

SÉCURITÉ DES

ARCHITECTURES ~~BIGDATA~~ LAMBDA

PRÉREQUIS

- ▶ ÉDITEUR YED
- ▶ EXCEL
- ▶ PAPIER



INTRODUCTION

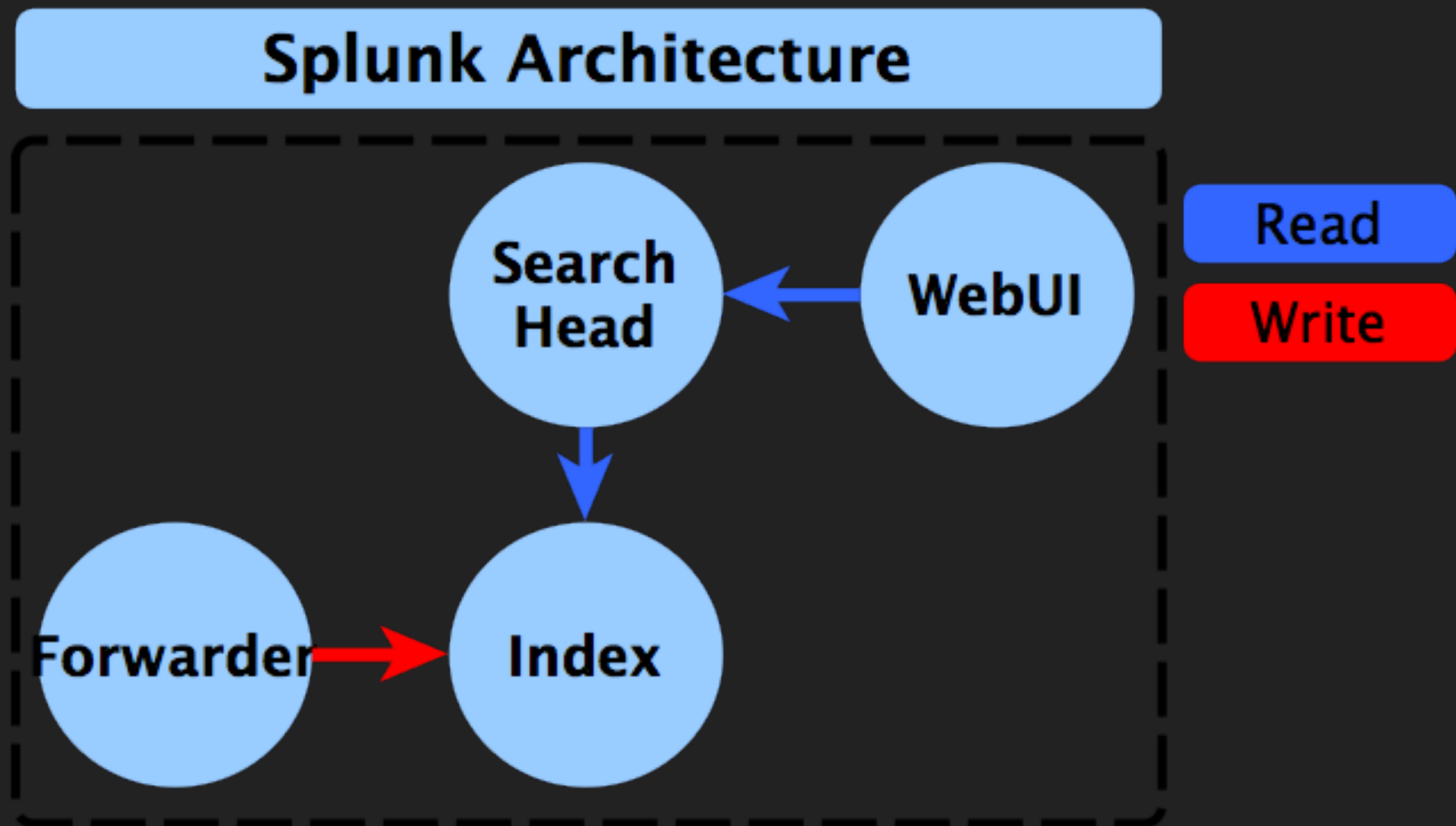
Un Client mystère pour ses besoins métiers souhaite déployer une architecture à base de Splunk chez lui, de façon sécurisée, isolée & autonome.

L'objectif étant évidemment de traiter un flux de données ...

