**Dossier d’Architecture Technique**

**48h - groupe 5**

[***Consignes sur la documentation technique***](https://sites.google.com/a/veolia.com/ist-efr-archi-perf/infos-pratiques/liste-des-docs-techniques)

**Table des matières**

[**1 Points en suspens & obsolescences 4**](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.1fob9te)

[**2 Présentation de l’application 5**](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.3znysh7)

[2.1 Contexte 5](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.2et92p0)

[2.2 Descriptif projet / application 6](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.tyjcwt)

[2.3 Positionnement SI 8](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.3dy6vkm)

[**3 Architecture technique 8**](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.2s8eyo1)

[3.1 Schéma 9](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.17dp8vu)

[3.2 Description des briques (Front, Back, Batch, autres) 11](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.3rdcrjn)

[3.2.1 Mon Appli 11](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.26in1rg)

[3.2.2 Appli A 11](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.lnxbz9)

[3.2.3 Appli B 11](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.35nkun2)

[3.3 Optimisation(s) 12](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.1ksv4uv)

[3.3.1 Performances 12](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.44sinio)

[3.3.2 Financière(s) 12](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.2jxsxqh)

[**4 Architecture Réseau 13**](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.3j2qqm3)

[4.1 Schéma 13](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.1y810tw)

[4.2 Matrice des flux 16](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.4i7ojhp)

[4.3 URL sortantes 16](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.2xcytpi)

[**5 Infrastructure 17**](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.2bn6wsx)

[5.1 Production 17](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.3as4poj)

[5.2 Pré production 18](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.1pxezwc)

[5.3 Qualification 18](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.49x2ik5)

[5.4 Développement 18](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.2p2csry)

[5.5 Autres 18](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.147n2zr)

[**6 Sécurité 19**](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.ihv636)

[6.1 Coffre fort 19](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.32hioqz)

[6.2 Authentification 19](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.1hmsyys)

[6.2.1 Procédure de gestion des accès 19](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.41mghml)

[6.2.2 Providers 19](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.2grqrue)

[6.2.3 Gestion des sessions 19](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.vx1227)

[6.2.4 Traçabilité/Auditabilité 19](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.3fwokq0)

[6.3 Liste des comptes non nominatifs et justifications 20](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.1v1yuxt)

[6.4 Console(s) d’administration 20](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.2u6wntf)

[6.5 Données à caractères personnelles ou sensibles 20](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.3tbugp1)

[6.6 Certificat(s) 21](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.28h4qwu)

[6.7 Plage de maintenance (patching,service managé ou pas) 21](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.nmf14n)

[**7 Plan de reprise d'activité 22**](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.1mrcu09)

[7.1 Périmètre 22](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.46r0co2)

[7.2 Processus de bascule 22](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.2lwamvv)

[**8 Chargement & Sauvegarde & Archivage 23**](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.4k668n3)

[8.1 Chargement initial et reprise des données 23](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.1egqt2p)

[8.2 Sauvegarde 23](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.3ygebqi)

[8.3 Archivage 23](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.2dlolyb)

[8.4 Purge 23](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.sqyw64)

[8.5 Restauration 23](https://docs.google.com/document/d/1LvsWvc_ytoqUGlMtdUvzhD_8FcPaaUY0/edit#heading=h.3cqmetx)

# 1 Points en suspens & obsolescences

| Lister ici :   * les points qui nécessitent un arbitrage et qui pourraient avoir un impact sur la définition de l'architecture * Les applications, modules, OS qui sont obsolescents. |
| --- |

# 2 Présentation de l’application

## 2.1 Contexte

## 

| ***Rédacteurs*** *: ynov - groupe 5*  ***Lecteurs*** *: Tous*  ***Valideurs*** *: Chapter*  ***Ce projet a pour objectif de configurer un programme permettant de superviser les machines présentes sur le site de Veolia. L’application est déployée via Docker Compose.***  ***Ce projet fonctionne dans un environnement hautement sécurisé et isolé d'Internet.***  *IL contient:*  *- un proxy*  *- une base de données pour la sauvegarde de log et de résultat d’oci* |
| --- |

