ITG\_DEPARTEMENT

**« INOPS »**

Nom Prénom

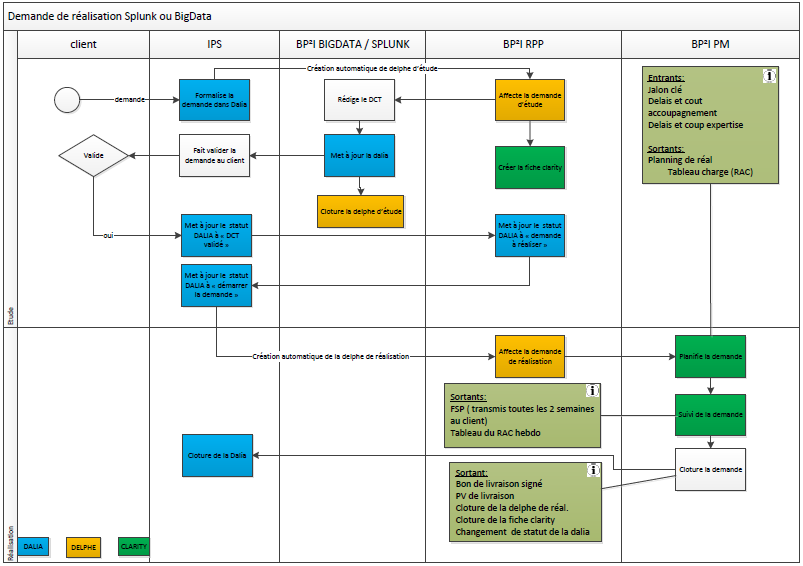
Lieu Date

# Information Projet

|  |  |
| --- | --- |
| **Nom du projet** | INOPS |
| **Code AP** |  |
| **Code PJ** | PJ55441 |
| **Métier bénéficiaire (\*)** | IRB |
| **PARDCG** |  |
| **Nom du CP MOE** | Pierre Le Guen |
| **Nom du BPM Métier** |  |
| **Validation Sponsor** | Fayçal Grigra |

# Rappel du service

## WorkFlow d’un projet standard



### Exemple de déroulement d’un projet

* Prise de contact avec IPS ou BP2i (**PARIS ITPS GLOBAL SPLUNK** ou **PARIS BP2I SPLUNK**)
* Réunion de cadrage (Présentation du besoin)
* Renseignement du template d’expression de besoin
* Action technique BP2i (Paramétrage de la collecte)
* Atelier technique IPS/BP2i/Métier (Validation de la structure des données « SourceType », exhaustivité des données collectées)
* Ateliers techniques IPS (Création des dashboard) / Expertise (Optimisation de tableaux de bord existant)

### Exemple de déroulement d’une évolution

* Demande Delphe auprès de BP2i pour ajout de collecte
* Demande IDelphe auprès d’IPS pour la réalisation du tableau de bord

## Solution envisagée

### Description de la Solution

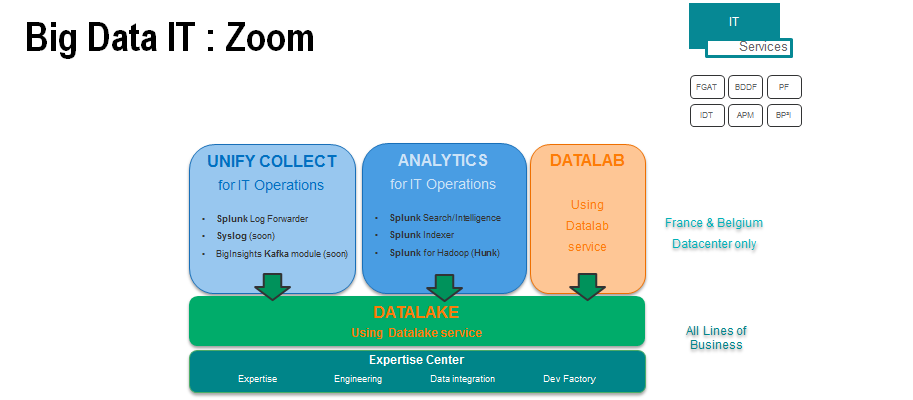
A la lecture de la demande ainsi que suite aux échanges avec les équipes en charge du projet, le centre d’expertise Splunk IPS IDT 11 & l’équipe BP2i TP36 Big Data Services propose un alignement sur leurs offres ITOA (Splunk). Cette offre inclus la mise à disposition d’un espace de travail sur la plateforme mutualisée Splunk, d’un mécanisme de collecte et d’analyse des données ainsi que la possibilité de créer et d’être accompagné dans la création des tableaux de bords construits sur les données collectées.