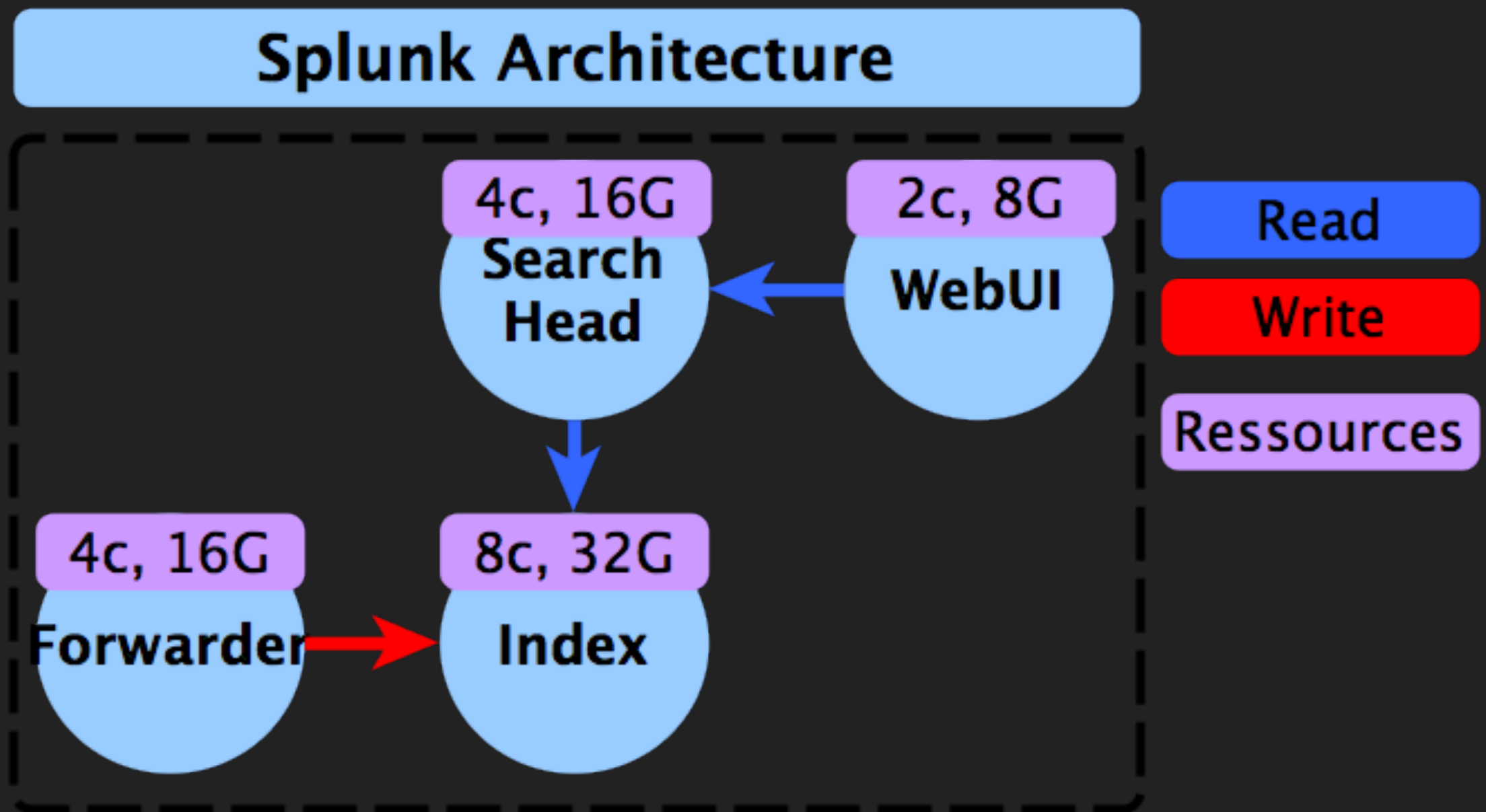
HYPOTHESES

- ▶ Flux raw data : **100GB / jour**
- ▶ Rétention raw data : **1 mois**
- ▶ Rétention hot data : **6 mois**
- ▶ Ratio de génération des hot data basé sur les raw data : **12%**
- ▶ Cluster Splunk
 - 1 index (1 mois),**
 - 1 index cloturé (6 mois)**
 - 3 Noeuds**

