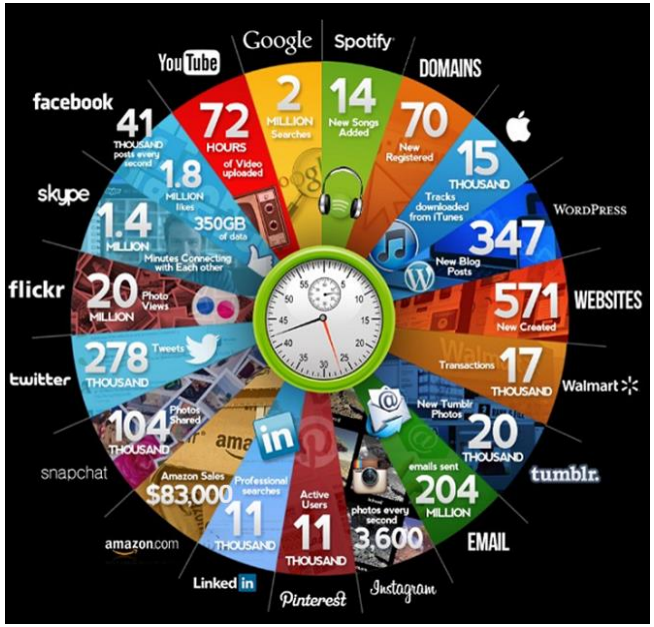
PRESENTATION DU BIG DATA
chez ITIM, GTS et BSC

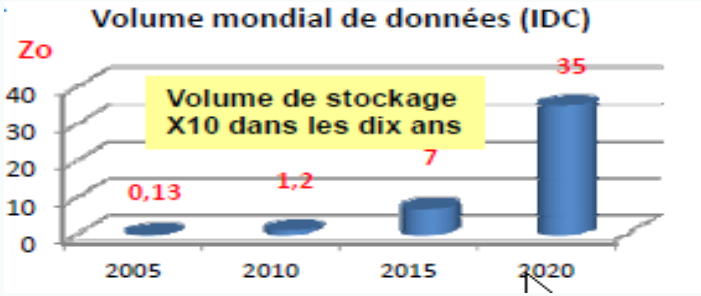
08/09/2017

La révolution de la donnée

L'humanité produit aujourd'hui en deux jours autant de données qu'elle en a produites jusqu'en 2003, de toute son histoire.

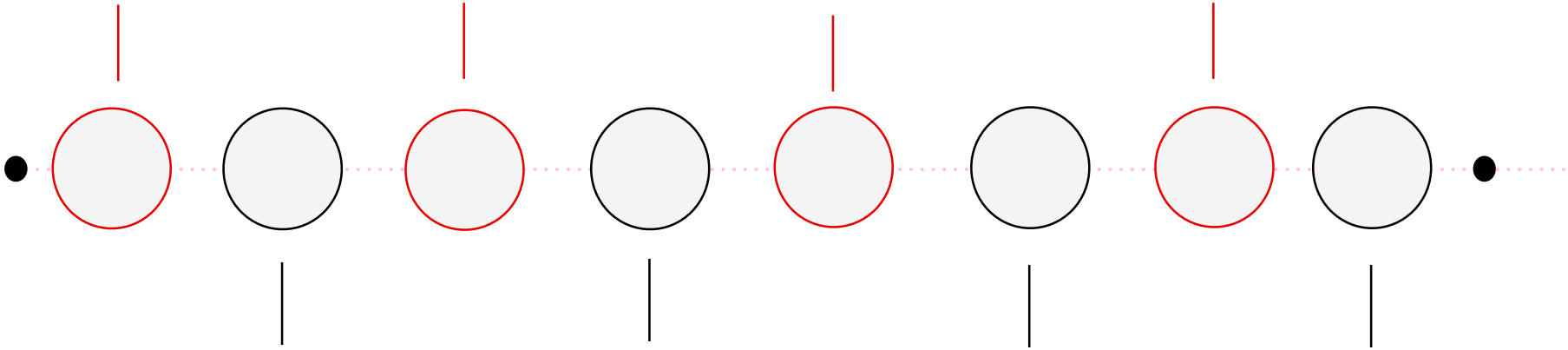


Explosion des données, structurées, non structurées ou semi-structurées (réseaux sociaux) : textes, dessins vectoriels, images, vidéo, voix, …



Gigaoctets (10^9 octets) >> Téraoctets (10^{12} octets) >> Pétaoctets (10^{15} octets) >> Exaoctets (10^{18} octets) >> Zettaoctets (10^{21} octets)

Un peu d'histoire…



2002
Moteur de Recherche Nutch

2003
Google publie un papier sur GFS,
Une architecture de stockage distribuée

2004
Google publie un papier sur Map Reduce,
Une architecture de traitement distribuée

2005
Map Reduce et HDFS au sein de Nutch

2006
Hadoop séparé de Nutch et devient un projet Apache

2008
Hadoop projet prioritaire de la fondation Apache

2011
Version stable 1.0 d'Hadoop

2013
Version majeure 2.2 d'Hadoop

Le Big Data et ses cas d'usage actuels

Big Data — ITIM | GTS | BSC — Centre de compétences

Définition du Big Data :

« données structurées ou non dont le très grand volume requiert des outils d'analyse adaptés » (en français : mégadonnées)

Caractéristiques du Big Data :

	AUJOURD'HUI	DEMAIN
	STRUCTUREES	NON STRUCTUREES
INTERNES	Transactions et opérations bancaires, données de référence, données de synthèse	Textes (outils CRM, documents dématérialisés, logs, mails, images, vidéo, … échangés entre collaborateurs, avec les clients, etc.
EXTERNES	Bases de données externes (partenaires, …), référentiels publics	Textes, images, vidéos, … issus d'internet et des réseaux sociaux

Les principaux cas d'usage à ce jour :

Améliorer la vision 360 du client
En complétant d'informations internes et externes sur, par exemple, le comportement, les centres d'intérêt

Exploration
Chercher, visualiser et comprendre les données pour améliorer la connaissance du business

Analyse de données IT
Analyser les données techniques (logs) des applications afin d'améliorer la qualité de service

Sécurité
Diminuer les risques avec la détection de fraudes et la mise en place d'une « cyber-sécurité » en temps réel.

Capacité de stockage
Augmenter l'efficacité opérationnelle de l'infrastructure (baisse des coûts de stockage, amélioration des performances, etc.)

Principes de construction du Big Data à la Société Générale (1/2)

En regard du contexte, la construction du Big Data au sein de la Société Générale a adopté les principes suivants :

DATALAKE

Constituer un « data lake » permettant un stockage unique d'un **maximum de données** (maximum de sources, maximum de variétés) pour répondre à **un maximum de besoins**

VISION

Avoir une vision ambitieuse (interconnexion de toutes les données de l'entreprise, voire avec les données externes) et associée à une stratégie des « petits pas » (expérimentation, méthode et structure agile, …).

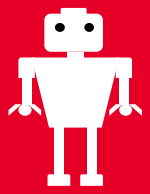
COOPERATION

Faire coopérer les différentes directions de l'entreprise, **facteur clé** de réussite dans la valorisation de la donnée (partage de la donnée)

SECURISATION

Avoir une politique de **sécurisation interne et externe de la donnée** et des usages pour être conforme aux réglementations sur les données personnelles, et pour **prévenir les risques opérationnels** et notamment le risque d'image

OPEN SOURCE



Etre **compatible** avec les outils Open Source pour être en capacité de suivre les évolutions technologiques

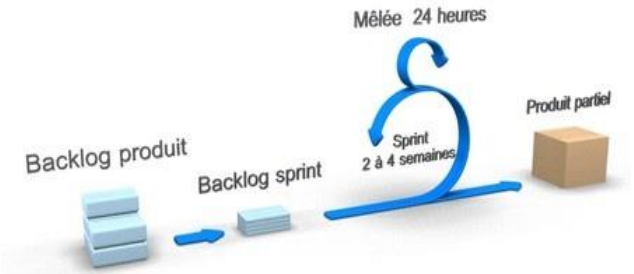
Principes de construction du Big Data à la Société Générale (2/2)

Le contexte nous impose de coller au plus près des besoins des clients, notamment pour réduire le Time to market.

Il est donc nécessaire de proposer un ensemble Big Data « agile » à tous les niveaux :

Agilité dans les **processus** (organisation et méthode)

- Organisation : pizza team , proximité avec les métiers, décloisonnement des services
- Méthodes : Lean Startup, développement agile, DevOps



Agilité dans **l'architecture** (logicielle et infrastructure)

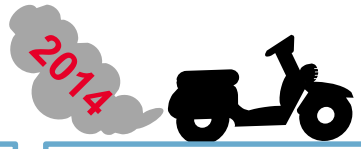
- Infrastructure : Construction par itération
- Logicielle : Proximité avec les outils Open Source

Timeline du Centre de Compétences

2013

- 2 ETP
- Location infra Hadoop 5 nodes

2014

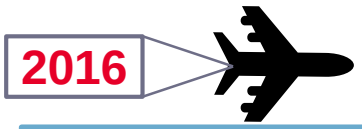


- 10 ETP
- Cluster Hadoop externe

2015

- 20 ETP
- Cluster Hadoop 11 nodes
- Cluster ElasticSearch 5 nodes
- 6 applications en production