***Entité, service et contacts***

| **Entité** | **Domaine** | **Code imputation** | **Prénom** | **Nom** |
| --- | --- | --- | --- | --- |
| IS&T EFR |  |  |  |  |

***Interlocuteur(s) à privilégier***

| **Entité** | **Prénom** | **Nom** | **Responsabilité** |
| --- | --- | --- | --- |
| IS&T EFR |  |  | Chapter Lead |
| IS&T EFR |  |  | Tech lead / Plateforme |
| IS&T EFR |  |  | Tech Lead / Chapter |

***Identification du projet***

| **Entité** | **Domaine** | **Chapter** | **Application** |
| --- | --- | --- | --- |
| IS&T EFR |  |  |  |

## 2.2 Descriptif projet / application

| **Rédacteurs** : Chapter / Squad  **Lecteurs**  : Tous  **Valideurs**  : Chapter  *Cette fiche permet d'avoir une idée rapide du projet.* |
| --- |

|  | **Choix** | **Explications** |
| --- | --- | --- |
| **Modules** | * WEB * Mobile * Service * Batch * Application locale |  |
| **Type de solution** | * SaaS * PaaS * CaaS * IaaS | sur infrastructure propre |
| **Internet** | * OUI * NON |  |
| **Nbre de Users** | * Mobile : * WEB : * Interne : * Externe : | Une machine par site |
| **Types utilisateurs** | * Interne * Indus * Partenaires * Internautes * Clients finaux * autres | Système utilisé sur l’infrastructure de l’entreprise |
| **Plages de fonctionnement**  **IHM** | 24/24 -- 7/7 |  |
| **Plages de fonctionnement**  **BATCH** | 24/24 -- 7/7 |  |
| **Astreinte** | * Oui * non |  |
| **Plages de maintenance** |  | Liste des modules (services) qui sont indisponibme pour cause de maintenance + plages |
| **PRA ou**  **Dispositif failover** | * Oui * non | Oui, via docker répliquée ( amélioration possible avec un kube ) |
| **Proxy sortant** | * Oui * Non * Pas concerné | Fournie dans la solution |

| Domaine applicatif | Criticité | Liste des référentiels impactés ou pas ? | Remplace l’application ? |
| --- | --- | --- | --- |
|  | Critique Majeur  Normal | Les infrastructures des sites |  |
|  |  |  |  |

Pour la criticité se référer au tableau suivant : [Criticités Métiers des Applications](https://docs.google.com/spreadsheets/d/1jPpgDrxa154yvHYJlWH6fsMBHbCfjdHfkf8nJs0ApP0)

## 2.3 Positionnement SI (cartographie)

| **Rédacteurs** : Chapter / Squad  **Lecteurs**  : Tous  **Valideurs**  : Chapter + Archi + sécu  *Machine utilisé comme dmz entre le site et le réseau externe*  *(proxy inclus)* |
| --- |

[Veuillez renseigner le lien sur votre carto](https://veglobal.service-now.com/apm_portal?id=apm_business_applications_list&table=cmdb_ci_business_app)

Faites une copie d’écran aussi :

PAS D’ACCÈS AU SITE

# 3 Architecture technique

# 3.1 Schéma

|  |
| --- |

| 1. Le script oci sur le réseau interne et les logs sont générés dans le réseau 2. Ils sont envoyés depuis le réseau interne sur la bdd 3. Les log et rapport sont visibles sur kibana et récupérable sur la bdd depuis le centre |
| --- |
|  |

## 3.2 Description des briques (Front, Back, Batch, autres)

| *Liste des composants logiciels avec version et date de fin de support*   * **Front** : Interface utilisateur minimale * **Back** : Gestion des machines supervisées * **Bdd** : Stockage des logs et des états des machines supervisées * **Batch** : Exécution de tâches de supervision planifiées |
| --- |

### 3.2.1 Mon Appli

| 1. Acteurs   Les log et rapport sont génère sur la machine puis, envoyer sur la bdd   1. Mes briques (faire apparaître toutes les briques)    1. Script oci   Fonction : génère le rapport oci au format json  Technologie : bash   1. kibana   Fonction : afficher les informations de la bdd  Technologie :   1. Bdd   Fonction : sauvegarde des log et rapport  Technologie :   1. Serveur de temps   Fonction :Permettre la synchronisation du temps entre les machine du site  Technologie : ntp   1. Proxy   Fonction :Sécurison du perimetre  Technologie : haproxy |
| --- |

