



**MINISTÈRE  
DE L'ÉDUCATION  
NATIONALE,  
DE L'ENSEIGNEMENT  
SUPÉRIEUR  
ET DE LA RECHERCHE**

*Liberté  
Égalité  
Fraternité*

**Secrétariat général**

Direction du numérique  
pour l'éducation  
Sous-direction des services  
numériques  
Bureau des services et outils  
numériques pour l'éducation  
(DNE SN1)

99, rue de Grenelle  
75357 Paris SP 07

Secrétariat général  
Service de l'action  
administrative et des  
moyens  
Sous-direction des achats  
(SAAM B)  
Bureau de la stratégie  
et de l'ingénierie des achats  
(SAAM B1)

61-65, rue Dutot  
75732 Paris Cedex 15

# **CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES**

**ANNEXE 04.0** : Document d'architecture technique (GAR)

**Procédure** : MEN-SG-AOO-24002

**Objet** : Prestations de prise en charge de la solution du gestionnaire d'accès aux ressources (GAR), d'hébergement, d'exploitation, de maintenance, de support et de développement de ladite solution pour le compte du ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche.

# RENATER - GAR - Plateforme GAR

**DAT**  
**17.00**

Référence :	Version	En date du
RENATER-GAR-E/DAT.0003.Plateforme GAR	16.02	19/07/2024

Version	Rédigé par	Objet	Vérifié		Validé	
			Par	Le	Par	Le
16.02	Wordline	Mise à jour dans le cadre de l'EB 479	Wordline	05/08/2024	RENATER  GAR 7.4 - Support GoNoGO MEP à con	01/05/2024

Version	Date	Description	Auteur(s)
1.0	16/09/2016	Création	Wordline
1.1	21/10/2016	Mises à jour suite aux retours MEN/Renater	Wordline
1.2	20/01/2017	Mises à jour suite aux retours MEN/Renater	Worldline
1.3	03/02/2017	Mises à jour suite aux retours MEN/Renater	Worldline
1.4	29/03/2017	Mises à jour suite aux retours MEN/Renater	Worldline
1.5	07/04/2017	Mises à jour suite aux retours MEN/Renater	Worldline
1.6	09/10/2017	Ajout de précisions suite aux échanges avec Renater Prise en compte de l'upgrade plateforme année 2 Ajout Gestion des DNS Ajout WS Liste des établissements Ajout de précisions sur les sauvegardes	Worldline
1.7	20/11/2017	Ajout de précisions dans le changelog de la version 1.6 Prise en compte des retours Renater de la fiche de relecture Fiche-de-lecture-DAT-Vx-RENATERaWL1.4.xlsx	Worldline
1.8	18/12/2017	Prise en compte des retours Renater de la fiche de relecture Fiche-de-lecture-DAT-Vx-RENATERaWL1.5.xlsx	Worldline
1.9	16/03/2018	Ajout de la politique de patch management	Worldline
1.10	12/11/2018	Prise en compte de l'upgrade plateforme année 3	Worldline
1.11	20/12/2018	Complément sur les services par machines	Worldline
1.12	15/02/2019	Revue des documents de références, §5.15 ajout du plan de production, §5.16 Stratégie de mise à jour des composants CentOS	Worldline
1.13	05/09/2019	Modifications infrastructure Versions applicatives Schéma logique Bdd Réplication Bdd	Worldline
1.14	09/09/2019	Mise à jour des graphiques du chapitre 5.4.x	Worldline
1.15	14/10/2019	Mise à jour du chapitre « accès ressources »	Worldline
1.16	24/12/2019	Mise à jour des versions des composants, Bdd de réplication et retrait de la plateforme POC Mobilité	Worldline
1.17	10/02/2020	Upgrade capacitaire 5M & Mise à jour schéma & inventaire des services	Wordline
1.17.1	05/03/2020	Retrait des lignes contenant des références au POC-Mobilité	Wordline
1.18	04/08/2020	Mise à jour de l'inventaire des services suite aux bench 5M/7M	Wordline
1.19	06/01/2021	Mise à jour de la plateforme de stats	Wordline
1.19	08/04/2021	Ajout serveurs de preprod STATS	Wordline
1.20	16/04/2021	Mise à jour infrastructure et services GAR	Wordline
1.20b	30/04/2021	Ajout du chapitre Site de communication ainsi que diverses corrections.	Wordline
1.21	08/07/2021	Mise à jour WS Ressources affectées à l'accédant	Wordline
2.00	21/07/2021	Version validée	Wordline
2.01	13/12/2021	Mise à jour MySQL8	Wordline
3.0	24/01/2022	Version validée	Wordline
3.0.1	01/02/2022	Mise à jour composants R6.0	Wordline
3.0.2	21/03/2022	Refonte des tableaux d'inventaires	Wordline
3.0.3	22/03/2022	Ajout des composants Site de communication	Wordline
3.0.4	07/04/2022	Report en annexe de l'inventaire plateforme	Wordline
04.00	13/04/2022	Version validée	Wordline