2016

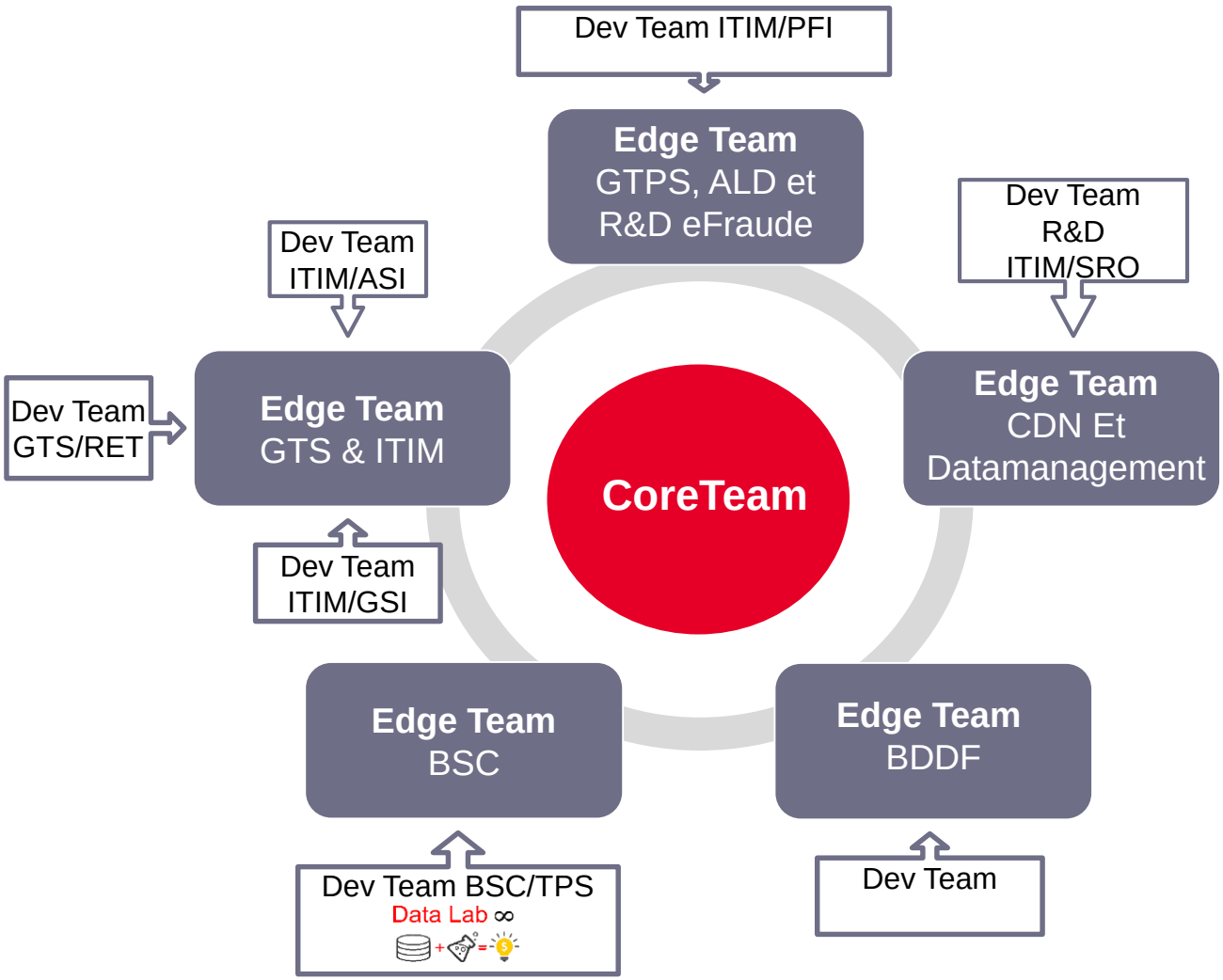


- 60 ETP
- Internalisation du Cluster Hadoop Production : 28 nodes (1200 core, 8,6 To Ram, 650 To utiles)
- 2 Po de stockage
- 175 serveurs
- 2 clusters dev / Hot
- Cluster ElasticSearch 20 nodes
- 22 applications en production
- 9 enseignes clients

2017

- Site de secours (28 serveurs)
- Ferme de serveur de datascience
- Cluster Hadoop Production : 50 nodes
- Ingestion de 1 milliards d'événements jour sur ELK

Organisation du Centre de compétence Big Data



Core Team

Equipe en charge de l'architecture technique, fonctionnelle, du datamanagement, de la sécurité, de l'infrastructure et de l'ensemble des sujets transverses (méthodologie, normes, support)

Edge Team

Equipe en charge du projet sur des technologies Big Data

Dev teams

Equipe à l'extérieur du Competency Center en charge d'effectuer les développements à partir des services mis à disposition par la Edge team

Le Big Data – Domaines d'application

- Amélioration de la connaissance client
- Détection de fraudes
- Développement / Amélioration de scores

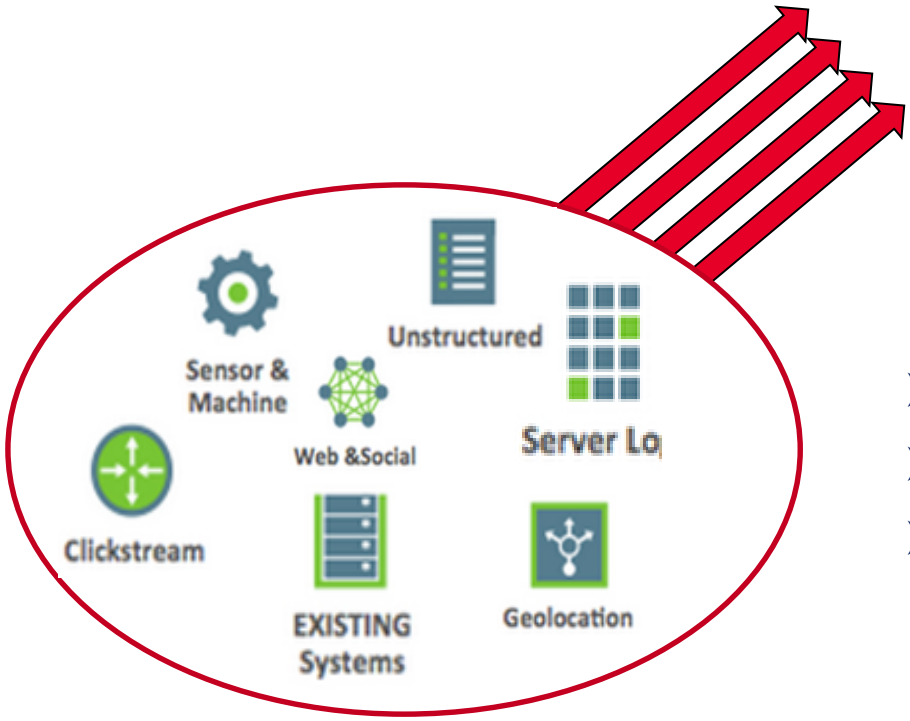
EXPLORATION

VISION 360

SECURITE

DONNEES IT

STOCKAGE



- Amélioration des process et organisation
- Monitoring et troubleshooting
- Optimisation des temps de traitements

Supervision & Innovation

« Projet Reporting SHIELD sur les équipements Réseaux Hélios »

Enjeux métiers

- Remplacer la plateforme d'hébergement Internet actuelle I2BD par la mise en place d'une nouvelle infrastructure baptisée HELIOS, qui devient en 2015 le nouveau Point d'Accès Internet du Groupe SG
- Répondre aux nouveaux besoins des utilisateurs et à l'accélération des évolutions des nouvelles technologies

Enjeux SI

- Rendre possible **l'analyse d'un volume important** de données quelques secondes après sa génération par les machines
- **Superviser** en temps-réel les nombreuses technologies mises en œuvre
- **Sécuriser** l'accès aux données, pour les administrateurs comme pour les applications utilisatrices d'Hélios

Solutions

hadoop

Hunk

elasticsearch.

30ème plateforme d'échanges avec Internet

200 applications hébergés en France et dans le Monde

9 millions de clients uniques par mois

550 serveurs sur 3 datacenters

1 milliard d'événements par jour classifiés C2

Offre de services

GESTION DES DONNEES

Collecte
Alimentation HADOOP
Exploitation des données

ACCES AUX DONNEES

Exploration de données

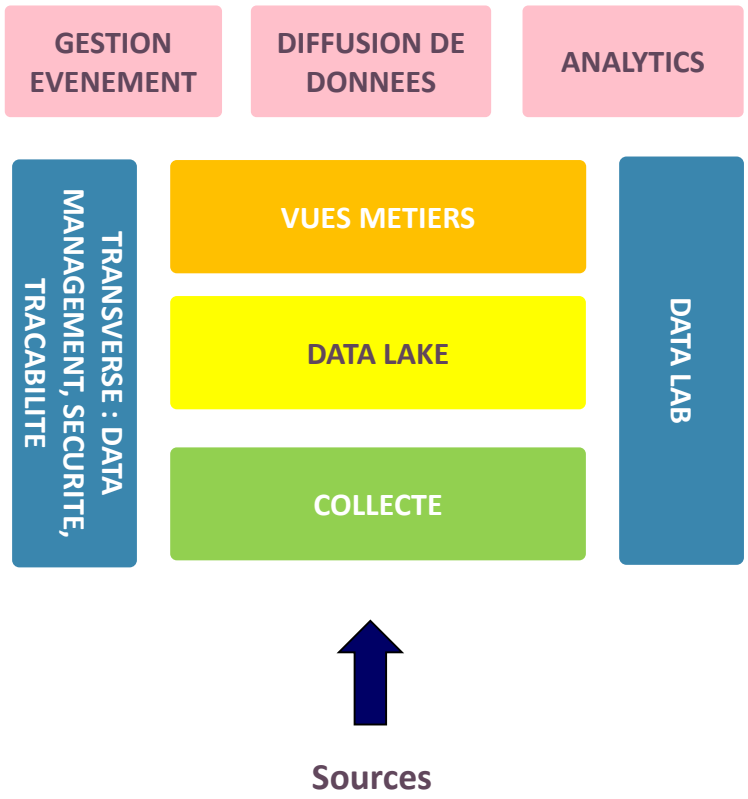
DATAMINING

Machine Learning
Modèles prédictifs
Analyse statistique

VISUALISATION DES DONNEES

Tableau de bords
Indicateurs

Architecture des fonctions de la plateforme Big Data



Fonctions transverses
Fonctions transverses de data-management sur le stockage élémentaire et sur les indicateurs, traçabilité des accès aux données, protection des données et traçabilité des usages