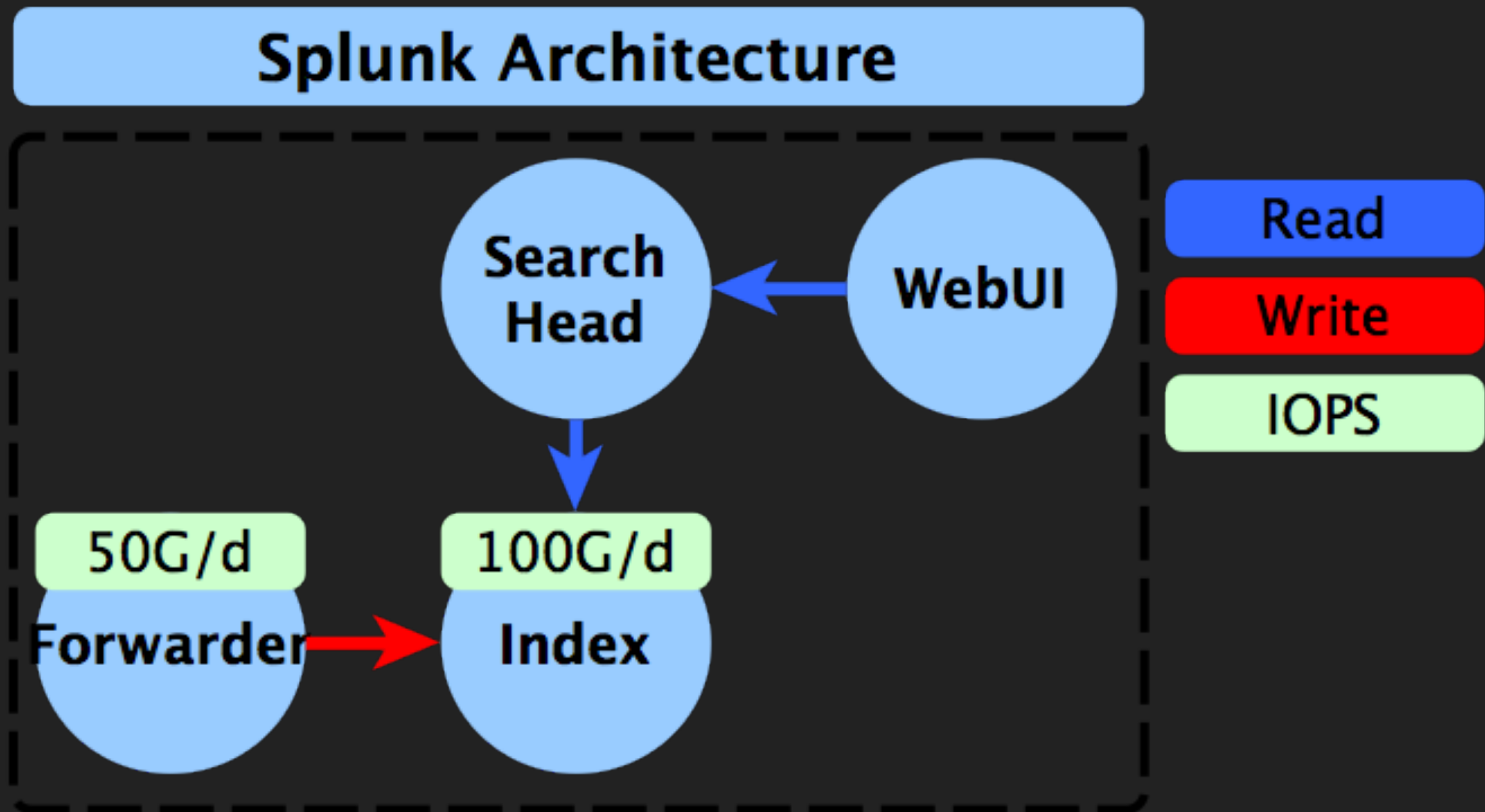
RAPPEL SPLUNK



RAPPEL SPLUNK



RAPPEL SPLUNK



ARCHITECTURE

- ▶ Défense périmétrique, sans défense en profondeur
- ▶ Isolation de la zone d'admin & internalisation des services IT
- ▶ SLA 99,999 (PCA)

LIVRABLES (1)

B.O.M

- ▶ Liste approvisionnement matériel
- ▶ Liste serveurs physiques
(Nom codifié, Fonction, Role, Zone, RAM, CPU, HDD, OS, ...)
- ▶ Liste des machines virtuelles
(Nom codifié, Fonction, Zone, Hyperviseur, RAM, CPU, HDD, OS, ...)
- ▶ Synthèse cout & allocation ressources

Outils : Excel

LIVRABLES (2)