Version	Date	Description	Auteur(s)
04.01	26/04/2022	Mise à jour dans le cadre de la release 6.1 du GAR Mise à jour dans le cadre du franchissement du palier capacitaire	Wordline
05.00	04/05/2022	Version validée	Wordline
05.01	21/07/2022	Ajout des composants SUMiT et mise à jour du schéma physique (modification site de communication) Mise à jour des informations de recopie suite au PRA 2022	Wordline
06.00	29/08/2022	Version validée	Wordline
05.04	26/08/2022	Mise à jour dans le cadre de la release 6.1.90 du GAR et montée de version spring Boot pour la gestion de la faille de sécurité Spring4Shell	Wordline
06.02	21/09/2022	Mise à jour dans le cadre de la version 6.2 du GAR	Wordline
06.03	26/09/2022	Mise à jour des versions des produits Statistiques	Wordline
07.00	28/11/2022	Validation des modifications apportées dans le cadre de la Release 6.2 du GAR	Wordline
07.01	18/10/2022	Mise à jour dans le cadre de la release 7.0	Wordline
08.00	27/02/2023	Validation des modifications apportées dans le cadre de la Release 7.0 du GAR	Wordline
08.01	06/03/2023	Ajout d'informations techniques sur la ressource de test	Wordline
08.02	17/03/2023	Ajout schéma de la ressource de test	Wordline
09.00	20/03/2023	Validation des modifications apportées dans le cadre de la Release 7.0 du GAR	Wordline
09.01	24/03/2023	Mise à jour dans le cadre de la version 7.1 : mise en cache des metadonnées	Wordline
10.00	16/05/2023	Version validée du document dans le cadre de la 7.1	Wordline
10.01	15/09/2023	Mise à jour dans le cadre de la release 7.2	Wordline
10.02	20/09/2023	Suppression d'éléments de révision	Wordline
11.00	29/09/2023	Validation du document	Wordline
12.00	18/10/2023	SUMIT-GAR Mise en place de l'interface	Wordline
12.01	03/11/2023	Correction version WordPress et PHP	Wordline
12.02	06/11/2023	Correction version PHP et Nginx	Wordline
13.00	06/11/2023	Validation du document	Wordline
13.01	06/11/2023	le cadre de la release 7.1.90	Wordline
13.02	11/12/2023	SUMIT-GAR Mise en place de l'interface générique	Wordline
14.00	11/01/2024	Version validée	Wordline
14.01	25/01/2024	Mise à jour dans le cadre de la release 7.3	Wordline
15.00	16/02/2024	Version validée	Wordline
15.01	16/05/2024	Prise en compte des remarques MEN	Wordline
15.02	17/05/2024	Prise en compte des remarques MEN	Wordline
16.00	24/05/2024	Version validée	Wordline
16.01	23/04/2024	Mise à jour dans le cadre de l'EB 479	Wordline
16.02	17/07/2024	Mise à jour suite relecture	Wordline
17.00	05/08/2024	Validation du document	Wordline