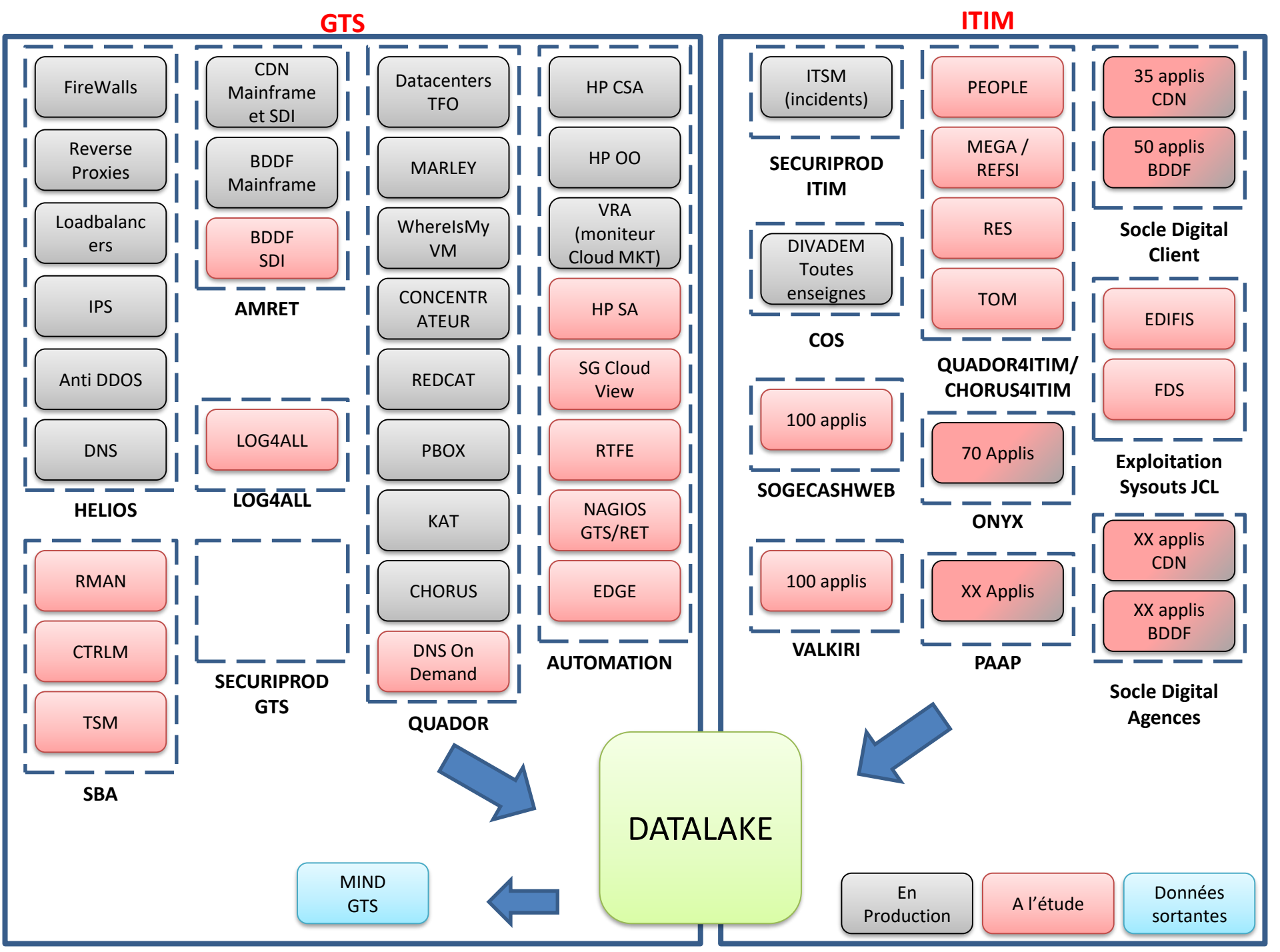
Services
Diffusion des données : restitutions produites par les traitements Big Data, pouvant être diffusées aux applications / utilisateurs du SIO ou SID
Analytics : exploration des données, traitements statistiques et machine learning
Gestion des évènements : alerting, modèle de prédiction, de règles

Datalab
Stockage des données brutes ou d'informations utiles (i.d. transformées) à des fins d'étude ou d'expérimentation

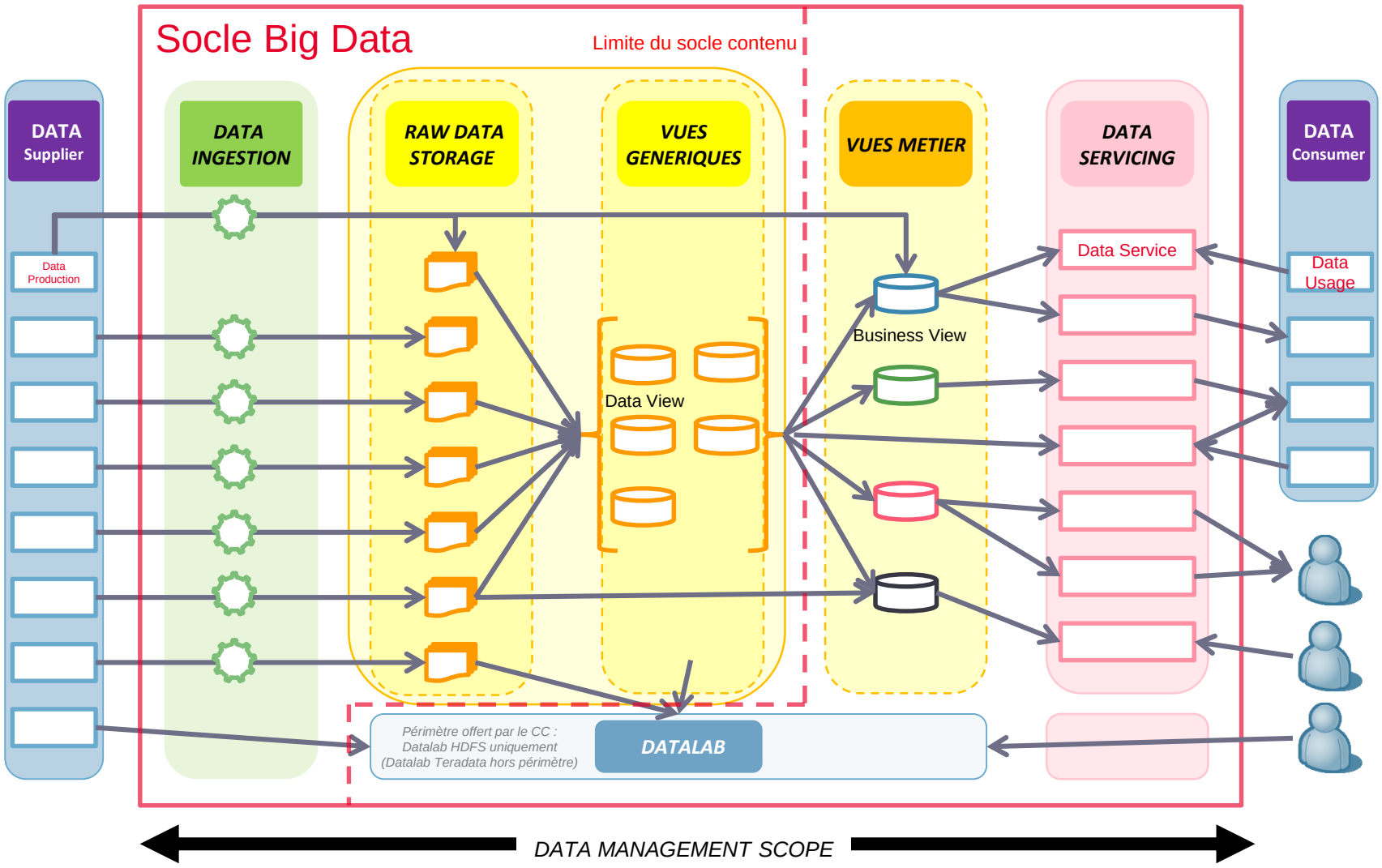
Vues métiers
Stockage d'informations utiles (données extraites du data lake, calculées agrégées ou transformées) ayant vocation à être utilisées par les services

Data Lake
Stockage des données brutes collectées sans aucune transformation
Stockage d'informations utiles, produites par le Big Data, communes à plusieurs vues métiers

