ITG

PLATFORM SERVICES

Datalake IT4IT Operational Analytics/ Splunk

ITG/ TP36B & PPM02

14/08/2018

BNP PARIBAS

The bank for a changing world

Sommaire

Contenu

Contenu du document

Ce document décrit le service IT Operational Analytics Splunk de type PaaS (Platform as-a-service) fournis par ITG.

Ce service est disponible pour les clients de BP2I.

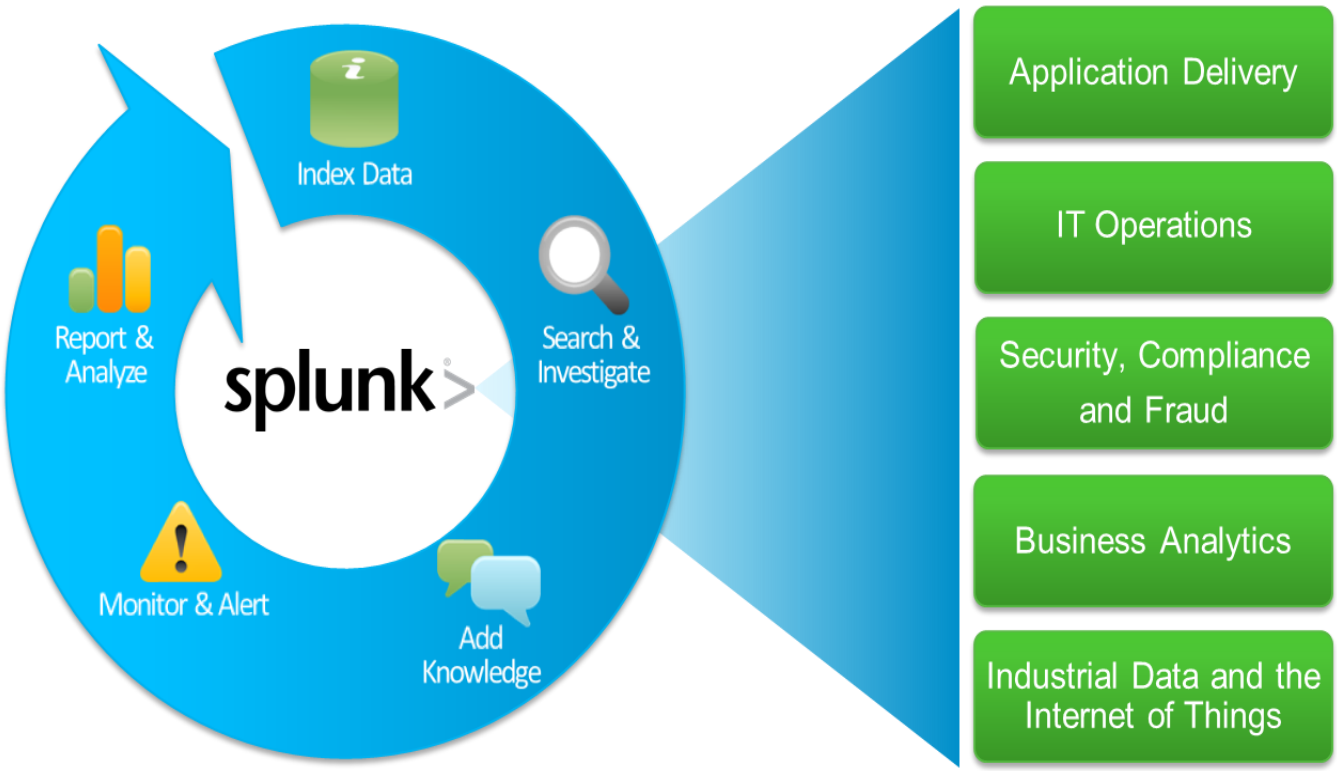
Objectif

Il n'est pas question de remplacer ou concurrencer le catalogue de service BP²I, ou ce qui est présent dans le Cloud.

A terme ce document devra être un 'mode d'emploi' des services qui seront accessibles par les moyens officiels de BP²I.

