles, y compris pour la connexion aux médias sociaux

### Sécurité réseau

Les pare-feux et les groupes de sécurité protègent les serveurs et les utilisateurs des activités malveillantes

### Certificats SSL

Chiffrez les données entre les applications client et serveur

### IBM Cloud Certificate Manager

Stockez et gérez de façon centralisée vos certificats dans un référentiel sécurisé

### Module de sécurité matériel

Unité physique avec gestion et stockage de clés

Discutons

## Services de protection Hyper

Protection au niveau du mainframe pour les données en mémoire, en transit et au repos

### IBM Cloud Data Shield

Activez le chiffrement de la mémoire d'exécution pour les conteneurs Kubernetes sans modifier les applications

### IBM Cloud Security Advisor

Centralisez vos moyens de gestion, d'analyse et de résolution conceranant la sécurité

Site feedback

### Key Protect

Gestion du cycle de vie des clés de chiffrement utilisées par les services IBM Cloud ou les applications personnalisées

# Bases de données

Un volumineux portefeuille de bases de données SQL et NoSQL conçu pour des charges de travail transactionnelles, des applications Web et mobiles et une analyse ultra-rapide. [En savoir plus](#)

### IBM Cloudant®

Magasin de documents JSON NoSQL optimisé pour les lourdes charges de travail de lectures et d'écritures simultanées

### IBM Compose

Moteur de base de données qui alimente plus de 10 bases de données SQL et NoSQL open source

### IBM Compose for JanusGraph

Discutons

Base de données graphique évolutive, optimisée pour stocker et effectuer des requêtes sur des données fortement interconnectées

### [IBM Compose for MongoDB for Cloud](#)

Indexation et interrogation puissantes associées à une évolutivité et une sauvegarde automatisées

Site feedback

### [IBM Compose for MySQL for Cloud](#)

SGBDR rapide et facile à utiliser avec des connecteurs incluant Python, PHP et C++

### [IBM Compose for RethinkDB for Cloud](#)

Base de données répartie, optimisée pour les documents JSON et le Web en temps réel

### [IBM Compose for ScyllaDB for Cloud](#)

Magasin NoSQL par colonnes qui affiche 1 million de transactions par seconde et par nœud

### [IBM Cloud Databases for Elasticsearch](#)

Combine la flexibilité d'un moteur de recherche en texte intégral à la puissance de l'indexation JSON

### [IBM Cloud Databases for etcd](#)

Magasin de valeurs de clés contenant les données correctes nécessaires à la gestion des clusters de serveurs

### [IBM Cloud Databases for PostgreSQL](#)

Une base de données SQL objet-relationnelle avec des fonctions et des pilotes de publication/d'abonnement JSON indexables

### [IBM Cloud Databases for Redis](#)

Utilisez les compteurs, les files d'attente, les listes et les « hyperlogs » pour traiter simplement des problèmes de données complexes

### [IBM Db2 Hosted Flex](#)

Discutons

Une base de données SQL multicharge à la demande avec un accès administrateur complet

### IBM Db2 on Cloud

Base de données cloud SQL entièrement gérée, configurée et optimisée pour des performances fiables

### IBM Db2 Warehouse on Cloud

Un service d'entrepôt de données Cloud entièrement géré et basé sur IBM BLU Acceleration for Cloud

### IBM Informix on Cloud

Moteur hautes performances qui intègre des données TimeSeries, Spatial, NoSQL et SQL

### IBM Lift

Migrez les données rapidement, facilement et en toute sécurité via une interface de ligne de commande

Site feedback

## Analytics

Recherchez des outils de science des données, des entrepôts de données et des plateformes pour exécuter des travaux d'analyse sur de grands ensembles de données. [En savoir plus](#)

### IBM Analytics Engine

Service combiné Apache Spark et Apache Hadoop pour la création d'applications d'analyse

### IBM Analytics for Apache Spark for Cloud

Cadre de traitement de clusters open source, polyvalent, avec analyse en mémoire rapide

### IBM Decision Optimization

Discutons

Environnement décisionnel en libre-service conçu pour exploiter un support basé sur l'optimisation

### [IBM Db2 Warehouse on Cloud](#)

Service d'entrepôt de données de cloud entièrement géré, alimenté par IBM BLU Acceleration

### [IBM Master Data Management on Cloud](#)

Obtenez une vue fiable des données dans un environnement informatique hybride.