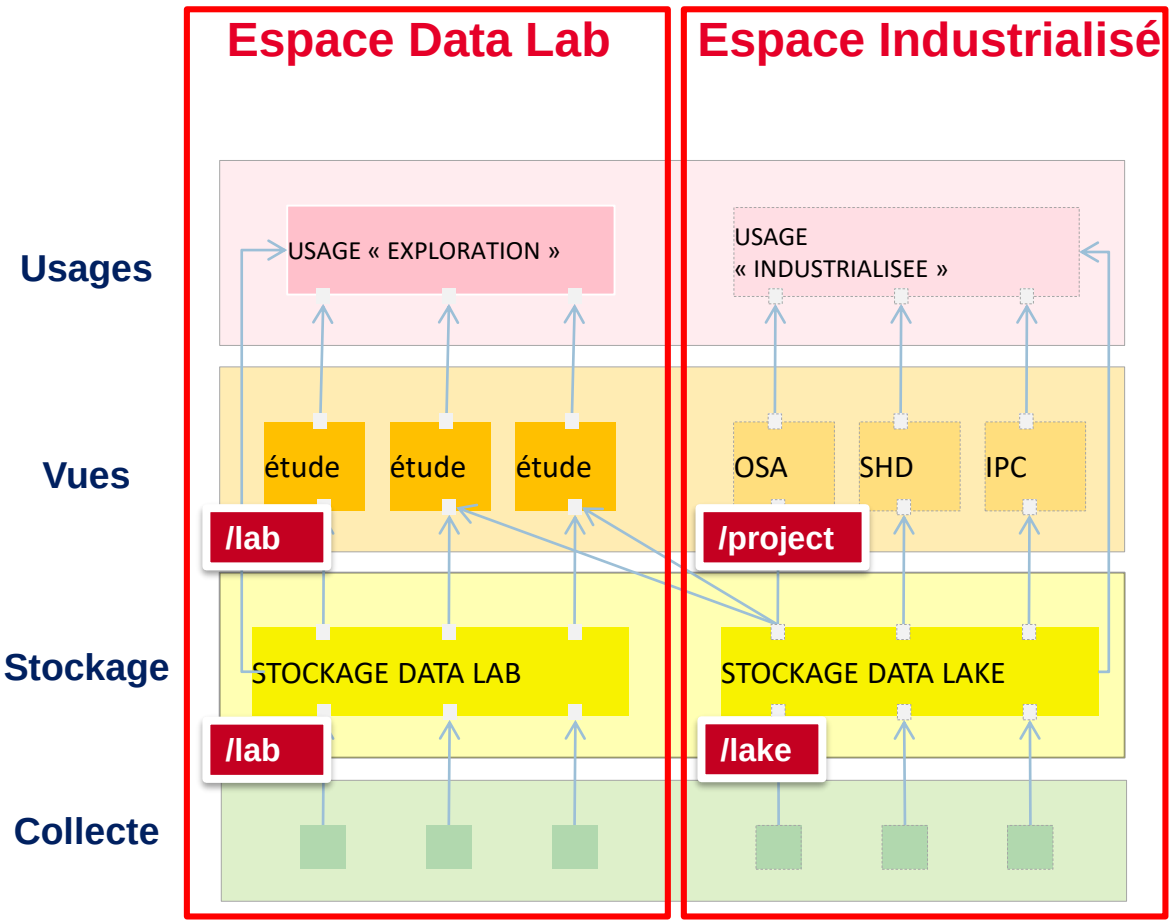
Collecte
Collecte des données des différentes sources (par batch ou au fil de l'eau)


GTS
ITIM
FireWalls
Reverse Proxies
Loadbalancers
IPS
Anti DDOS
DNS
HELIOS
CDN Mainframe et SDI
BDDF Mainframe
BDDF SDI
AMRET
LOG4ALL
LOG4ALL
RMAN
CTRLM
TSM
SBA
SECURIPROD GTS
Datacenters TFO
MARLEY
WhereIsMy VM
CONCENTRATEUR
REDCAT
PBOX
KAT
CHORUS
DNS On Demand
QUADOR
HP CSA
HP OO
VRA (moniteur Cloud MKT)
HP SA
SG Cloud View
RTFE
NAGIOS GTS/RET
EDGE
AUTOMATION
ITSM (incidents)
SECURIPROD ITIM
DIVADEM Toutes enseignes
COS
100 applis
SOGECASHWEB
100 applis
VALKIRI
PEOPLE
MEGA / REFSI
RES
TOM
QUADOR4ITIM/ CHORUS4ITIM
70 Applis
ONYX
XX Applis
PAAP
35 applis CDN
50 applis BDDF
Socle Digital Client
EDIFIS
FDS
Exploitation Sysouts JCL
XX applis CDN
XX applis BDDF
Socle Digital Agences
DATALAKE
MIND GTS
En Production
A l'étude
Données sortantes

DATA MANAGEMENT - Périmètre & écosystème



Exploration des données dans l'environnement Big Data



- Usage « exploration » pour le marketing (exemple : manipulation des données avec SAS, R Hadoop, HIVE, Hunk)
- Vues : stockage physique ou logique des données pour un usecase ou un ensemble de usecases cohérents.
  1. Les vues de l'espace Data Lab peuvent accéder aux données de l'espace de stockage Data Lab et Data Lake
  2. Les vues de l'espace industrialisé ne peuvent accéder qu'à l'espace de stockage Data Lake
- Stockage Data Lake : stockage pour les usages métiers industrialisés (process automatisé de la collecte, de calcul d'indicateur, …) organisé par sources de données

- Stockage Data Lab : Stockage pour les usages métiers adhoc, ie usage oneshot, exploration, recherche de modèle. Les process ne sont pas industrialisés. Le calcul des indicateurs est pris en charge par les métiers (écriture des scripts, lancement, …). Cf. détail page suivante
- Collecte :
  1. alimentation Data Lab manuelle (via BT ou interface)
  2. alimentation automatisée par batch ou au fil de l'eau

OSA : logs applicatives du poste de travail PUMA
SHD : logs techniques des points d'accès internet
IPC : logs de navigation web

Architecture logicielle
Des outils sélectionnés et positionnés

Big Data — ITIM | GTS | BSC

SOURCE DE DONNEES

- EXISTING Systems
- Web &Social
- Sensor & Machine
- Clickstream
- Geolocation
- Server Logs
- Unstructured

INTEGRATION DE DONNEES

Ingestion (batch)

Sqoop, Flume, Logstash, Pig, TOM, talend, syslog-ng

Streaming (fil de l'eau)

Storm, kafka, Flume, Spark Streaming, syslog-ng

USAGES DES DONNEES

- **Analyse batch** : HUE, SQL, Pig, Hunk
- **Analyse interactive** : HUE, Kibana, SQL, Hunk
- **Analyse prédictive** : Spark MLlib, H2O, SAS, R Studio
- **API** : d3.js, node.js, WebHDFS

VUES METIERS

- **Batch** : Hive, Map Reduce
- **Interactif NoSQL** : mongoDB, APACHE HBASE
- **Interactif Search Engine** : IDOL OnDemand, elastic
- **Temps réel** : Spark

DATA LAKE - DATALAB

HDFS : système de fichiers distribué — hadoop HDFS

TRANSVERSE : DATA MANAGEMENT, SECURITE, TRACABILITE

Data Management | Habilitations : **Ranger, Shield, LDAP, Knox** | Audit : **Ranger** | Cryptage : hp **Encryption**

EXPLOITATION

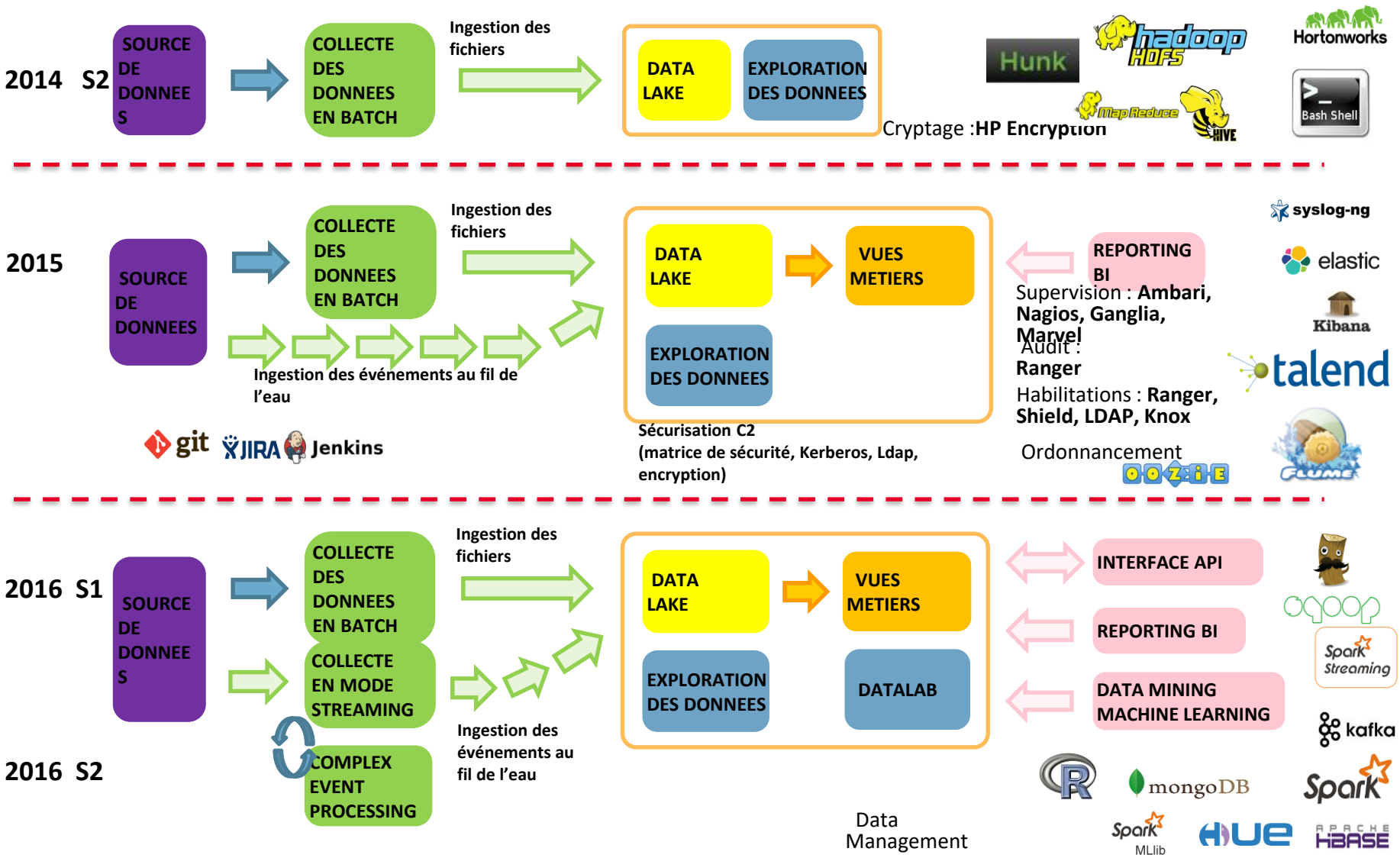
Supervision : **Ambari, Nagios, Ganglia, Marvel** | Ordonnancement : OOZIE