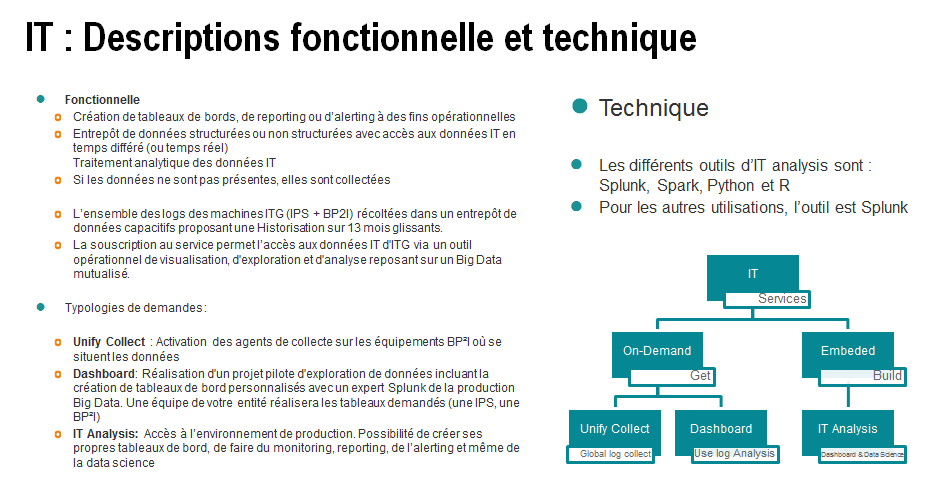
Responsabilités des équipes :

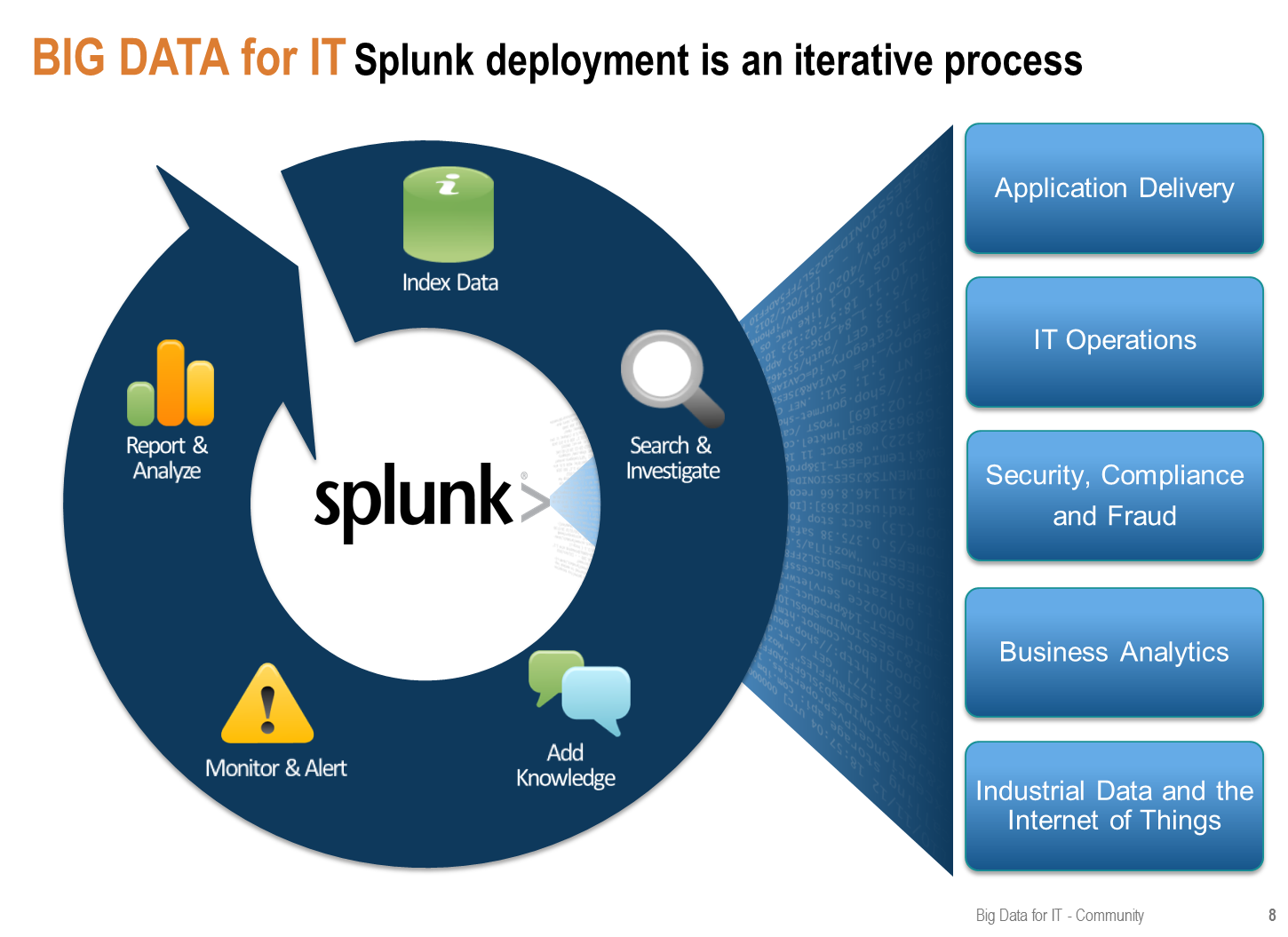
Le centre d’expertise Splunk IPS IDT 11 :> Développement de tableaux de bords et accompagnement des projets IPS