## Table des matières

1.	Introduction .....	8
1.1	Objet du document .....	8
1.2	Responsabilités liées au document.....	8
1.3	Documents de référence.....	8
1.4	Autres documents utilisés .....	9
1.5	Abréviations .....	9
1.6	Glossaire .....	9
2.	Contexte .....	10
3.	Présentation générale de la solution GAR.....	11
4.	Architecture logicielle .....	14
4.1	Les composants du GAR .....	14
4.2	La solution logicielle .....	19
4.2.1	Socle API.....	23
4.2.2	Batchs .....	25
4.2.3	Web Services REST .....	25
4.2.4	IHM .....	25
4.2.5	Module d'accès aux ressources .....	25
4.2.6	Module de moissonnage des ressources .....	29
4.2.7	Module Import données ENT.....	29
4.3	Site de communication GAR .....	31
4.3.1	Solution technique .....	31
4.3.2	Infrastructure d'hébergement .....	31
4.4	Service support GAR (Jira).....	33
4.4.1	Infrastructure d'hébergement .....	33
4.5	WS Interfaçage SUMiT/Agent GAR .....	33
4.5.1	Solution technique .....	33
4.5.2	Infrastructure d'hébergement .....	34
4.6	Module migration des idOpaques.....	34

4.7	WS Ressources affectées à l'accédant.....	35
4.8	WS Rapport d'Affectation .....	35
4.9	WS Décompte d'Affectations (et Batch) .....	36
4.10	Simulateur ENT .....	36
4.10.1	Présentation générale de la solution Simulateur .....	36
4.10.2	Les composants du Simulateur .....	37
4.10.3	Mediacentre .....	40
4.11	Ressources GAR de test et RTC .....	41
4.12	Interface de lancement des batchs en validation .....	41
4.13	Bases de données .....	43
4.13.1	Liste .....	43
4.13.2	Gestion des connexions .....	43
4.13.3	Règles de nommage.....	43
5.	Architecture applicative .....	45
5.1	Version logicielle .....	45
5.2	Composants communs techniques.....	46
5.2.1	Serveurs SMTP .....	46
5.2.2	Log management.....	46
5.2.3	Authentification portail GAR.....	49
5.2.4	Service de diffusion des vignettes GAR .....	49
5.2.5	Aide en ligne IHM Affectation. ....	49
5.2.6	Batch de suppression des comptes support .....	49
5.3	Stratégie d'ordonnancement des services .....	50
5.4	Interfaces du système .....	50
5.5	Design patterns .....	51
6.	Architecture technique .....	52
6.1	Description architecture logique.....	52
6.1.1	Introduction .....	52
6.1.2	Zones réseau .....	52
6.1.3	Architecture de production .....	54
6.1.4	Architecture de pré-production .....	55
6.1.5	Architecture de validation fonctionnelle/tests partenaires .....	56
6.2	Schéma architecture physique .....	57
6.2.1	Scopes réseaux et VLANs – environnements hors production .....	59
6.2.2	Scopes réseaux et VLANs – environnement de production .....	59
6.3	Disponibilité des ressources .....	61
6.4	Schéma logique des BdD GAR .....	63
6.4.1	Stratégie de répartition des accès BdD .....	64