DEVELOPPEMENT

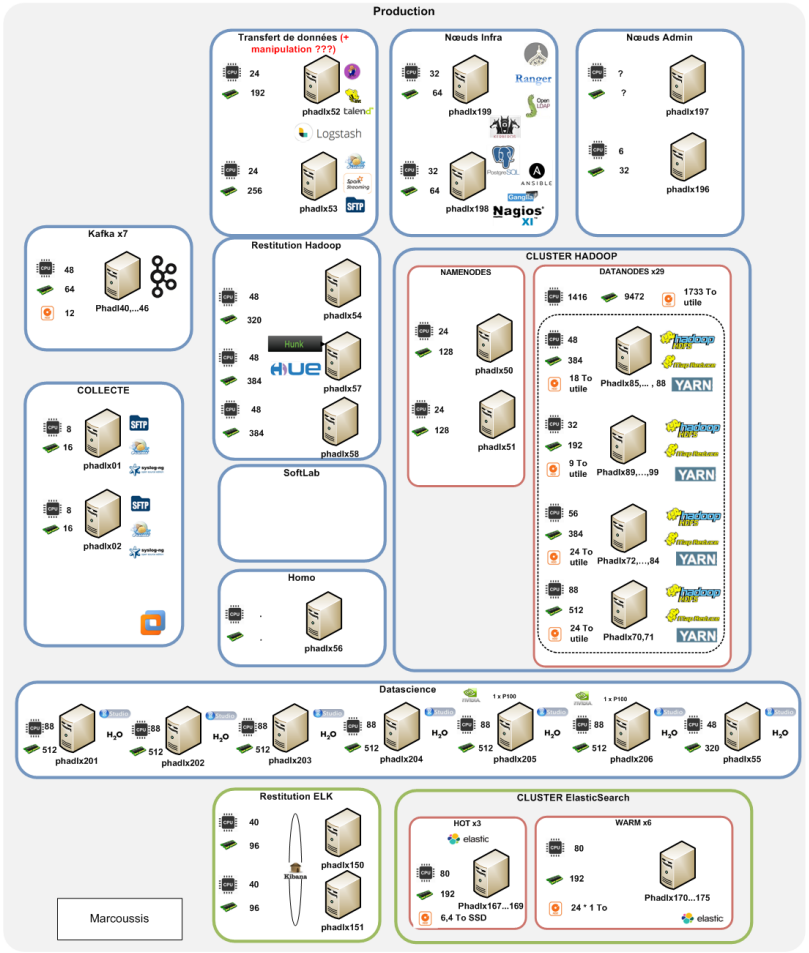
talend | DEVOPS | git | JIRA | Jenkins | Nexus

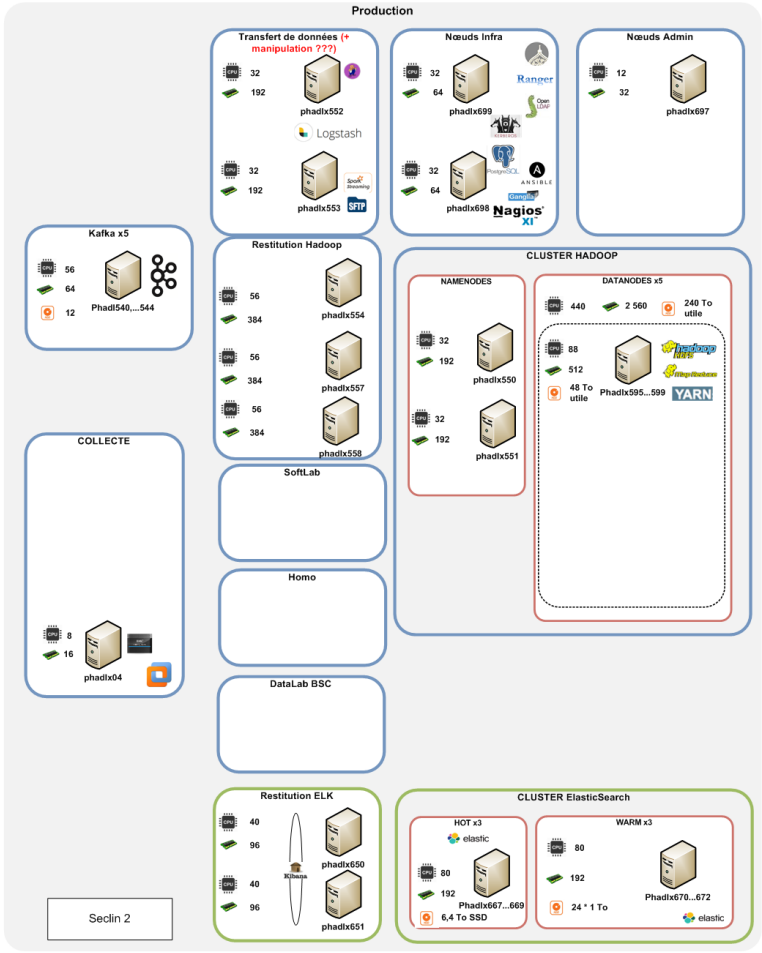
Le BIG DATA – L'intégration dans le SI au travers des travaux du CC.

Big Data
ITIM | GTS | BSC



Architecture physique





Sécurité – Préconisations et solutions mises en oeuvre

- **Mettre en place des outils de protection de la données de bout en bout**
  - Chiffrement global du transport des données sur toute l'infrastructure
  - Chiffrement des données stockées, sur le NAS GTS pour le serveur de collecte, et sur disque local chez HP avec transmission des clés depuis 2 appliances HSM situées chez GTS
- **Renforcer la traçabilité et les contrôles de tous les composants de la solution**
  - Traces d'audit activées sur l'ensemble de l'infrastructure (syslog et auditd) et archivage chez LogColCor. Traçabilité des actions d'exploitation GTS via l'outil ObservIT.
  - Supervision des logs via des rapports et alertes HUNK et bientôt Log4All
- **Renforcer la sécurité des serveurs exposés**
  - durcissement OS et détection des vulnérabilités par le SOC
- **Renforcer l'authentification et les habilitations**
  - Gestion des comptes utilisateurs depuis SAFE
  - Retrait des comptes à privilèges chez l'exploitant (dont root) au profit d'un catalogue de commandes prédéfinies
  - Solution automatisée d'export des bases de comptes (LDAP, SAFE) pour revue mensuelle des droits
  - Sécurisation des accès au cluster : ACL (Ldap, Ranger, Knox, Shield pour ELK) et Kerberos
- **Mettre en œuvre une démarche risque adaptée pour les nouveaux cas d'usage**
  - Audit Sécurité à chaque livraison d'un dispositif Sécurité

Principe d'alimentation en streaming

Le cluster Kafka est exclusivement réservé au transport des données (pas de calcul ni de parsing). N sources de données 1 seul port d'entrée.

2 flux de données brutes vont sortir de KAFKA. 1 flux est envoyé vers SPARK et 1 flux est traité par le parser puis renvoyé dans KAFKA puis vers SPARK.

Les flux de données brutes et parsés, sont respectivement envoyés en mode streaming vers HDFS et ES.

Les données brutes sont stockées et conservées dans **HDFS** dans un espace réservé (/lake) par entité bancaires et directions métiers. Les données brutes sont rangées par date yyyymmdd. Les données modifiées depuis /lake sont déposées dans **/project**.

Parser = prendre la données brute et la découper en plusieurs champs

DATALAKE

ORDONNANCEMENT

Les calculs d'agrégats sont ordonnancés par Oozie.

3 indexes globaux sont construits

agents de collecte

S_1

S_2

S_n

FRONTAL INJECTION

kafka

parser

Spark Streaming

HDFS

HIVE

elastic

FRONTAL RESTITUTION

parser

Hunk Splunk Analytics for Hadoop

Kibana

NoSQL

mongoDB

AngularJS

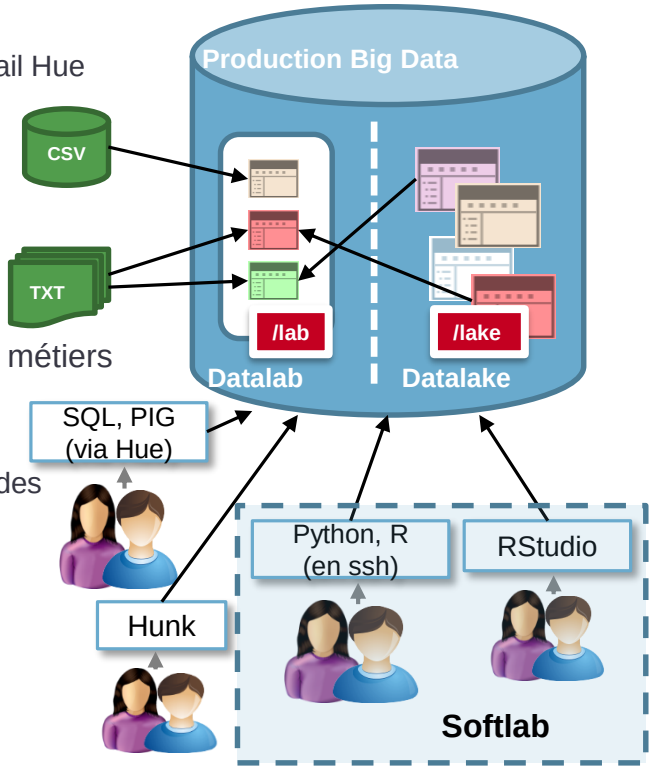
node

INDUS

Focus Datalab / Softlab

Datalab :

- **Objectif :** offrir un espace de travail en production pour des besoins d'étude, de découverte de données, de modélisation ou de prototypage
- **Principes :**
  - Espaces privatifs par direction métier (lecture / écriture, quota par direction)
  - Chargement et utilisation possible de données externes
  - Accès en lecture aux données du datalake
  - Avec les performances de la production mais non prioritaire par rapport aux traitements industriels et sans automatisation des traitements
  - Accès aux données :
    - en utilisant Hive SQL, langage PIG, navigateur de fichier depuis le portail Hue
    - en utilisant des outils d'analyse (Hunk)
    - en utilisant des outils du Softlab
- **Mise à disposition des datalabs :**
  - création des datalabs effectuée pour les équipes BSC, BDDF, CDN et SRO