Site feedback

### [IBM InfoSphere Information Server on Cloud](#)

Comprenez, gérez, créez, maintenez, transformez et délivrez des données de qualité

### [IBM Streaming Analytics](#)

Analysez un large éventail de données en streaming : texte, vidéo, audio, géospatiales et de capteurs

## IA

Tirez parti d'IBM Watson pour le traitement du langage naturel, la reconnaissance visuelle et l'apprentissage automatique. [En savoir plus](#)

### [IBM Watson Studio](#)

Créez et formez des modèles d'IA, et préparez et analysez les données, le tout dans un seul environnement intégré

### [Catalogue IBM Watson Knowledge](#)

Reconnaissance intelligente de données et d'actifs d'analyse, catalogage et gouvernance pour alimenter les applications d'IA

### [IBM Watson Assistant](#)

Discutons

## Construisez et déployez des assistants virtuels

### [IBM Watson Discovery](#)

Découvrez des connexions dans les données en combinant l'ingestion automatisée et des fonctions d'IA avancées

Site feedback

### [Plateforme IBM Watson IoT](#)

Exploitez un service entièrement géré et hébergé dans le cloud pour l'enregistrement des appareils, la connectivité, le contrôle, la visualisation rapide et le stockage des données

### [IBM Watson Speech to Text](#)

Transformez facilement des données audio et vocales en texte écrit

### [IBM Watson Text to Speech](#)

Convertissez le texte écrit en audio naturel dans toute une variété de langues et de voix

### [IBM Watson Language Translator](#)

Traduisez dynamiquement des actualités, des brevets ou des documents conversationnels

### [IBM Watson Natural Language Classifier](#)

Interprétez et classifiez le langage naturel avec confiance

### [IBM Watson Natural Language Understanding](#)

Analysez le texte pour extraire les métadonnées du contenu, par exemple les concepts, les entités et les sentiments

### [IBM Watson Visual Recognition](#)

Étiquetez, classifiez et recherchez du contenu visuel en utilisant l'apprentissage automatique

### [IBM Watson Tone Analyzer](#)

Analysez les émotions et les tons dans le contenu écrit

Discutons

## IBM Watson Personality Insights

Prévoyez les caractéristiques de personnalité, les besoins et les valeurs via le texte écrit

## IBM Data Refinery

Un outil de préparation des données en libre-service pour les spécialistes des données, les ingénieurs et les analystes métier

## IBM Watson Machine Learning

Créez, formez et déployez des modèles d'auto-apprentissage à l'aide de flux de travaux collaboratifs automatisés

## Apprentissage en profondeur

Concevez et déployez des modèles d'apprentissage en profondeur à l'aide de réseaux neuronaux, évoluez facilement jusqu'à des centaines de cycles de formation

## IBM Watson Discovery for Salesforce

Activez des agents de service client sur Salesforce Service Cloud pour rechercher les sources de données d'entreprise et résoudre les cas complexes

## IBM Watson Knowledge Studio

Entraînez Watson à comprendre les nuances linguistiques de votre secteur industriel

## IBM Watson OpenScale

Utilisez et automatisez l'IA tout au long de son cycle de vie, avec confiance et transparence

# IoT

Explorez une plateforme permettant de connecter des appareils et des données avec des ensembles de données et des API de The Weather Company. [En savoir plus](#)

Discutons

## Plateforme IBM Watson IoT

Connectez appareils, passerelles et réseaux, et gérez, sécurisez et analysez les données associées

### API de données météorologiques

Intégrez les données météorologiques de The Weather Company dans des applications

Site feedback

## Mobile

Utilisez la plateforme et les outils pour créer des applications mobiles natives et des backends mobiles robustes. [En savoir plus](#)

### IBM Mobile Foundation

Accès mobile sécurisé et évolutif qui simplifie l'intégration aux services de back end et de cloud

### IBM Cloud App ID

Ajoutez une fonction d'authentification à vos applications Web et mobiles, y compris pour la connexion aux médias sociaux

### IBM Mobile Analytics

Surveillez les performances et l'utilisation de toutes vos applications depuis votre ordinateur de bureau ou votre tablette

### IBM Push Notifications

Envoyez des notifications en temps réel aux applications mobiles et Web

## Outils de développement

Discutons

Découvrez les outils de pipeline et d'interface CLI nécessaires pour fournir de nouvelles mises à jour, en continu et de meilleure qualité. [En savoir plus](#)

## IBM Cloud Continuous Delivery

Mettez à disposition des chaînes d'outils, automatisez des builds et des tests, et contrôlez la qualité avec l'analytique

## IBM Cloud DevOps Insights

Données pour améliorer la productivité des développeurs, la qualité du code et écourter les cycles de distribution

## IBM Cloud Lift CLI

Une façon unifiée d'interagir avec les applications, les conteneurs, l'infrastructure et les services

## Kits de démarrage

Utilisez ces kits pour créer rapidement des applications cloud prêtes à la production

## IBM Cloud Developer Console for Apple

Générez et déployez des applications sur IBM Cloud pour la plateforme Apple

Site feedback

# Blockchain

Développez la confiance dans les transactions avec un grand livre blockchain non modifiable.