6.5	Scalabilité.....	65
6.6	Stratégie et architecture pour sauvegardes, restaurations, purges, archivages .....	66
6.6.1	Sauvegarde des serveurs physiques de Base de données.....	66
6.6.2	Sauvegarde des serveurs virtualisés hors Base de données .....	67
6.6.3	Sauvegarde des serveurs virtualisés de Base de données .....	67
6.6.4	Restauration des données .....	67
6.6.5	Tests de restauration des données.....	67
6.7	Stratégie et architecture pour la supervision du système.....	68
6.8	Stratégie et architecture pour la métrologie du système.....	68
6.9	Stratégie de gestions des logs .....	69
6.9.1	Gestion des logs applicatifs .....	69
6.9.2	Gestion des logs système .....	69
6.10	Stratégie de sécurité du GAR.....	71
7.	PROCEDURE DE PLAN DE REPRISE D'ACTIVITE.....	72
7.1	Généralité.....	72
7.2	Définition d'un sinistre Majeur .....	72
7.3	Rappel des engagements.....	73
7.4	Présentation de nos Datacenters .....	73
7.4.1	Datacenter de Seclin/La Pointe .....	73
7.4.2	Datacenter de Seclin/ Dassault .....	74
7.4.3	Interconnexion de nos deux Datacenters .....	75
7.5	Plan de Continuité des Services du GAR sur plusieurs sites actifs.....	76
7.5.1	Description du Plan de Reprise d'Activité .....	77
7.5.2	Périmètre et impact du Plan de Reprise d'Activité.....	77
7.5.3	Principe du Plan de Reprise d'Activité .....	78
7.7	DESCRIPTION DU PLAN DE REPRISE D'ACTIVITE.....	80
7.7.1	Etape 1 – Décisionnelle.....	80
7.7.2	Etape 2 – Bascule technique .....	80
7.8	ANNEXES .....	84
7.9	Volumétrie .....	85
7.9.1	Hypothèses d'usage de la solution GAR.....	85
7.9.2	Analyse des besoins réseaux de la solution .....	85
7.9.3	Projections dimensionnement plateforme .....	86
7.10	Interconnexion avec le réseau RENATER .....	87
7.11	Référencement IPs publiques .....	88
7.12	Stratégie DNS.....	88
7.13	Architecture NTP .....	88
7.14	Inventaire plateformes .....	89

---

7.15	Stratégie de mise à jour de composants Redhat/Centos.....	89
8.	Annexe.....	91
8.1	Description offre cloud mutualisé .....	91
8.1.1	ESXi.....	94
8.1.2	Virtual Center .....	94
8.2	Matrice de flux.....	94
8.3	Plan d'adressage des IP publiques.....	94



# 1. Introduction

## 1.1 Objet du document

Ce document est le Dossier d'Architecture Technique pour la plateforme GAR (Gestionnaire d'Accès aux Ressources).

## 1.2 Responsabilités liées au document

Le chef de projet Worldline est responsable de la rédaction du Dossier d'Architecture Technique, RENATER et le Ministère de l'Education Nationale (MEN) sont responsables de sa validation.