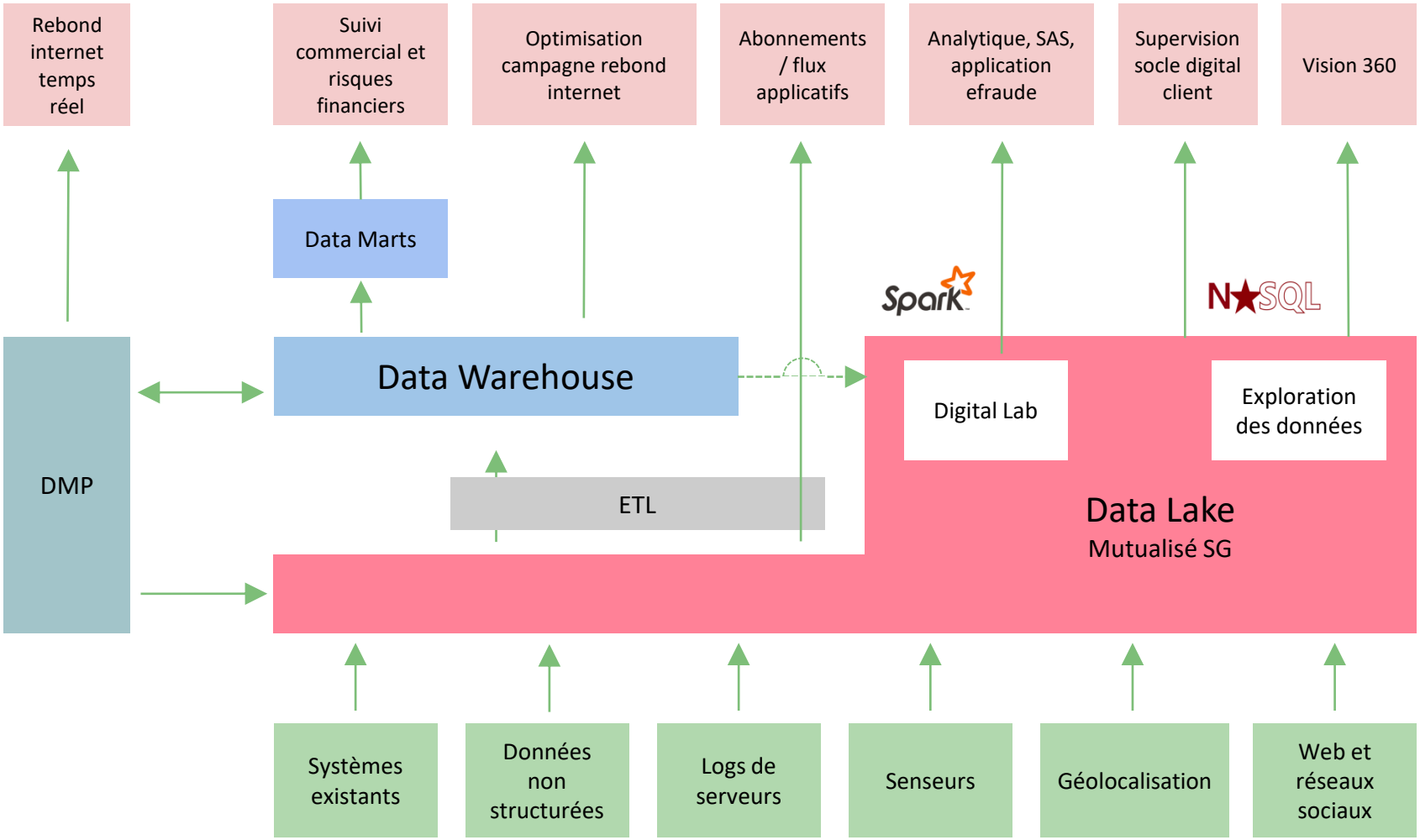
Softlab :

- **Objectif :** proposer un dispositif en production permettant de mettre à disposition des métiers des outils dans le but de les tester ou de les utiliser dans un mode non industriel

- **Principes :**
- Choix des outils par le métier avec une évaluation du CC Big Data (licence, sécurité, gestion des ressources). Le métier se charge de la relation avec le fournisseur.
- Installation des outils par le CC Big Data mais pas de support applicatif
- Traitements lancés par le Softlab moins prioritaires que les traitements industriels
- Réinstallation possible des outils du Softlab sur un serveur industriel au besoin

- **Mise à disposition du Softlab :**
  - mise à disposition en production du serveur avec installation des outils :
    - Python 3.4 et ses différentes librairies
    - R 3.2.2, ses différents librairies ainsi que l'interface web Rstudio Server
    - configuration pour permettre les accès en ligne de commande (ssh)

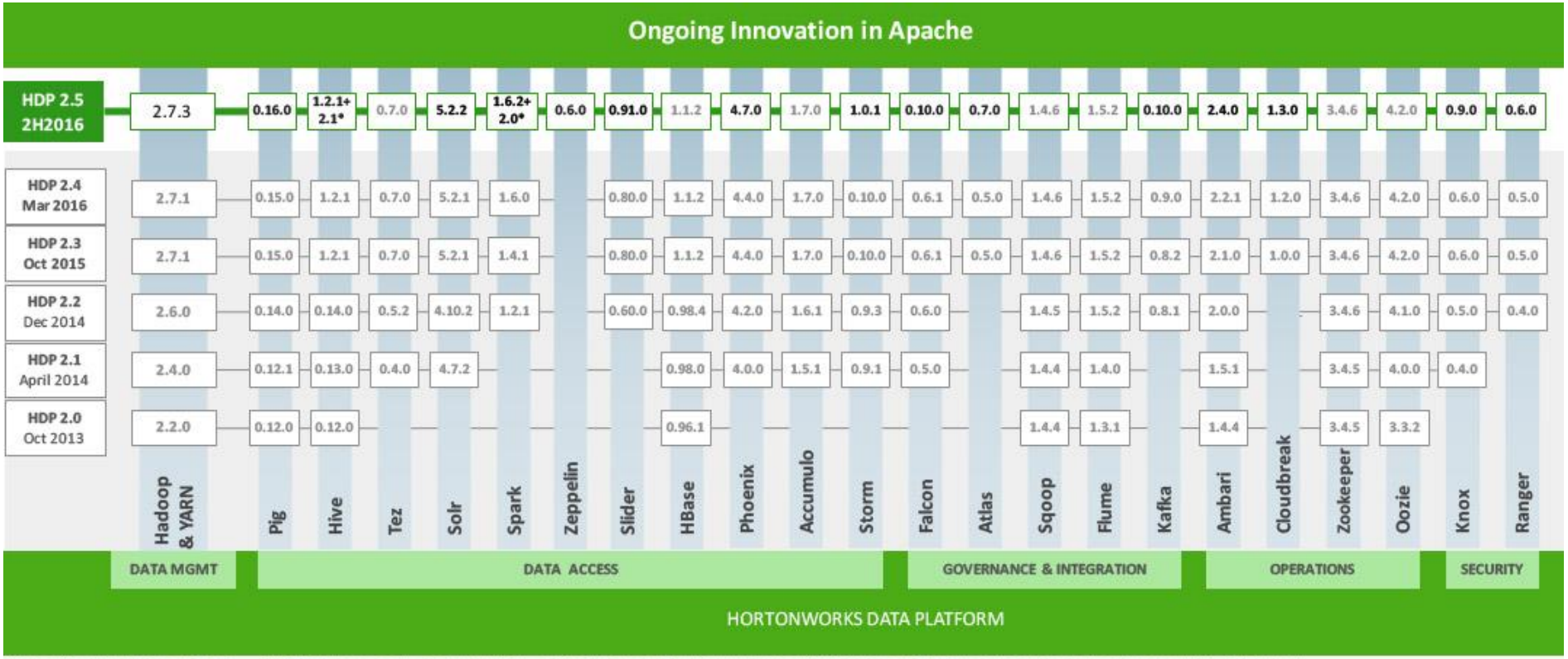
Architecture de référence détaillée – Schéma général



Annexe 1 : Choix des outils d'ingestion/diffusion

				Produits						
Thèmes	Sous thèmes	Avantage	Use cases	talend	IBM DataStage	Spark	kafka	Flume	logstash	nifi
Ingestion Traitement Batch	ELT (Extract Load Transform)	• Scalabilité • Traçabilité • Gain en maintenance	Tous types de use cases	✓						
	Spécifique s'éxécutant sur l'ensemble du cluster	• Scalabilité • Optimisé pour le use case	Pour des besoins particuliers nécessitant des optimisations			✓				
	ETL	• Traçabilité • Gain en maintenance	Pas recommandé		?					
Ingestion Traitement fil de l'eau	Collecte et ingestion	• Résilience • Scalabilité	Socle digital (IED)			✓	✓		✓	?
	Ingestion	• Scalabilité	Hélios (HLS)					✓	✓	
Complex Event Processing	Calcul événementiel	• Résultat de calcul au plus près du temps réel	eFraude (EFR)			✓				