Schéma

- ▶ Fonctionnel
(Zone, Equipements de sécurités, fonctions, rôles & serveurs virtuels)
- ▶ Physique
 - ▶ Fonctionnel + serveurs physique, Switch & Firewall
(yED ou Visio)
 - ▶ ~~Plan de rackage~~
(yED ou Visio)
 - ▶ ~~Plan de cablage~~
(Excel)
- ▶ Réseaux
 - ▶ Switch, Firewall, VLAN & LAN
(yED ou Visio)

PRÉPARATION B.O.M & ARCHITECTURE

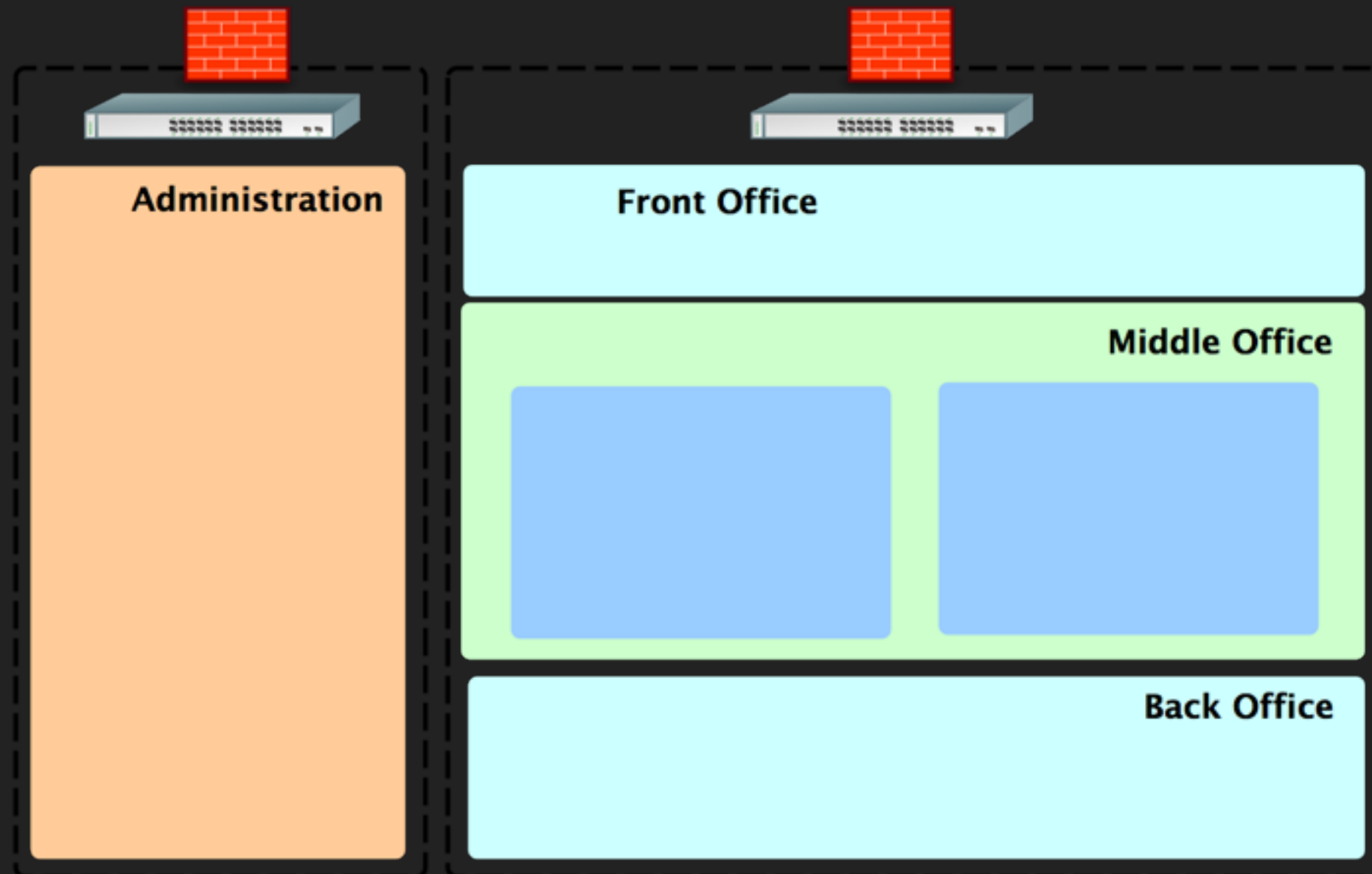
- ▶ Achat d'une licence Splunk, choix de la licence adéquate
 - ▶ 80K la licence
- ▶ Achat de serveur « *Super Micro* »
 - ▶ *Serveur lambda S : 5K*
 - ▶ *Serveur lambda M : 10K*
 - ▶ *Serveur lambda XL : 20K*
- ▶ HDD
 - ▶ *2TB : 1K*
 - ▶ *4TB : 2K*
- ▶ Carte réseaux : 0,5K
- ▶ Firewall : 15K (*XX ports*)
- ▶ Switch : 5K (*24 ports*)