## 1.3 Documents de référence

Número	Réf. Document	Type
DR1	P.COS.0001.1.1.FINALE – Plan d'Assurance Sécurité	PAS
DR2	GAR-S2.COS.0001.Politique de Sécurité Opérationnelle.V01.00	PSO
DR3	GAR-S2.PQP.0001.Plan Qualité Projet.V03.00	PQP
DR4	GAR-S2.PAQ Convention de service opérationnelle V02.00	PAQ
DR6	GAR-S2.DSFD.0001.WS_Gestion_Des_Abonnements.V09.00	DSFD
DR7	GAR-S2.DSFD.0002.Spécification_du_WS_Liste_Ressources.V05.00	DSFD
DR8	GAR-S2.DSFD.0004.Affectations_automatiques_et_pré-affectations.V06.00	DSFD
DR9	GAR-S2.DSFD.0007.Spécifications_du_moissonneur.V07.00	DSFD
DR10	GAR-S2.DSFD.0008.Spécifications_de_la_Brique_de_Collecte_des_Données_ENT.V07.00	DSFD
DR11	GAR-S2.DSFD.0006.Specifications_des_statistiques_et_rapports.V09.00	DSFD
DR12	GAR-S2.DSFD.0012.IHM_affectation.V08.00	DSFD
DR13	GAR-S2.DSFD.0013.IHM_portail_GAR.V09.00	DSFD
DR14	GAR-S2.DST.0001.Modèle de données annexes.V06.01	DST
DR15	GAR-S2.DSFD.0010.Processus_d_acces_aux_ressources.V10.00	DSFD
DR16	R.DSFD.0005.2.14.VA-Administration_du_GAR	DSFD
DR17	GAR-S2.DSFD.0011.Post_moissonnage.V06.00	DSFD
DR18	GAR-S2.DSFD.0025.SSO des IHM GAR.V07.00	DSFD
DR19	GAR-S2.DSFD.0014.Batch_d_import_ENT.V11.00	DSFD
DR20	R.NOE.0003.09.SV Matrice de notifications du GAR	NOE
DR21	R.NOE.0005.01.4.SV PLAN BATCH	NOE
DR22	GAR-S2.DSFD.0016.Purge_des_donnees_ENT.V03.00	DSFD
DR23	GAR-S2.DSFD.0017.Liste_etablissements.V02.00	DFSD
DR24	R.NOE.0001.1.24.SV Matrice de flux	NOE
DR25	R.NOE.0007.1.8.DR annexe plan d'adressage	NOE
DR26	R.DAT.0002.1.0.AV Plateforme GAR – Simulateur ENT	DAT
DR27	R.DSFD.0027.1.4.VA Conservation ID opaque	DSFD
DR28	GAR-S2.DSFD.0028.Spécification_du_WS_Ressources Affectées de l'Accédant(RAA).V01.05.docx	DSFD
DR29	GAR-S2.DSFD.0036.Site_De_Communication.V01.00	DSFD
DR30	GAR-S2.DAT.0003.Plateforme GAR – Annexe Inventaire PTF.V02.01.xlsx	DAT
DR31	GAR-S2.DSFD.0035.WS_Rapport_Affectation.V01.00	DSFD

DR32	GAR-S2.DSFD.0034.Batch_Suppression_Des_Comptes_Support.V01.00	DSFD
DR33	GAR-S2.DSFD.0038.Pré-Collecte.V01.00	DSFD
DR34	GAR-S2.DSFD.0040.WAYF NATIVES.V03.00	DSFD
DR35	GAR-S2.DSFD.0041.Interfaçage_SUMIT.V04.02	DSFD
DR36	GAR-S2.DSFD.0045.Lanceur manuel des batchs	DSFD
DR37	Procédure de PRA GAR Saison 2	PROC
DR37	GAR-S2.DSFD.0048.WS Décompte d'affectations.V02.00.docx	DSFD
DR38	GAR-S2.DSFD.0049.Batch Décompte d'affectations.V02.00.docx	DSFD

## 1.4 Autres documents utilisés

Numéro	Réf. Document
1	D07-2-Annexe 2 du Marche Subsequent n°2 – Cahier des charges du GAR.pdf

## 1.5 Abréviations

Abréviation	Signification
DAT	Dossier d'Architecture Technique
ENT	Espace Numérique de Travail
GAR	Gestionnaire d'Accès aux Ressources
MEN	Ministère de l'Education Nationale
WS	Web Service
VM	Virtual Machine
SMTP	Simple Mail Transfert Protocol – Protocole d'envoi de mail
SSO	Single Sign On – Gestion unifiée de l'identification
HDFS	Hadoop Distributed File System
IHM	Interface homme machine
CMS	Content Management System

## 1.6 Glossaire

Terme	Signification

Glossaire projet : <https://docs.renater.fr/pad/p/GARGlossaire>

## 2. Contexte

Le Gestionnaire des Accès aux Ressources (GAR) est l'une des plateformes de l'environnement national du plan numérique, annoncé par le Président de la République le 7 mai 2015.

Le GAR, est d'abord un cadre de confiance entre d'une part les acteurs de l'éducation Ministère, collectivités territoriales, académies, établissements et écoles, et d'autre part les acteurs du marché, industriels du numérique pour l'éducation.