L’équipe BP2i TP36 Big Data Services :> Maintien en condition opérationnel de la plate-forme Splunk mutualisée et mise en place de la collecte des données ainsi que des tâches d’administration

Description de la Solution ci-dessous (encadré rouge) :

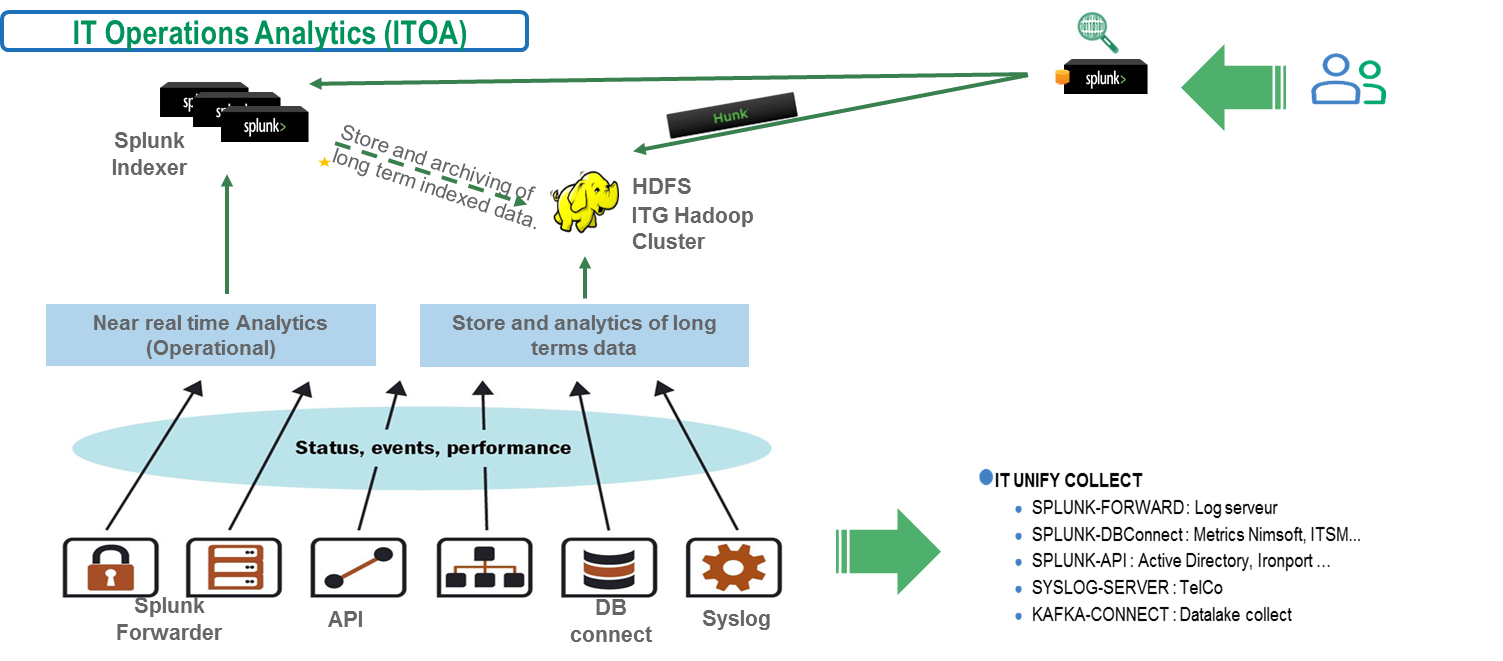






### Présentation des environnements

* Utilisation de l’environnement qualification ou de production mutualisée pour définir que la collecte des logs est effective ainsi que de structurer l’information afin de pouvoir alimenter des tableaux de bords.
* Automatisation de la remontée d’information
  + Pour information : Un chantier de déploiement sur les machines opéré par BP2I est en cours avec une cible de couverture du périmètre France, Fortis, BNL pour fin d’année 2017
  + On parle ici de la collecte unifiée, dans des cas spécifiques nous utiliserons également une collecte différente basé sur l’installation d’agent de collecte splunk « lourd » Heavy forwarder ceci afin d’être capable de capter les flux réseaux ou d’appliquer des filtres sur les données collectées.
  + Certains équipements réseaux nécessitent également une configuration de collecte via Syslog.