MÉTHODOLOGIE

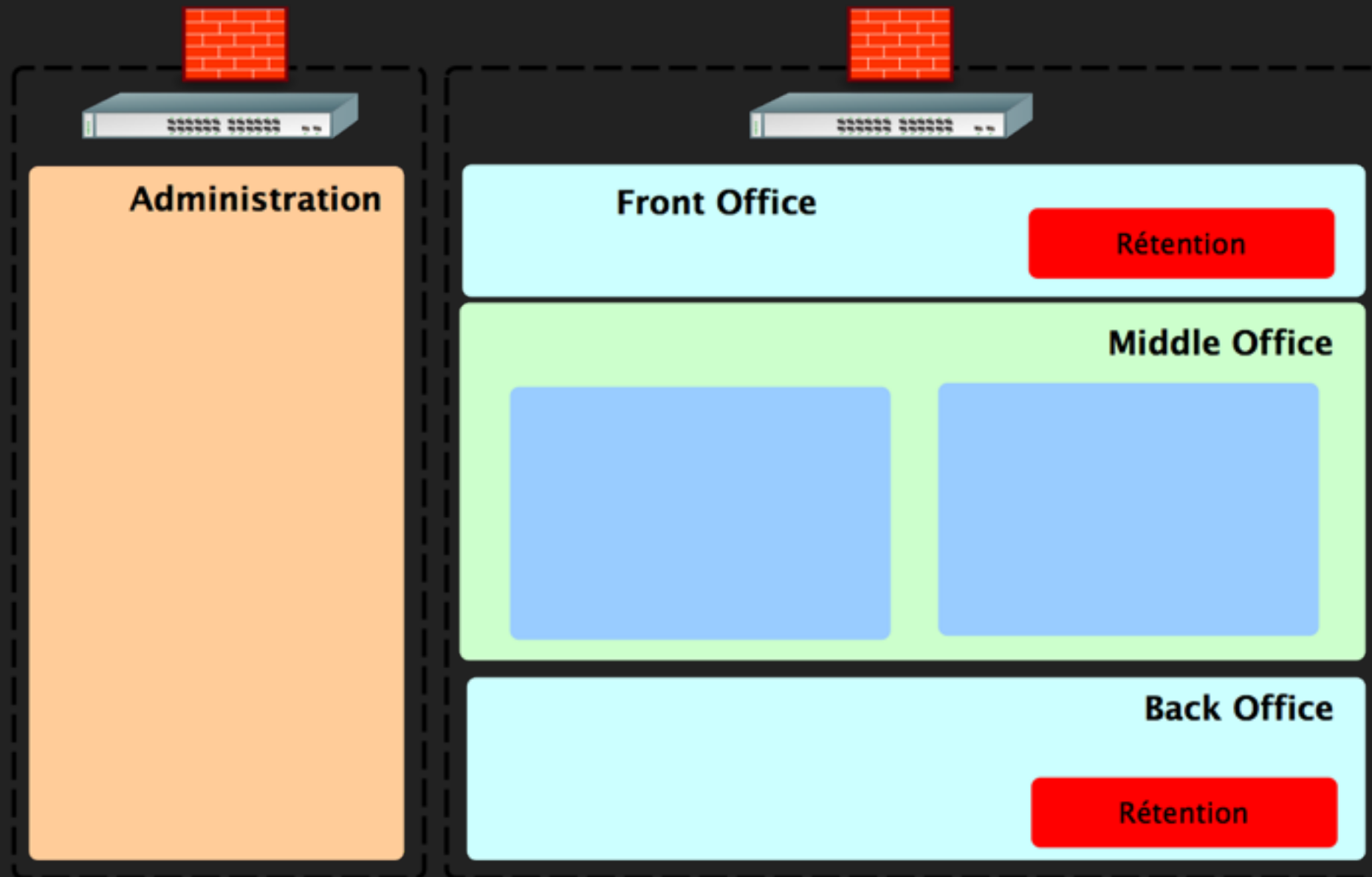
- ▶ Sizing de l'architecture en fonction des hypothèses
- ▶ Schéma « Macro »

CONSTRUCTION DES DIFFÉRENTES VUES

LET'S GO!



DON'T FORGET



EXEMPLE