Le GAR comprend deux volets :

- La fédération d'acteurs (« Fédération d'acteurs GAR »), pour le volet juridique, administrée par le Ministère, qui permet aux acteurs volontaires de s'engager comme membres en respect d'un ensemble de prérequis ;
- La solution GAR pour le volet technique, plateforme portant les services professionnels réservée aux membres de la fédération et aux responsables habilités des établissements. La plateforme filtre les données échangées (principe de proportionnalité) via un « hub » de connexions transparent pour les usagers finaux, élèves et enseignants, lors de l'accès à leurs ressources numériques pour l'éducation depuis tout type d'équipement.

La solution technique GAR a été confiée par le Ministère de l'Éducation Nationale et de l'enseignement supérieur et de la recherche au GIP Renater, le GIP apportant son expérience réseaux et fédération éducation recherche (FER).

### 3. Présentation générale de la solution GAR

La solution GAR mise en place par le Groupement permet de gérer les interactions avec les acteurs externes suivants (cf 1.6 Glossaire) que l'on peut regrouper en 2 catégories :

- Les acteurs qui accèdent au GAR ou qui alimentent le GAR :
  - Gestionnaire Administratif du GAR
  - Gestionnaire Technique du GAR
  - Distributeur commercial de ressources
  - Distributeur technique de ressources
  - Gestionnaire d'entrepôt OAI
  - Exploitant ENT
  - Responsables d'affectations et responsables délégués d'affectation
  - les équipes du Ministère pour l'alimentation des données (RDMEN) et l'interfaçage des guichets d'authentification
- Les accédants qui utilisent les services du GAR
  - Les élèves
  - Les enseignants
  - Les enseignants-documentalistes
  - Les autres personnels

On peut également citer les dispositifs suivants :

- Les entrepôts OAI
- Les sites distributeurs :
  - Les sites distributeurs techniques assurent l'hébergement et l'accès,
  - Les sites distributeurs commerciaux de ressources assurent uniquement la transmission des abonnements par WS
- Les projets ENT

Le diagramme suivant est un diagramme de contexte qui illustre les interactions entre le GAR et les acteurs externes (personnes ou systèmes)