# 4 Architecture Réseau

| *Ce chapitre décrit tous les aspects liés au réseau. L'objectif est de référencer l'ensemble des ressources réseaux utilisées.* |
| --- |

## 4.1 Schéma

| *Bdd : 9200*  *Ntp : 123 udp*  *kibana : 5601*  *Haproxy : 8080,8530* |
| --- |

| Ceci est une template que vous pouvez copier.  L'exemple ci-dessous fait apparaître les ports et les protocoles, en fonction de la complexité de vos architectures, vous pouvez avoir plusieurs schémas (soit en zoomant, soit par typologie à afficher …) |
| --- |

## 4.2 Matrice des flux

***Utiliser le modèle Google sheet ⇒*** [***Modèle “Matrice des flux”***](https://sites.google.com/a/veolia.com/ist-efr-archi-perf/infos-pratiques/liste-des-docs-techniques)

## 4.3 URL sortantes

| *Faire apparaître la liste des url sortantes dans le tableau suivant.* |
| --- |

| **Composant  Impacté** | **Service Description** | **Service URL** | **Authentification Compte / clé / token** | **Commentaires** |
| --- | --- | --- | --- | --- |
| Server de temps | Serveur de temps | docker-url:123 |  |  |
| *kibana* | *kibana* | docker-url:5601 |  |  |
| bdd | bdd | docker-irl:9200 |  |  |
|  |  |  |  |  |

# 5 Infrastructure

## 5.1 Production

| Ressource AWS, Tags :  Liens AWS "Groupes de ressources" |
| --- |

## 5.2 Pré production

| Ressource AWS, Tags :  Liens AWS "Groupes de ressources" |
| --- |

## 5.3 Qualification

| Idem. |
| --- |

## 5.4 Développement

| idem. |
| --- |

## 5.5 Autres

| Idem. |
| --- |

# 6 Sécurité

## 6.1 Coffre fort

| *Est ce que vous utilisez un coffre fort ?*   * *Lequel :* * *Où :* * *Qui a acces :* * *Où est stocké le mdp du coffre fort* * *Périmètre (infra, app, chapter, domaine, app) :* * *Indiquer aussi si vous utilisez des clés SSH et des token.* |
| --- |

## 6.2 Authentification

### 6.2.1 Procédure de gestion des accès

|  |
| --- |

### 6.2.2 Providers

|  |
| --- |

| Module | Provider | Protocole | Politique de mot de passe | Double authentication |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 6.2.3 Gestion des sessions

### 6.2.4 Traçabilité/Auditabilité

## 6.6.4 Console(s) d’administration

| *Préciser ci-dessous l'existence de console d'administration autres que fonctionnelles qui permettent d'administrer et sur quel environnement la console est activée.* |
| --- |

| Module / serveur / service | Console | URL | Fonction | Env. activée ? |
| --- | --- | --- | --- | --- |
| kibana | kibana | dockerurl:5601 | Voir les log et les rapport oci |  |
|  |  |  |  |  |
|  |  |  |  |  |

| Module | Managé / vm | Plage de maintenance | Indisponibilité |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | Total / partielle |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# 8 Chargement & Sauvegarde & Archivage

| **Rédacteurs** : Chapter / Squad & Plateforme  **Lecteurs**  : Tous  **Valideurs**  : Plateforme & Chapter  *L'objectif de ce chapitre est de décrire tous les aspects liés à la data de votre application.*  *La restauration est un point important car elle peut aussi couvrir le rafraîchissement d'un environnement depuis un autre.* |
| --- |

## 8.1 Chargement initial et reprise des données

Utilisation de volumes Docker montés sur des disques résilients.

## 8.2 Sauvegarde

Snapshots réguliers des volumes Docker

## 8.3 Archivage

Conservation des logs sur 6 mois

## 8.4 Purge

Rotation automatique des logs

## 8.5 Restauration

Redéploiement via Docker Compose avec états sauvegardés