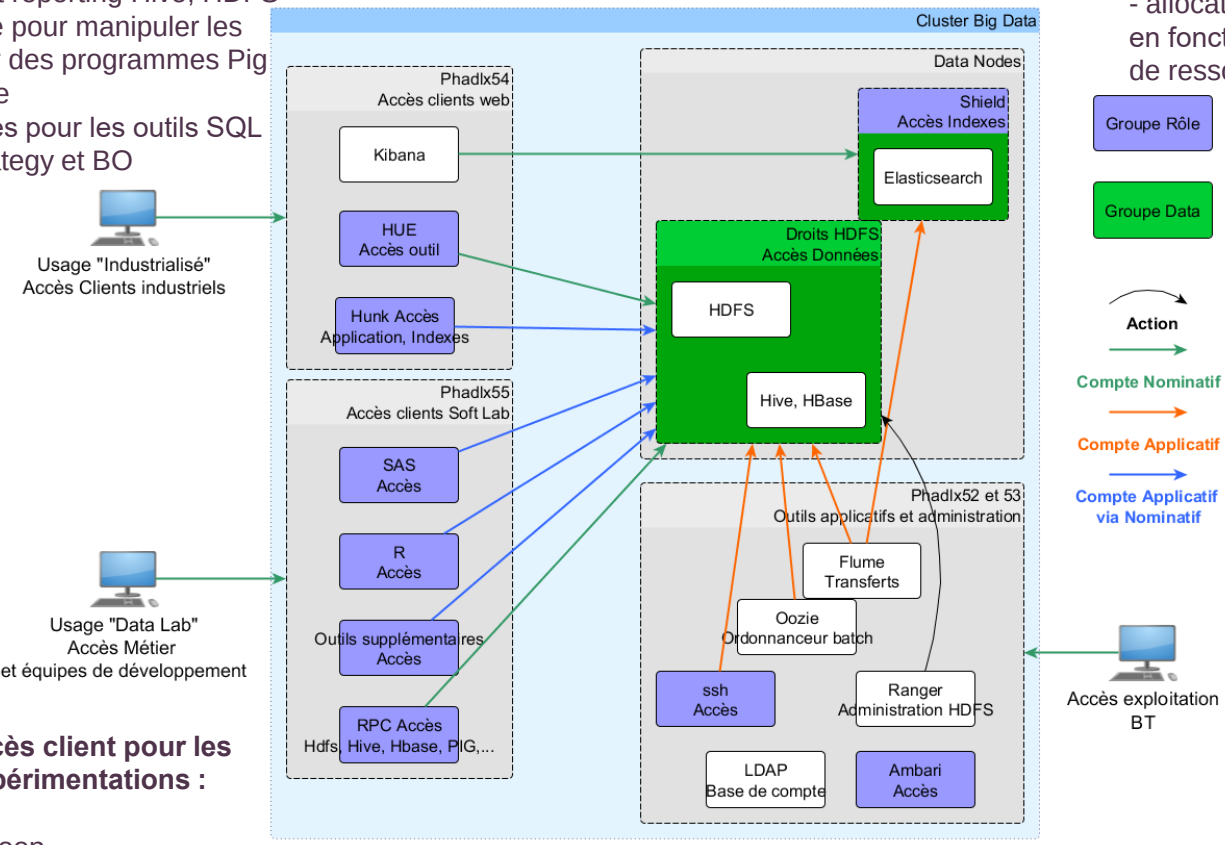
Annexe 2 : Distribution Hortonworks



** Spark 1.6.2+ Spark 2.0 – HDP 2.5 support installation of both Spark 1.6.2 and Spark 2.0. Spark 2.0 is Technical Preview within HDP 2.5.*
Hive 1.2.1+ Hive 2.1 – Hive 2.1 is Technical Preview within HDP 2.5.

Annexe 3 : Principe de l'architecture technique

Serveur d'accès client pour les accès typés industriels :
- interface Kibana pour ElasticSearch
- interface Hunk pour exploration, visualisation et reporting Hive, HDFS
- interface Hue pour manipuler les fichiers, lancer des programmes Pig et du SQL Hive
- frontal d'accès pour les outils SQL type MicroStrategy et BO



Serveur d'accès client pour les besoins d'expérimentations :
- accès SAS
- accès R Hadoop
- outils complémentaires à tester
- accès unix client (non disponible pour l'instant)

DataNode :
- serveur de traitement et de stockage
- comprenant des espaces Data Lab et industrialisé
- allocation de ressources dynamiques en fonction d'un profil de consommation de ressources (queue YARN)

Groupe Rôle

Groupe Data

- sécurité d'accès aux données géré par des groupes
- données organisées par enseigne/direction pour le Data Lab et par SI/application source pour l'espace industriel

Action

Compte Nominatif

Compte Applicatif

Compte Applicatif via Nominatif

Serveurs d'accès pour les besoins d'administrations et pour l'automatisation des traitements :
- interface d'administration du cluster : Ambari
- outillage de planification et d'automatisation
- serveurs en haute disponibilité pour assurer les alimentations industrielles en cas de problème ainsi que l'administration

Annexe 4 : CoPil d'architecture Big Data
Executive Summary

• Notre situation actuelle

- Nous disposons d'un Data Lake et de DataWarehouse indépendants
- Nous souhaitons intégrer le Data Lake dans l'architecture du SID (Système d'Information Décisionnel) afin de promouvoir les usages exploratoires
- Nous avons étudié la façon d'intégrer le Data Lake et nous avons réfléchi aux principes de construction et aux impacts de l'architecture de référence

• Les principes de notre architecture de référence

- **Agilité** : Privilégier les usages exploratoires grâce à la flexibilité permise par le Data Lake
- **Ouverture de la donnée** : Mise à disposition rapide de la donnée au niveau le plus granulaire possible
- **Utilisation pragmatique** : Choix des solutions les plus adaptées à chaque usage
- **Rationalisation et simplification des SI** : Centralisation progressive de la donnée dans le Data Lake et simplification de l'utilisation des infrastructures pour l'utilisateur final
- **Anticipation** : Préparation aux usages futurs et amélioration du time-to-market
- **Pérennité** : Mise en place de règles d'utilisation afin de maintenir l'ordre sur le Data Lake et de garder la maîtrise des données

• Impacts de l'intégration du Data Lake

• Conclusions

- Le Data Lake peut servir de solution de stockage à bas coût grâce à l'hybridation des types de stockage permise par Hortonworks
- L'usage du Data Lake est sécurisé, et sa résilience est en cours d'amélioration
- De nombreuses actions visant la mise en place de règles de gouvernance de la donnée sont en cours

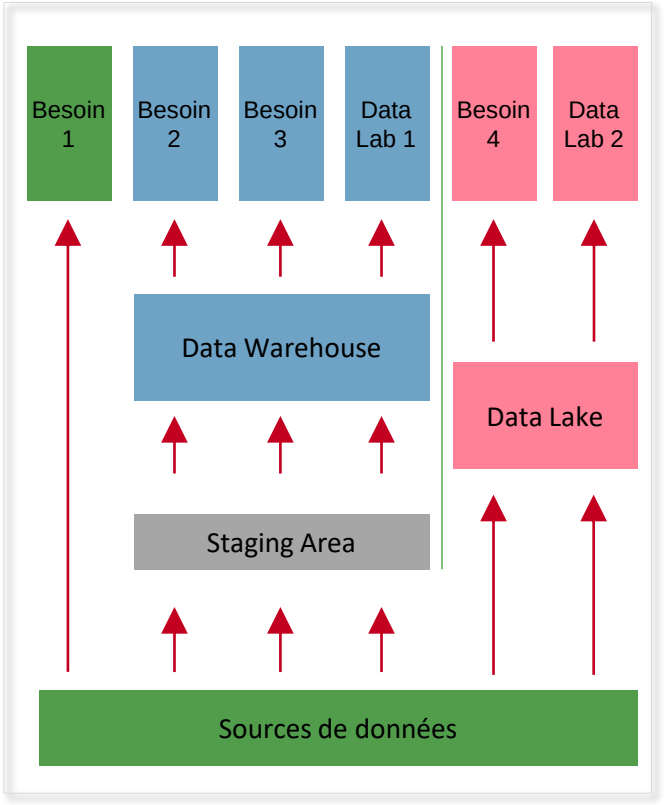
• Orientations à valider

- Validons nous le fait de baser notre **système d'alimentation au fil de l'eau** sur les **capacités Big Data** ?
- Devons-nous **restreindre la quantité d'outils** qui seront utilisés en sortie du Data Lake, notamment au niveau des **usages exploratoires** ?
- Partageons-nous l'idée de mettre en place des **grilles d'outils recommandés** pour chaque usage sur la base d'études internes ?
- Devons-nous mettre en place des **outils de gouvernance / Data lineage** de la donnée ?
- Validons-nous le fait de **rapatrier les flux de données existants** vers le Data Lake de **façon progressive**, au fur et à mesure de la **présence avérée de use cases** ?

Annexe 4 : CoPil d'architecture Big Data

Nous avons alors repensé l'architecture afin de profiter des avantages du Data Lake

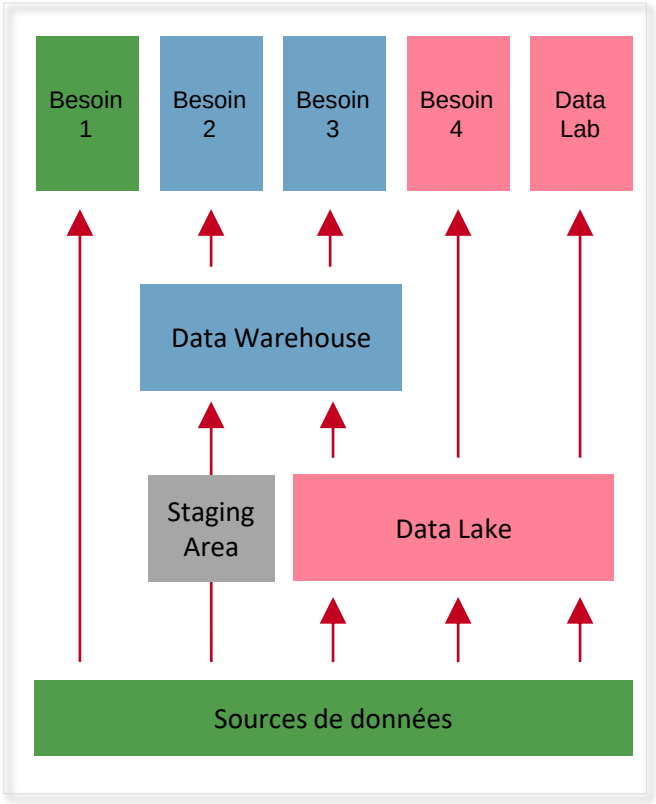
Architecture existante



Principales évolutions :