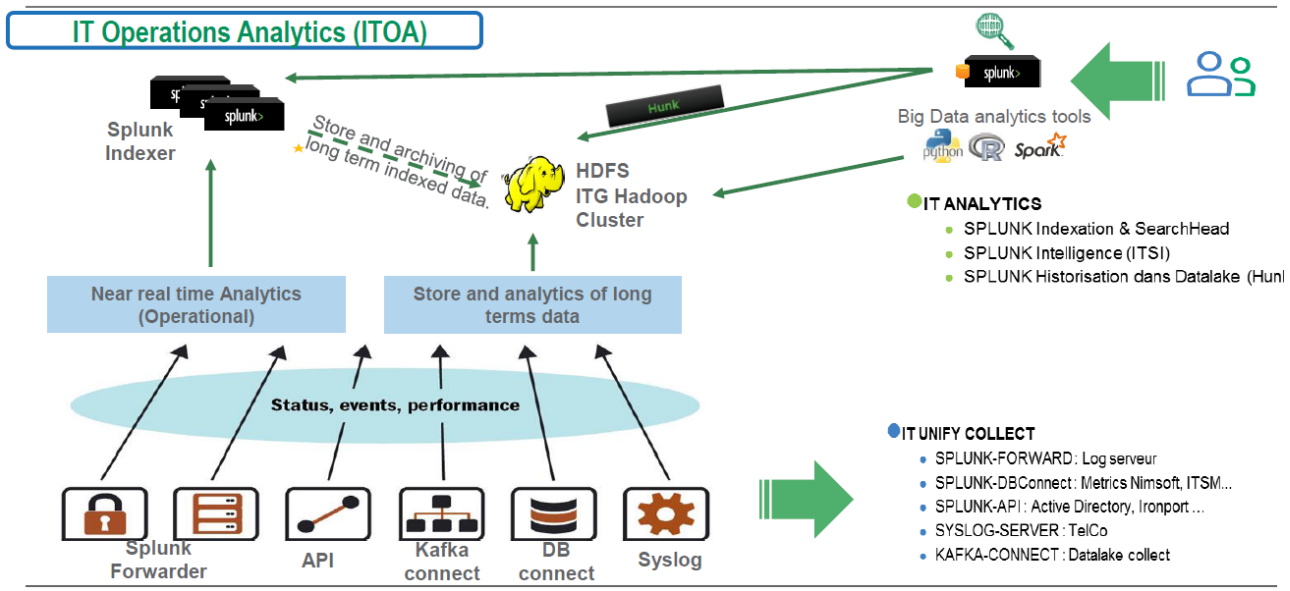
Synthèse service ITOA/Splunk

ITOA/ Splunk	Service d'aide à l'exploitation en mode Saas
Description	L'outil permet la centralisation des logs IT dans des indexes et sur un Datalake IT à des fins d'analyse post-production ou de maintenance préventive, alerting mail et supervision en temps réel.
Méthode de souscription	- une demande d'étude DCT puis une demande de réalisation à saisir dans l'outil Dalia - une Delphes pour BNL - IDelphes vers Splunk IPS pour toutes demandes de développements hors besoins BP2I
Conditions d'éligibilité au service	- Toutes les données IT (technico-applicatives non fonctionnelles/business) en provenance des assets opérées par BP2I lisibles par Splunk. - Toutes les données de sécurité ou confidentiel vers le Splunk IPS.
Statut	- L'infrastructure est Serious - L'ICP : Moderate et Serious fin 2018 - Les classes de service cf tableau Charges Run



Fonctions internes (incluses de base dans le service ou composant)		
Collecte unifiée des données de l'IT	Central Universal Forwarders : - Universal Forwarders - Db-Connect - API - Syslog server - JMX - HEC	Mars 2017
Indexation et enrichissement des données	Indexeurs	Mars 2017
Visualisation, exploration et analyse des données	SearchHead	Mars 2017
Réalisation des tableaux de reporting & alerting à des fins opérationnelles	SearchHead	Mars 2017
Historisation dans le Datalake 4IT sur 13 mois glissants	Hunk→Hadoop NAS	Mars 2017

Fonctions optionnelles (à activer lors de la demande de création/instanciation du service ou composant)		
Acquittement des logs collectés pour les besoins réglementaires	Via le port 9999	Septembre 2017



Eléments/options non fonctionnels		
Plage de support	Heures ouvrés (C3)	Mars 2017
Environnements possibles	• Training/LAb • Qualification • Pré-Production (en cours) • Production	Janvier 2018 Mars 2017 Mars 2017

Process de souscription :