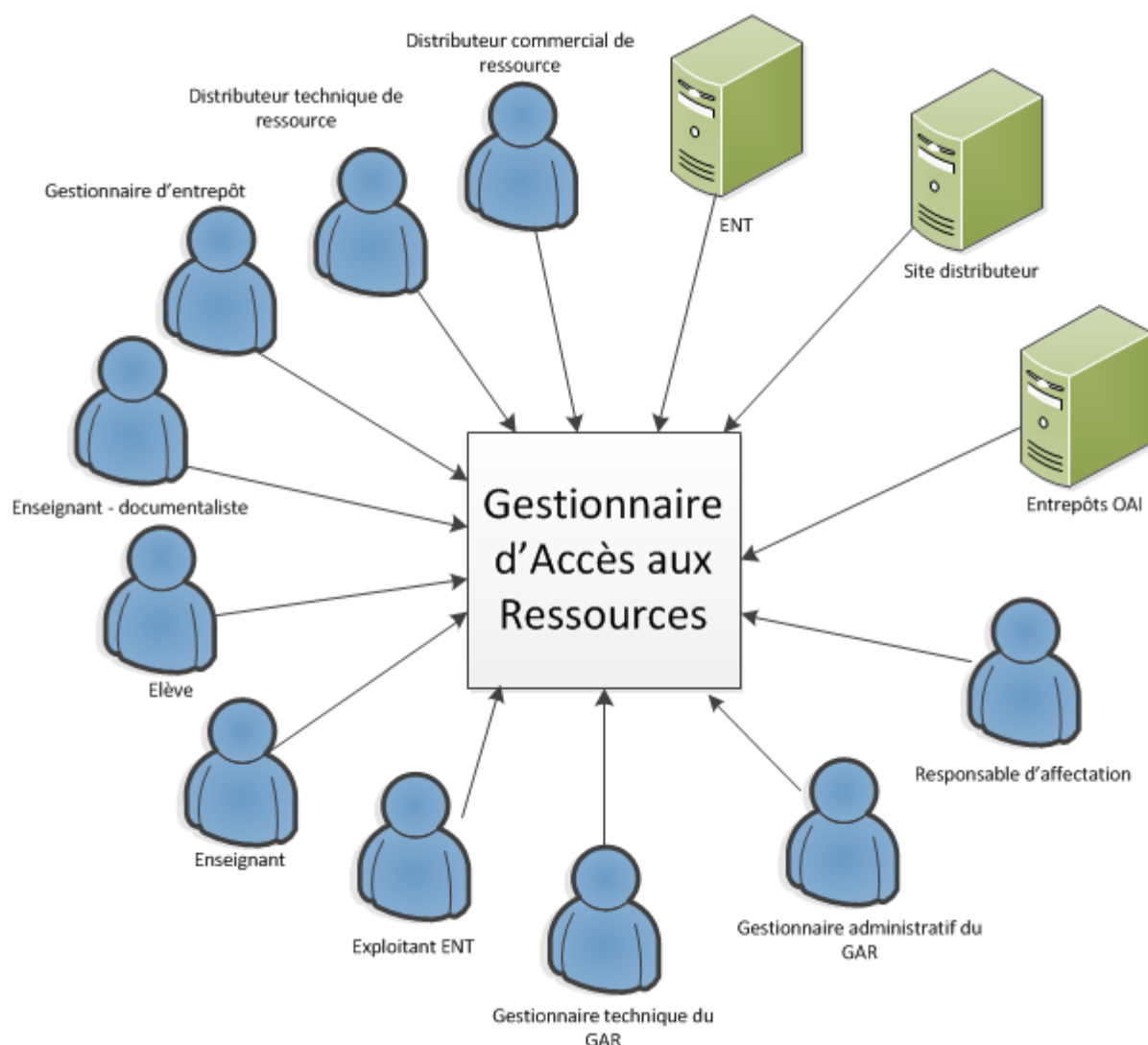


Figure 1 – Diagramme de contexte du GAR

Le GAR permet :

- La collecte des données ENT et académiques, permettant l'intégration dans le GAR de l'ensemble des identités ;
- Le moissonnage permettant l'importation des données des entrepôts de ressources ;
- La collecte des abonnements des éditeurs ;
- La gestion des affectations de ressources aux accédants par les responsables et les responsables délégués d'affectation ;
- L'accès aux ressources permettant de lister les ressources et de gérer la continuité du SSO entre ENT, GAR et distributeurs de ressources.
- la gestion des demandes de validation d'attributs, la consultation des abonnements, la gestion des propriétés du compte, la consultation des ressources diffusables, l'export des données et la consultation de statistiques au travers d'un portail.
- Une traçabilité des actions à travers les logs

Exigences et contraintes :

- **Accessibilité** : Les interfaces web développées dans le cadre du GAR, à savoir le Médiacentre GAR, le WAYF, le WAYF Natives, l'IHM d'affectation et le portail GAR, sont réputés respecter le RGAA en vigueur.

- Exigences de qualité de service : les exigences en qualité de service sont décrites dans le plan qualité gestion des services (cf. [DR4](#))

## 4. Architecture logicielle

### 4.1 Les composants du GAR

Le diagramme suivant présente l'ensemble des composants de la solution GAR et les interactions avec les différents acteurs :