## IBM Blockchain Platform

Accélérez le développement, la gouvernance et le fonctionnement d'un réseau pluri-institutionnel

Discutons

# Intégration

Intégrez des applications et des données via des API, des outils de messagerie et de mise en réseau. [En savoir plus](#)

Site feedback

## [IBM API Connect](#)

Création et gestion d'API, avec sécurité et gouvernance intégrées

## [IBM App Connect](#)

Solution d'intégration avec des centaines de connecteurs intégrés pour systèmes de données sur site et SaaS

## [IBM Aspera on Cloud](#)

Transférez, échangez et automatisez la distribution de vos données volumineuses sur les clouds hybrides à une vitesse maximale

## [IBM Event Streams](#)

Apache Kafka sous forme de service, hébergé et entièrement géré, pour un réseau principal de messagerie hautes performances et évolutif

## [IBM MQ on Cloud](#)

Messagerie d'entreprise qui simplifie et accélère l'échange fiable et sécurisé des données

## [IBM Cloud Messages for RabbitMQ](#)

Acheminez, suivez et mettez en file d'attente des messages en utilisant plusieurs protocoles

## [Lien direct IBM Cloud](#)

Sécurisez et accélérez le transfert de données entre l'infrastructure privée et IBM Cloud

Discutons

## [Passerelle sécurisée](#)

Établissez un tunnel sécurisé entre les ressources spécifiques que vous souhaitez connecter

## Migration

Migrez vos applications et données existantes vers le cloud à l'aide d'un portefeuille d'outils et de services de migration.

Site feedback

### [IBM Lift](#)

Migrez les données rapidement, facilement et en toute sécurité via une interface de ligne de commande

### [IBM Cloud Mass Data Migration](#)

Déplacer des téraoctets ou des pétaoctets de données en toute sécurité en utilisant des unités de stockage protégées de capacité 120 To

### [IBM WebSphere Application Server on Cloud](#)

Lancez des applications Java nouvelles ou existantes dans le cloud, avec des options à service exclusif et à service partagé

## Cloud privé

Expérimenez la puissance du Cloud avec un meilleur contrôle, une sécurité renforcée et un isolement accru.

### [IBM Cloud Private](#)

IBM Cloud derrière votre pare-feu et dans votre centre de données

### [IBM Cloud Dedicated](#)

Discutons

Un environnement IBM Cloud à service exclusif hébergé dans l'un des data centers d'IBM

## VMware

Migrez vos charges de travail VMware existantes vers le cloud avec l'aide d'IBM et des services partenaires.

Site feedback

### [IBM Cloud for VMware Solutions](#)

Déplacez des charges de travail VMware d'un site local vers IBM Cloud

### [F5 on IBM Cloud](#)

Déplacez en toute fluidité des charges de travail VMware vers IBM Cloud à l'aide de la plateforme F5 qui conjugue performances, disponibilité et sécurité

### [Fortinet on IBM Cloud](#)

Transférez des règles de sécurité sur site vers IBM Cloud for VMware Solutions avec un riche ensemble de fonctions de pare-feu virtualisées et physiques

### [IBM Cloud Secure Virtualization](#)

Fournit du matériel pour protéger les charges de travail virtualisées jusqu'au niveau des microprocesseurs

### [IBM Cloud for Skytap Solutions](#)

Répliquez l'environnement complet de centre de données des applications existantes pour faciliter la migration vers le cloud

### [IBM Spectrum Protect Plus on IBM Cloud](#)

Mettez à disposition une solution de protection et de disponibilité des données dans un environnement VMware existant ou nouveau

### [Veeam on IBM Cloud](#)

Discutons

Combinez sauvegarde, restauration et réPLICATION pour mieux gérer les environnements vSphere et Hyper-V

### VMware Horizon on IBM Cloud

Offre une solution de bureau virtuel de bout en bout entièrement gérée

### Zerto on IBM Cloud

Protégez, développez et migrez des charges de travail d'hyperviseur existantes, y compris VMware, vers IBM Cloud

Site feedback

## Que pouvez-vous construire avec IBM Cloud ?

Contactez-nous

Discutons

# **FIN DE LA FORMATION**

# **CLOUD 101**



**BNP PARIBAS**

La banque d'un monde qui change



BNPP Classification : Internal