- ✓ Levée de la séparation en **silo**
- ✓ **Intégration cohérente** du Data Lake plus qu'une fusion
- ✓ Utilisation du Data Lake pour le **Data Staging**
- ✓ Concentration des **usages exploratoire** sur le Data Lake
- ✓ Construction d'un système d'**alimentation au fil de l'eau**
- ✓ Mise en place de processus de **gestion de la donnée**

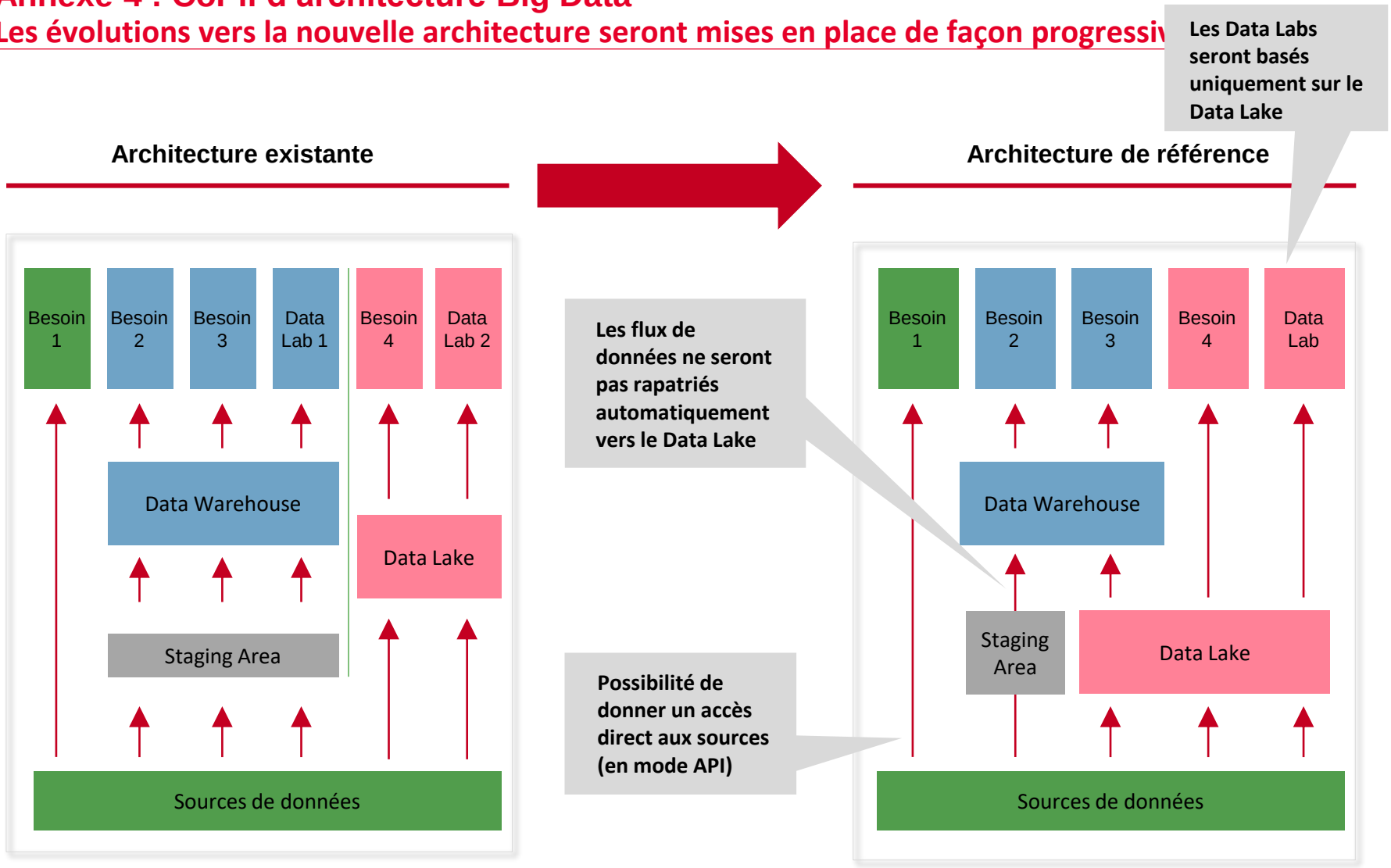
Architecture de référence *



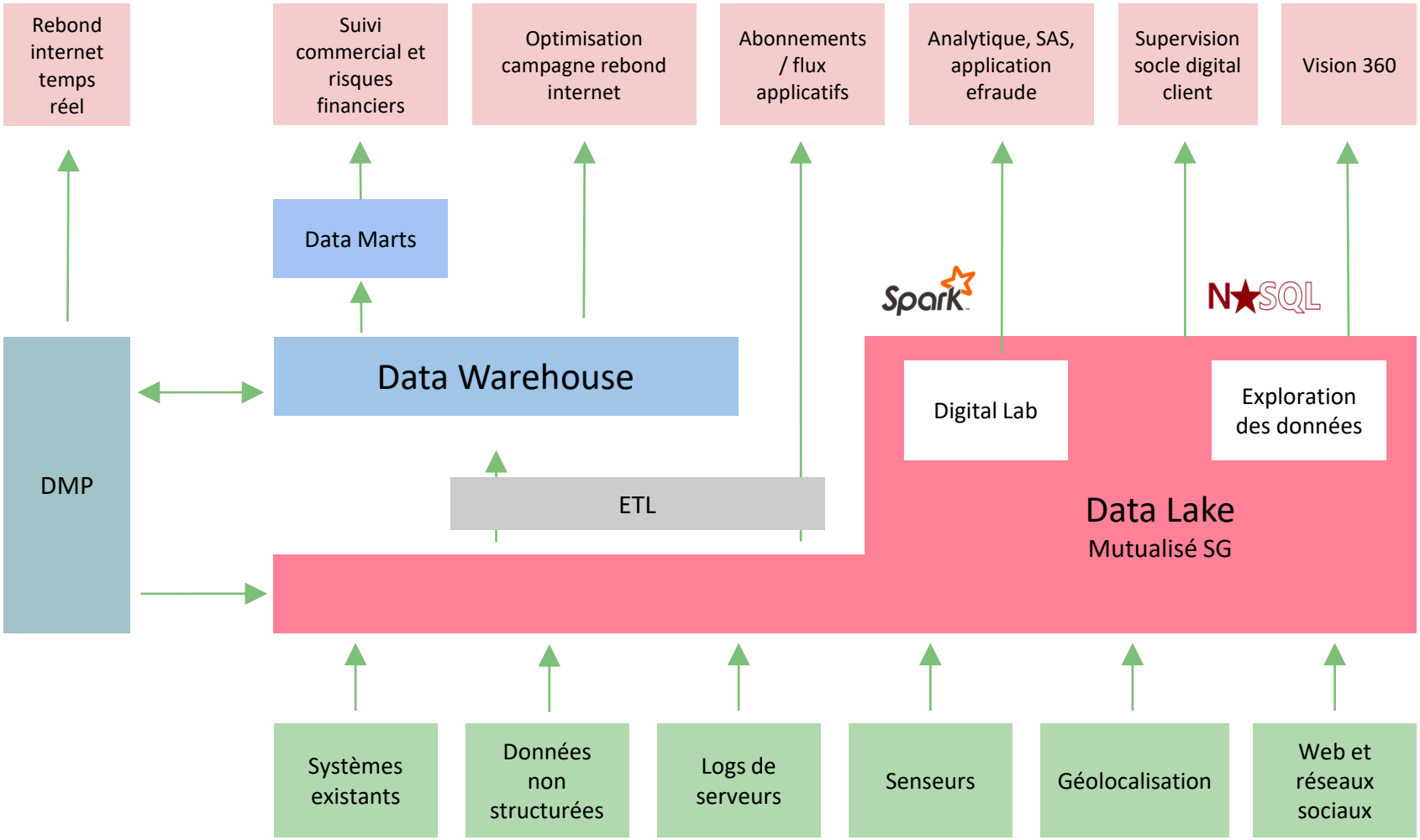
* Le schéma général d'architecture de référence et son instanciation pour BDDF et CDN se trouvent en annexe.

Annexe 4 : CoPil d'architecture Big Data

Les évolutions vers la nouvelle architecture seront mises en place de façon progressiv



Annexe 4 : CoPil d'architecture Big Data
Architecture de référence détaillée – Schéma général



Annexe 5 : CoPil d'architecture Avenir 3D
Executive Summary Etude « Avenir 3D »

- Ce comité a pour objectif de présenter pour validation les conclusions et les préconisations de l'étude d'architecture sur l'avenir du distributeur de données 3D, réalisée en collaboration avec le BSC .

- En synthèse :
  - S'appuyer sur 3D est **viable à court terme**, mais les **risques à moyen terme** sont à considérer :
    - 3D n'a pas la possibilité d'évoluer pour contribuer à la transformation de notre SI (mise à disposition des données pour des usages fil de l'eau / temps réel, mode service, time-to-market, continuous delivery, …)
    - La technologie sous-jacente à 3D (ETI-Extract) est en obsolescence structurante
  - Devant ce constat, **3 options sont envisageables** :
    1. Ne rien faire
    2. Lancer un projet de migration de 3D en 2017
    3. Mettre sous contrôle l'usage de 3D, limiter son usage et poser les premières briques de la solution alternative à 3D
  - L'étude menée en Q2 2016 a abouti à **préconiser l'option 3**, qui se traduit par
    - Une étude de faisabilité à lancer sur la/les solution(s) d'échanges (adossée à l'écosystème Big Data) qui se substituerait à 3D
    - La mise en place des KPI permettant de suivre l'évolution de 3D au sein d'ITIM
    - Des règles d'encadrement de l'usage de 3D à mettre en place

Annexe 5 : CoPil d'architecture Avenir 3D

Architecture d'échange de données : cible