### Description du livrable

Livraison d’un environnement utilisateur sur plateforme de qualification et de production mutualisée.

Mécanisme de collecte industriel sur le périmètre identifié en réunion : liste indiquée dans l’onglet « Arbo Applicative ».

Fonction d’export via l’interface (automatisable) au format csv. (si besoin fonction native de l’outil Splunk)

Accès – environnement de Production & Qualification

* Jusqu’à 30 utilisateurs nominatifs sur l’environnement qualification et de production.
* Création de deux types de rôle pour l’application dans Splunk : Power & user

### Investissement Matériel & logiciel

Les projets splunk (en 2017) seront hébergés sur l’environnement de production mutualisée Splunk groupe : les investissements matériel, et les charges récurrentes sont portés par l’infrastructure BIG DATA / ITOA pour l’année 2017.

L’UO de refacturation de l’offre est encore en cours de définition et pourra donner une mise à jour de ce DCT pour les investissements logiciels (UO basée sur le volume en Go indexé par jour).

Si les volumétries constatés sont conséquente une DS (Demande de Service) devra être faite afin d’acquérir une License suffisante pour absorber les pic haut de consommation de volumétrie journalière indexées dans la plateforme

### Charges JxH liées à la mise en œuvre de la solution

Un nouveau DCT devra être émis en cas d’évolutions majeurs (Qualification des évolutions à la charge des équipes IPS IDT 11 & BP2I TP36 BIG DATA Services.

## Engagements et Risques

### Responsabilité et Obligations Client

Les délais de livraison au sein du macro-planning (livré dans le DCT) sont basés sur une estimation. Ils ne sont donc pas garantis.

Le macro planning (livré dans le DCT) ne prend pas en compte les retards liés à des prérequis spécifique. Exemple :

* Ouverture spécifique de ports réseaux pour la collecte spécifique
* Problème lors du déploiement de la collecte : Accès aux équipements impossible, pas assez de place sur les serveurs, ….

Les utilisateurs pourront disposer d’accès utilisateurs avancé afin de pouvoir créer de nouveaux tableaux de bords (nominatif, rôle « power » ou « user ») et les éditer. Ils ne pourront cependant pas les publier dans l’application Splunk (passage en mode public) car ceci est une tâche d’administration aux mains des équipes BP2I BIG DATA/ITOA SPLUNK.

L’équipe TP36B Big Data Services est garante des performances de la plateforme mutualisée. Dans ce sens des ajustements de configuration peuvent être mise en place afin de garantir l’optimisation de l’utilisation de l’infrastructure.

Exemple : les aspects liés à la collecte sont de la responsabilité des équipes BP2I BIG DATA/ITOA SPLUNK.

**L’équipe IPS IDT11 est garante des performances des recherches et tableaux de bords Splunk sur la plateforme mutualisée. Dans ce sens des ajustements de développement peuvent être mise en place afin de garantir l’optimisation de l’utilisation de l’application.**

### Niveau de service - information

Pour le moment même si l'infra mutualisée (clusteur multi-site + infra cloud = redondance physique et logique) permettra d'assurer un service *serious*, le niveau de service actuel est ***low***, il passera en *moderate* courant 2017 et *serious* pas avant 2018.

Splunk ne disposera pas d'UOT avant fin 2018 = pas de facturation à l'usage, en attendant le coup de l'infra splunk est ventilé dans le coup global d'infra BP²I que chaque UPM paie

Seules les volumétries jugées « conséquentes » pourront amener à une refacturation en directe donnant lieu à une Demande de Service.

Les informations ci-dessus sont des informations susceptibles d’évoluer et ne sont pas engageantes mais informatives.

# Use Case N°1

## Description

*Affichage des anomalies sur les environnements critique de la PROD en faisant une corrélation entre les incidents et les événements système, log, BDD, URL*

### Décrire le Use Case

*A voir en fonction des possibilités*

### Sources de données

*A voir en fonction des possibilités*

### Calcul

*N/A*

### Délai d’interrogation

*Temps réel*

## Représentation du UseCase

*A travailler*

## Exemple de donnée

*Le demandeur doit fournir un exemple de source de donnée appliqué au cas usuel.*

# Charges BP2I

*Ajouter le tableau Excel des charges*

# Charges IPS

*Ajouter le tableau Excel des charges*