



# Implémentation de NSI avec un large volume de log

*Architectures*



## 1. Impact du type de traitement sur le choix de la solution

Les critères qui guident le choix de tel ou tel architecture de log sont multiples :

- Le volume de log total à analyser
  - Impact CPU :
    - Traitement temps réel
  - Impact Disque :
    - Ecriture des données dans la base SQL
    - Ecriture des logs bruts en archivage légal
    - Ecriture des logs enrichis / contextuels en archivage
- Durée de rétention en base (Raw Data – Daily Aggregation – Monthly Aggregation)
  - Impact CPU :
    - Temps d'agrégation
  - Impact Disque :
    - Temps d'agrégation
    - Temps de génération des rapports
    - Temps de purge
- Durée de rétention en Archive
  - Impact Disque :
    - Capacité d'archivage
- Constructeur et produit analysés
  - Impact CPU :
    - Certains constructeurs ont des logs dont le traitement est plus gourmand que d'autres.
    - Le traitement de multiples formats de logs avec de types de rapports et d'agrégation est plus consommateurs qu'un seul type de données.
- Utilisation du portail web
  - Impact CPU & Disque :
    - Quantité de rapports demandés en génération automatique
    - Quantité de rapports & de cubes générés à la demande
    - Simultanéité des demandes, et nombre d'accès au portail web simultanés
    - Cas particulier d'un envoi massif de mensuels (MSSP)

## 2. Impact du hardware sur le choix de la solution

L'impact de la configuration du Hardware est aussi important :

- Mémoire
  - 4-8 Go pour faciliter le fonctionnement de la base de données SQL
- CPU
  - 1 à 2 processeurs quad cœur pour la rapidité du traitement
- Disque
  - Vitesse de 10k 15k pour la rapidité des accès disques
- Raid
  - Type 1 (vitesse) ou 5 (sécurité)
- Cache disque
  - Le cache disque est un élément important pour fluidifier les accès disques



## 3. Architecture

Nous allons étudier plusieurs types d'architectures. Les effets de bords font que, dans les limites de classes, le choix de l'une au l'autre des architectures peut être envisagé.

Vous trouverez le tableau récapitulatif des configurations en fin de document

### 3.1. Moins de 2 millions de lignes de log

Il peut être envisagé de monter un Serveur Virtuel pour le héberger l'application.

Dans ce cas, nous recommandons la mise en place d'une connexion à la base de données sur un serveur physique et pas dans le serveur virtuel.

### 3.2. Moins de 30 millions de lignes de log par jour

L'Architecture est simple : un seul système matériel peut gérer la totalité de la solution. On y trouve Click&DECiDE NSI, la base de donnée SQL et le portail Web avec l'option Click&DECiDE BAI.

Il est recommandé de prévoir lorsque l'on est proche des 30 millions, de déplacer l'archivage sur une zone SAN / NAS externe.

### 3.3. Moins de 60 millions de lignes de log par jour

L'Architecture est double :

- Un système dédié va gérer les logs, les recevoir, les trier, les enrichir, préparer les fichiers d'archive et envoyer les logs dans la base de donnée SQL dédiée du deuxième serveur.
- Un système dédié va traiter les données de la base de données, agréger les données, générer les rapports, cubes et les alarmes. Ce système va aussi héberger le portail Web.

### 3.4. Moins de 90 millions de lignes de log par jour

L'Architecture est triple :

- Deux systèmes dédiés vont gérer les logs, les recevoir, les trier, les enrichir, préparer les fichiers d'archive et envoyer les logs dans la base de donnée SQL dédiée du troisième serveur.
- Un système dédié va traiter les données de la base de données, agréger les données, générer les rapports, cubes et les alarmes. Ce système va aussi héberger le portail Web.

### 3.5. Plus de 90 millions de lignes de log par jour

Merci de nous consulter



## 4. Tableau récapitulatif

Lignes de log par jour	Harware #1				Harware #2 - SQL Entreprise				Option SAN pour l'archivage
	CPU	RAM (Gb)	Disque (Gb)	Raid	CPU	RAM (Gb)	Disque (Gb)	Raid	Disque (To)
1 000 000	Dual Core	3	60	-					
2 000 000	Dual Core	4	80	-					
5 000 000	Quad core	4	160	5					
10 000 000	Quad core	4	320	5					
15 000 000	2 x Quad core	4	480	5					
20 000 000	2 x Quad core	4	630	5					
30 000 000	2 x Quad core	6	600	5					1
60 000 000	2 x Quad core	4	600	5	2 x Quad core	8	600	5	2
90 000 000	2 x Quad core (2 système)	4	600	5	2 x Quad core	12	900	5	3