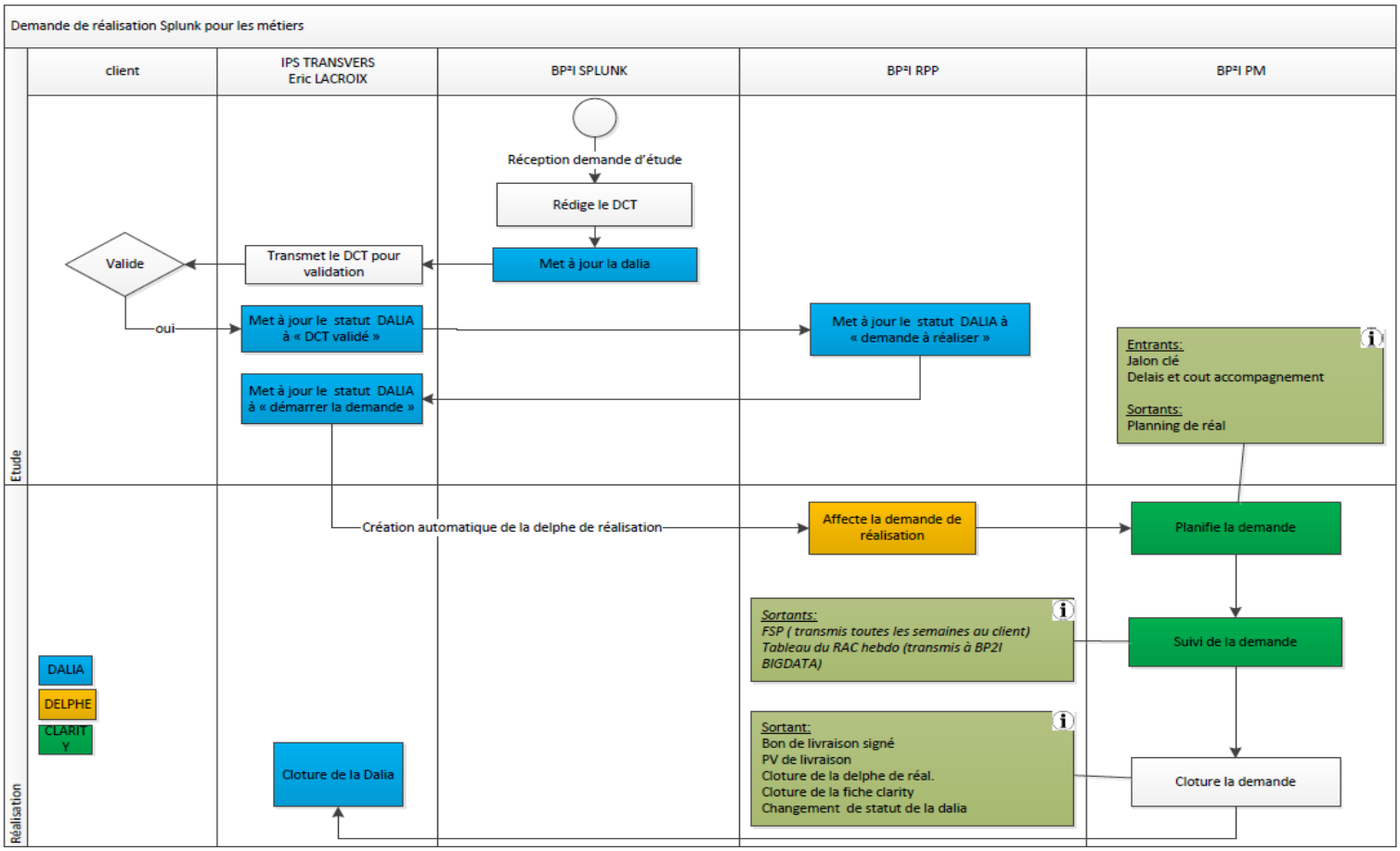
La souscription au service permet l'accès aux données IT d'ITG via un outil opérationnel de visualisation, d'exploration et d'analyse reposant sur un Big Data mutualisé.

- Fonctionnement :
  - ✓ Description du besoin
  - ✓ identification des sources de données et droits associés*
  - ✓ identification des users
  - ✓ chargement manuelles des données : jeux de données fournis
  - ✓ Déploiement des agents de la collecte unifiée
  - ✓ Développement des dashboards
  - ✓ Automatisation de la collecte (activation le mécanisme de collecte sur des machines spécifiques afin d'en remonter les données dans Splunk): validation des hypothèses de volumétrie journalière indexée

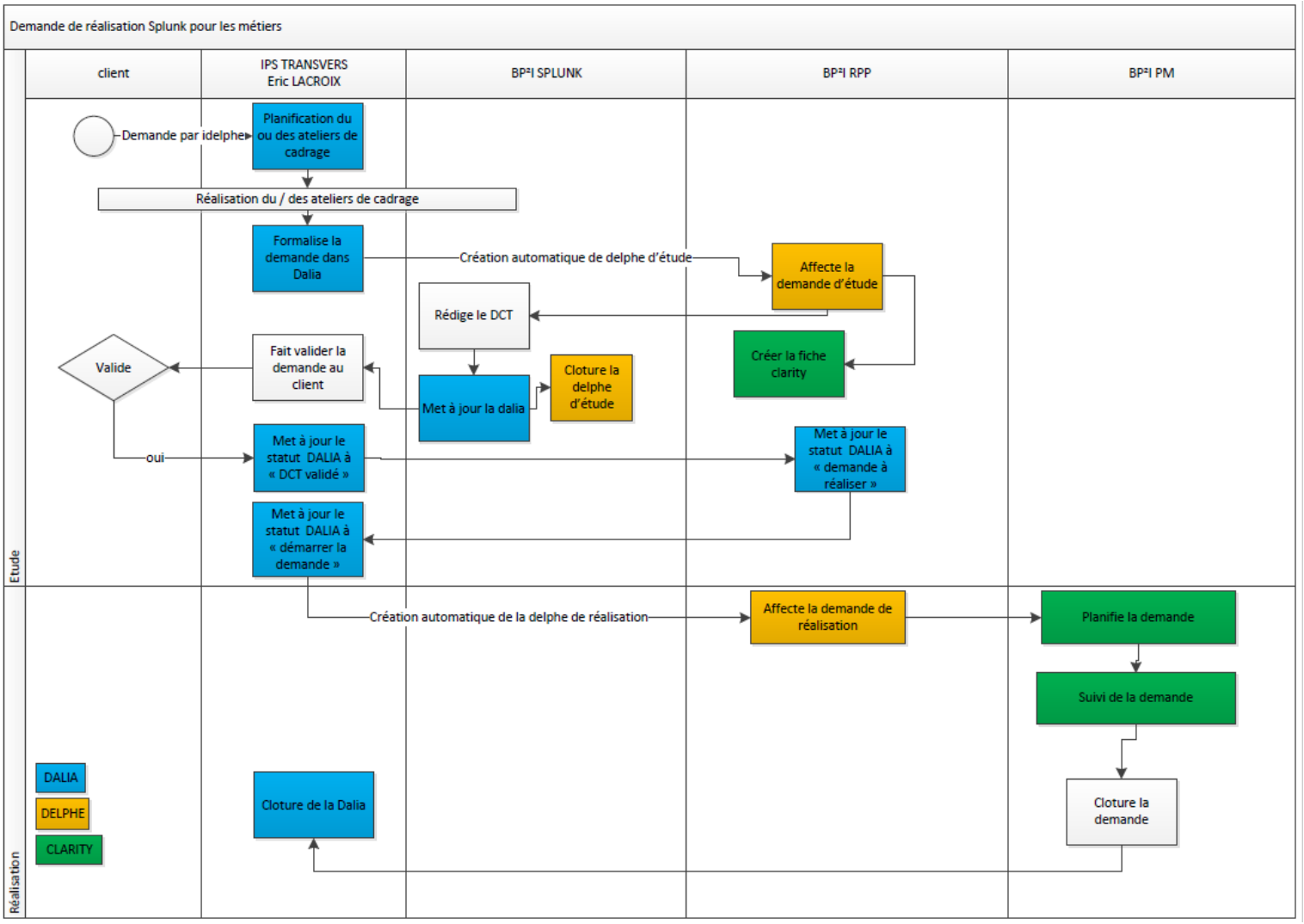
* l'utilisateur doit vérifier la compatibilité de lecture avec Splunk

Workflow d'une demande projet standard

- Demande d'étude Splunk pour les métiers



- Demande de réalisation Splunk pour les métiers



Tarif propal :

Charges Projet

Prestation	Service	Estimation charge BP2I TP36B
Expertise & support d'administration ITOA	Standard	1
Déploiement manuel + automatique	Standard	0,5
Accompagnement lors d'ateliers techniques (collecte spécifique, paramètrage, ...)	Standard	0,5
Etude DCT pour la solution et participation aux réunions de suivi	Standard	0,5
Industrialisation de la collecte	Standard	0,5
Coordination Projet – commande et suivi	Standard	0,5
Contribution phase d'étude, participation aux réunions/ateliers techniques	Standard	0,5
Création d'espace de travail Splunk	Standard	0,5
Création utilisateurs / Gestion des rôles et profils	Standard	0,5
Suivi des performances utilisateurs et ajustement si nécessaire	Spécifique	0,5
ADMINISTRATION : installation et configuration des tableaux de bords sur environnement de production	Spécifique	0,5
Qualification de l'environnement avant livraison	Standard	0,5
Publication des tableaux de bords et mise en place d'alertes	Spécifique	0,5
Evolutions mineurs sur l'année	Spécifique	-
Estimation du Macrochiffrage JH / Projet		7

- <10 serv <20 users --> 5jh
- >50 serv --> +5jh
- >20 users --> +2jh
- DB Connect --> +5j
- Rsyslog --> +5jh par plateforme syslog.

Sources spécifiques --> +2jh par typologie de source

Macro-planning prévisionnel

Description	Date
Accord du client et réception par l'équipe TP36B de la Delphes de réalisation avec fiche de 'GO'	T0
mise en place de la collecte	T0 + 2 semaines = T1
livraison d'un environnement sur plateforme de production avec remontée des données	T1 + 2 semaines = T2
Bascule des tableaux de bords sur env de production et suivi des développements IPS	T2 + 4 semaines
Fin projet estimé	T0 + 8 semaines

Macro-planning réalisation

Activités	Détail	Delai Max (JO)
Mise en place d'une collecte	Configuration agents (agents déjà installés)	5
	Configuration agents (agents non installés)	20
	Mise en place collecte Syslog (1 syslog)	20
	Mise en place collecte DB-Connect (1 DB connect)	20
	Configuration de collecte	10
	Creation idx + apps	
	Creation users	10
Dashboard pour BP2I	Creation de dashboard	A estimer en fonction de la charge

Charges Run

Numéro	Type de collecte	Criticité	SLA	Astreintes	Garantie de perte des données	Run
Service 1	AGENTS	1	P2	Oui	Oui (Ack)	200 jours de RUN par an(1ETP) pour 500 agents par client
Service 2	AGENTS	2	P3	Non	99%	200 jours de RUN par an(1ETP) pour 10 000 agents par client
Service 3	Syslog	3	P5	Non	Non	20 jours de RUN par an et par config Syslog
Service 4	Db-connect	3	P5	Non	Non	20 jours de RUN par an et par config Syslog
Service 5	Spécifique	3	P5	Non	Non	à déterminer

Investissement Matériel & logiciel

Volumétrie Licences

Revue mensuelle sur consommation constatée entre PPM02 et BP2I

Les activités des équipes Splunk PPM02 & BP2I

L'activité de PPM02 :

- ✓ Gestion des demandes IPS ou métiers passant par l'UPM
- ✓ Coordination avec BP2i sur les aspects source de données, sécurités
- ✓ Réalisation des applications
- ✓ Support aux utilisateurs IPS/Métiers,
- ✓ Validation des dashboards pour le passage en production
- ✓ Gestion et exploitation de l'infrastructure Splunk IPS

L'activité de BP2i :

- ✓ Gestion de l'infrastructure
- ✓ Gestion de l'exploitation
- ✓ Gestion des demandes BP2i
- ✓ Réalisation des tableaux de Bord pour BP2i
- ✓ Transfert de compétence aux utilisateurs BP2i

Responsabilités des équipes :

- Le centre d'expertise Splunk IPS PPM02 :
  →Développement des tableaux de bords et accompagnement des projets IPS
  → Maintien en condition opérationnel de la plate-forme Splunk IPS
- L'équipe BP2I TP26 Big Data Services :
  → Maintien en condition opérationnel de la plate-forme Splunk BP2I
  → Mise en place de la collecte des données ainsi que les taches d'administration.

Typologie des demandes :

Type de demande	Actions	Canal	Acteur	Client
Déploiement d'agent Splunk	Ajout/Modification/Suppression	- Demande Dalia - Idelphe pour les projets Hors scope	BP2I	BP2I/ITG/Fortis/BNL/ITRMG
Mise en place de la collecte des logs	Ajout/Modification/Suppression	- Demande Dalia - Idelphe pour l'infra secu PPM02	BP2I	BP2I/ITG/Fortis/BNL/ITRMG
Indexation		-Demande Dalia -Idelphes PPM02	BP2I	BP2I/ITG/Fortis
Gestion des utilisateurs	Ajout/Modification/Suppression	- Demande Dalia - Idelphe PPM02 - My Access en cible	BP2I	BP2I/ITG/Fortis
Réalisation des Dashboard	Ajout/Modification/Suppression	-Demande Dalia - Idelphes PPM02	BP2I	BP2I
Réalisation des Dashboard	Ajout/Modification/Suppression	-Demande Dalia - Idelphes PPM02	UPSI	ITG

Typologie des données collectées

Usages	Détail	Clients	Collecte	Comment	Indexation	Visualisation
Application Delivery	Collecte des logs technico-applicatives Collecte des métriques serveurs Vue temps réel de la qualité de service Analyse « deep dive » de log Corrélation et alerting mail	**BDDF** : Mabanque, DM 2020, Vioto, SDO, Spirit, API Mgt **PF :** SPEED **BP2S** : Mercury, Calypso, Vegas **CIB** : Atlas **FGAT** : RefSG, Easst, Klimt **UPSI** : SIBR, MoveDC, INS, BBR **IRB :** Sauron	BP²I	Agents DbConnect	BP²I	IPS
IT Operation	Collecte des logs HW/MW Collecte des métriques serveurs Vue temps réel de la qualité de service Analyse « deep dive » de log Corrélation et alerting mail	**Network** : WeatherMap, Rivage, Spectrum **Produits** : Monit E2E CFT, MQ, HADOOP, Autosys, Netcool, Was, Citrix => **Programme Qualité de la production**	BP²I	Agents (18 000) Syslog DBconnect « SNMP »	BP²I	BP²I
Security, Compliance	Collecte des logs d'accès aux équipements (serveurs, réseaux, infra HW…)	**BP²I Sécurité** ITRMG CSP (Swift) LPM	BP²I	Agents Syslog	BP²I	BP²I
	Collecte de logs infra de sécurité (FW, DNS, IronPort, AD, Poxy…)	**IPS – STG**	BP²I/ IPS	Agents Syslog	IPS	IPS

Informations complémentaires

Typologies de collecte:

Standard :

Universal forwarders : est un agent Splunk installé sur les serveurs cibles en zone intranet et internet qui permet de collecter les logs en temps réel

Spécifique :

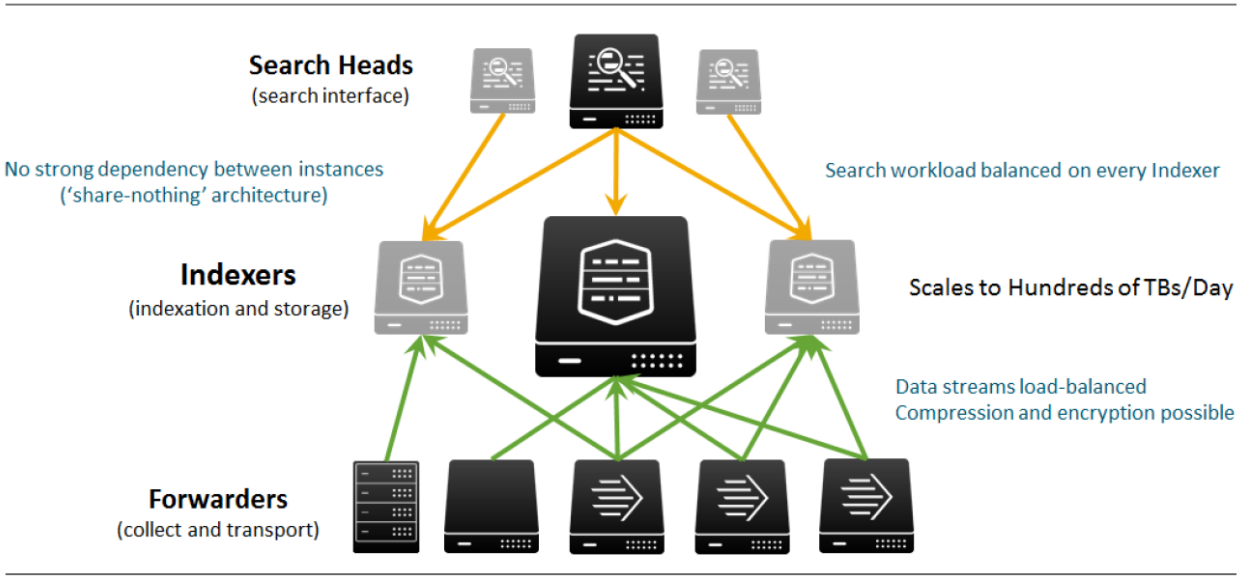
Heavy forwarder : c'est un agent Splunk « lourd » qui capte les flux réseaux ou d'appliquer des filtres sur les données collectées et d'envoyer un ACK pour les logs soumis par exemple à la LPM

API Web : pour la collecte des données CA PM

Db connect : add-on permet de réaliser une collecte planifiée des logs SGBD (Oracle, MSSQL, DB2)
JMX : add-on de collecte des logs KAFKA

Syslog : permet de collecter les logs en temps réel en mode TCP (sauf pour les machines Solaris) les sources non compatibles Splunk (équipement réseaux, legacy…).

Description détaillée du service/composant de service :

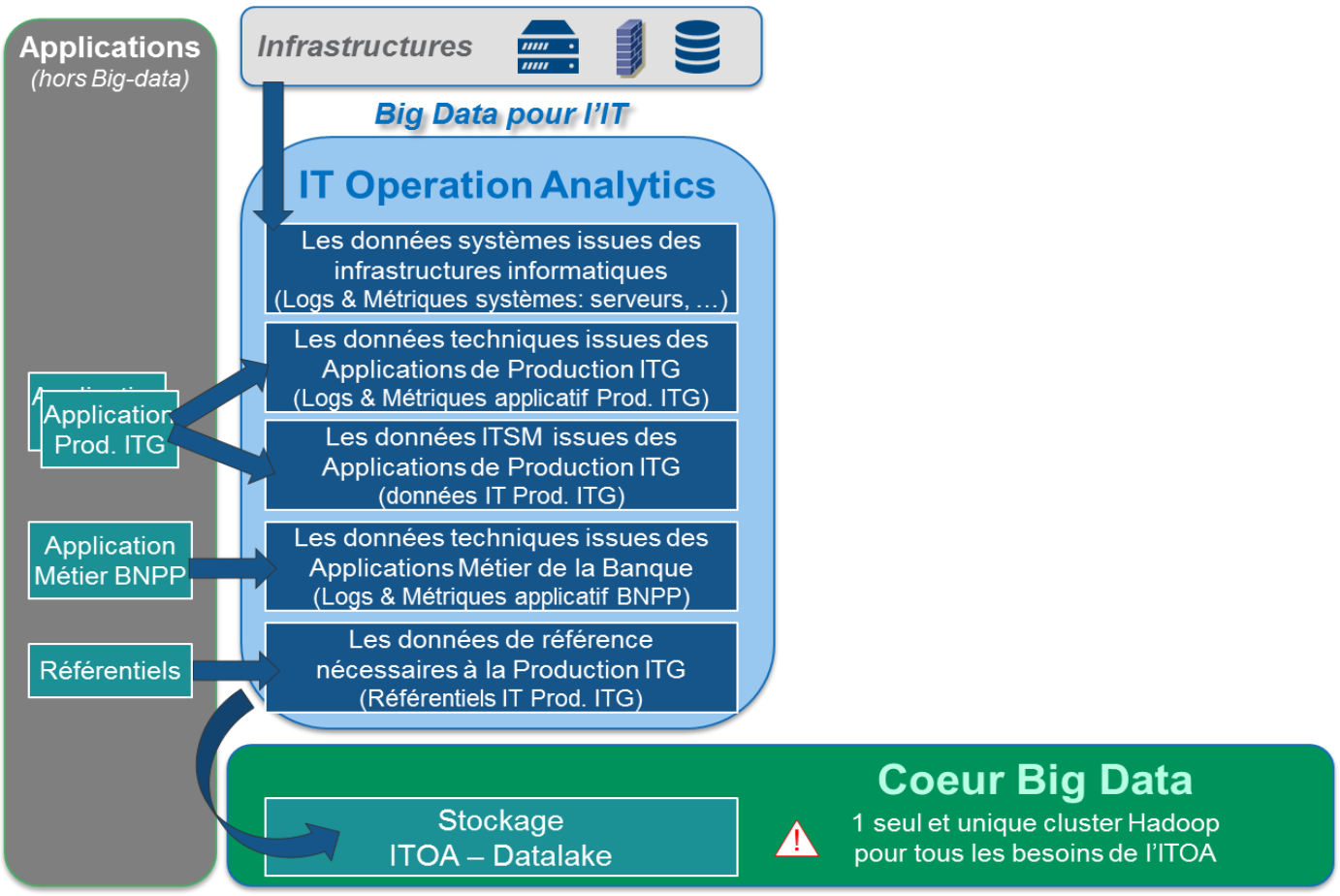


L'infrastructure ITOA/ Splunk est centralisée avec :
- une plate-forme de collecte mutualisée et entièrement opérée par BP2I pour sécuriser la production
- une plate-forme Splunk d'indexation et de requêtage mutualisable (possibilité pour certains projets de conserver une infrastructure dédiée, cependant la collecte des évènements sera opérée à partir de la plateforme de collecte centralisée).

Cartographie des environnements ITOA/ Splunk :

Plate-forme de Production (Mutualisable)	• > 40 Machines (7 Search Head, 16 Indexeurs, 2 Cluster Master, 2 DMC, 2 Deployment Serveurs, 8 collecteurs + 2 Internet, 1 DB-Connect)
Plate-forme Pré-production	• > 24 Machines (3 Search Head, 8 Indexeurs, 2 Cluster Master, 2 DMC, 2 Deployment Serveurs, 4 collecteurs + 2 Internet, 1 DB-Connect)
Plate-forme de Qualification et de formation interne	• > 12 Machines (2 Search Head, 2 Indexeurs, 2 Cluster Master, 2 DMC, 2 Deployment Serveurs, 2 collecteurs)
Plate-forme de Training	• > une machine (all in one) dédiée à l'auto-formation des utilisateurs

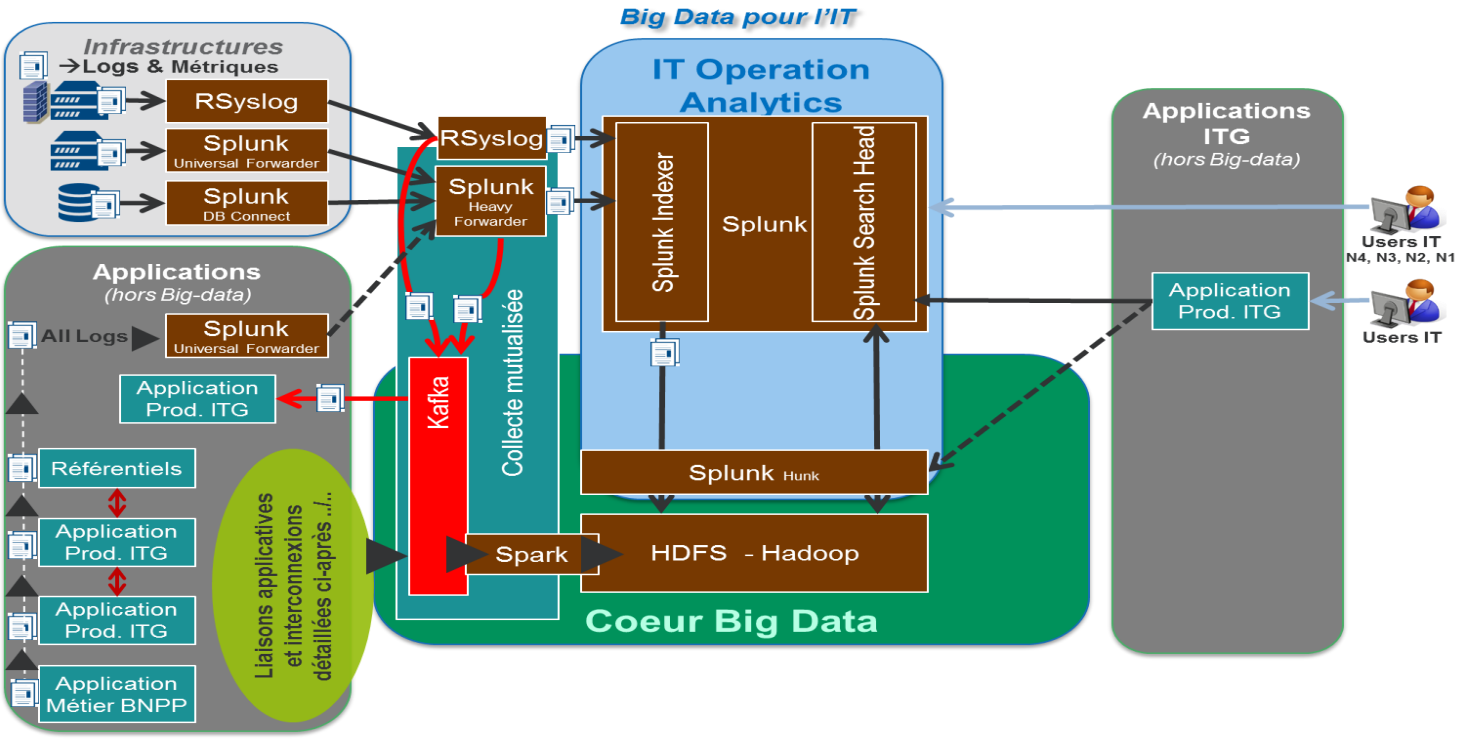
Typologie des données hébergées :



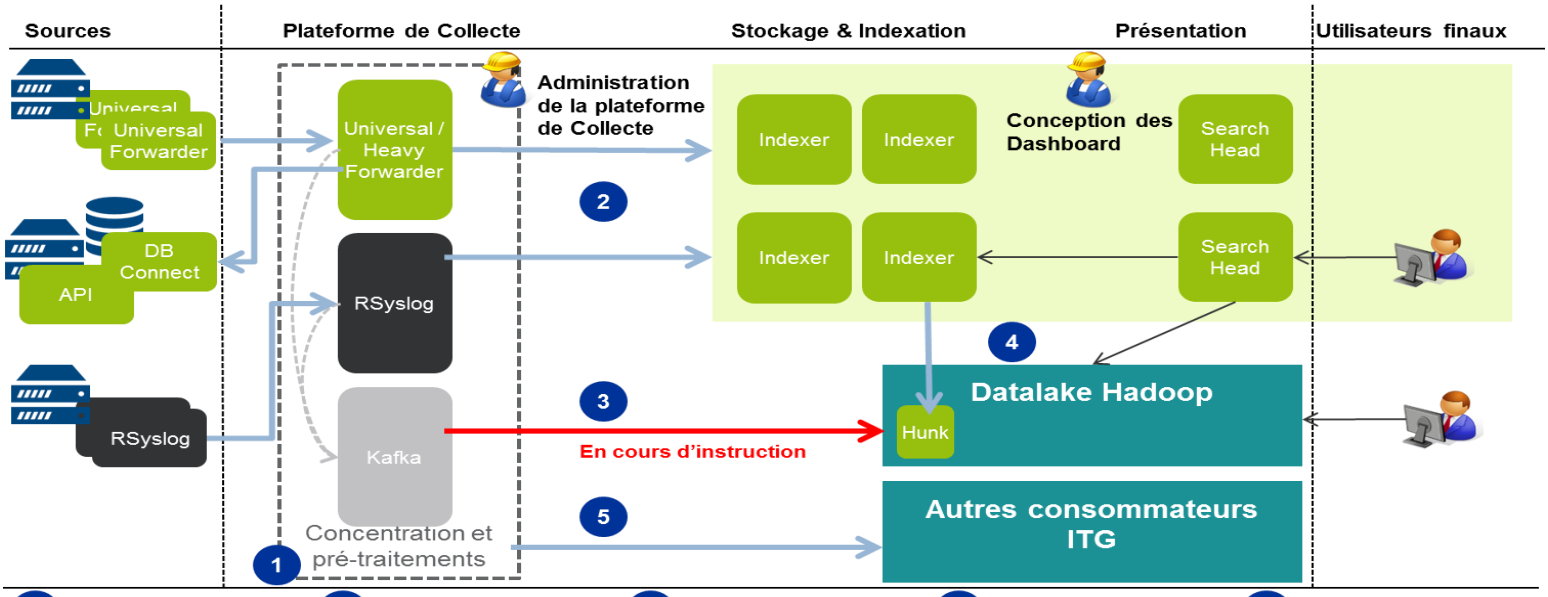
Pilotage du service

Le pilotage du service est mis en place sur la plate-forme de production avec Nimsoft et consignes AEL associées.
Tableau de bord et alerte custom par et pour TP36B.

Architecture fonctionnelle de la solution ITOA/Splunk :



Architecture applicative de la solution ITOA/Splunk :



1. La plateforme de collecte centralise l'ensemble des flux entrants (serveurs, équipements télécom, etc.)
2. Les indexer Splunk réceptionnent les données au format Splunk ou Syslog (formats pré-traités)
3. Toutes les données sont également envoyées au format brute dans le Datalake, via le bus Kafka
4. Les Datamart Splunk sont historisés dans Hadoop, et requêtables via les Search Head
5. D'autres consommateurs peuvent s'interfacer à la plateforme de collecte, et demander l'ajout de flux

Chaîne RSys | Chaîne Splunk | Kafka

Rappel des SLA

Le service est disponible pour les utilisateurs déclarés dans le Refog
La collecte ne concerne que les assets BP2I

L'infrastructure est Serious ready :
- Résiliences multiples (100% Cloud, Clusters Géodistants, FileaaS)
- Évolutif (ajout de tout type de nœud prévu)
- Gestion fine des habilitations

L'intégrité et la non perte des données est garantie depuis la source jusqu'aux indexeurs.

L'archivage des données dans le Datalake de l'IT est garanti.

Contacts BP2I :

Business Onwer / Product Manager : James BENKEMOUN
Service Owner / Manager : Pascal GOUPIL
Technic Leader : Jean-François NOEL
Product Owner : Sébastien GESSATI & Julián GUDIEL
Project Manager : Ilham SEHMAOUI

Support Mail : PARIS BP2I SPLUNK

MICA : SUP BP2I SPLUNK N2