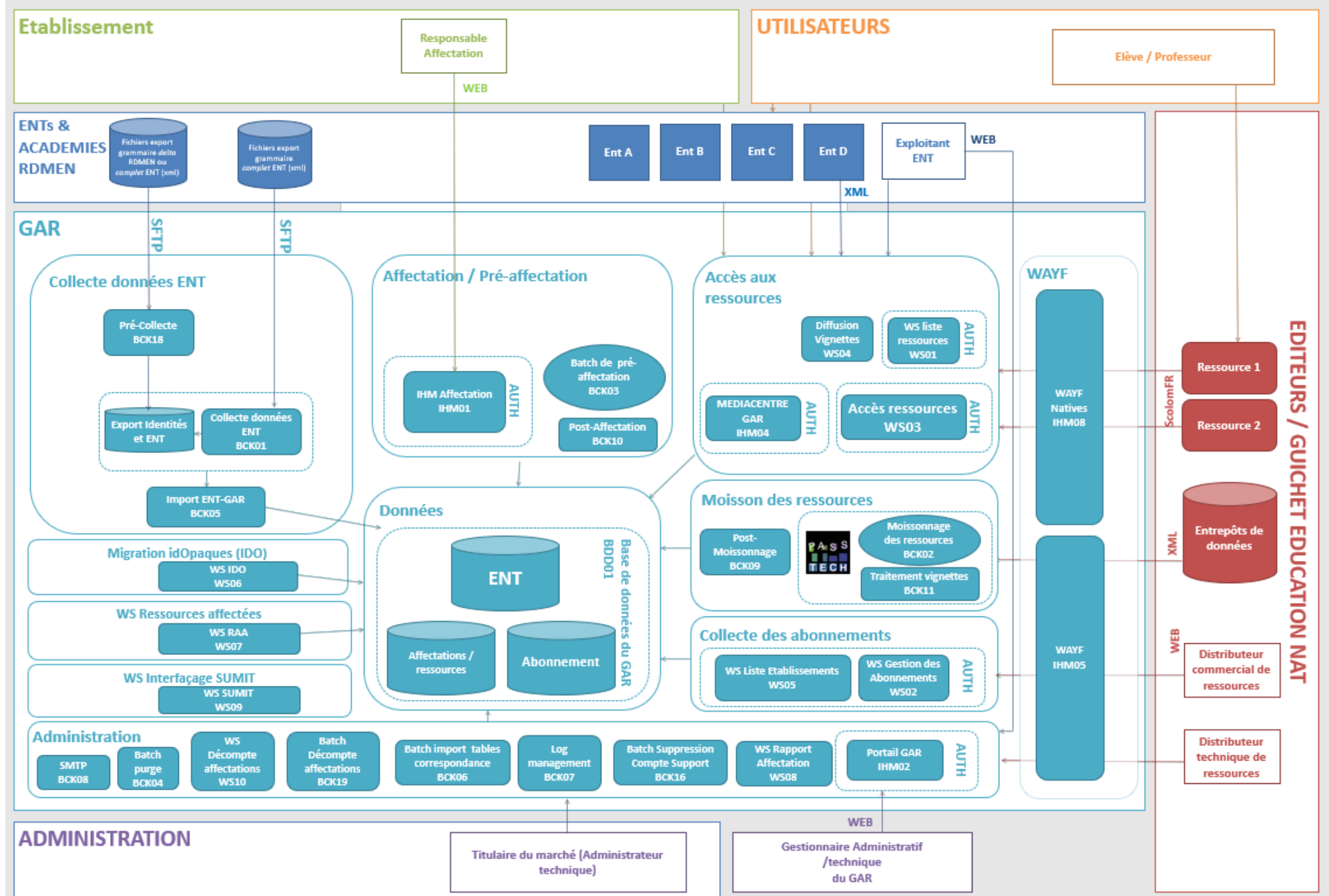


Figure 2 - Diagramme d'architecture du GAR



On retrouve notamment :

- Le composant de collecte des données ENT, permettant l'intégration dans le GAR de l'ensemble des identités ENT.
- Le composant de moissonnage, permettant l'importation des données des entrepôts de ressources.
- Le composant de collecte des abonnements, permettant aux éditeurs d'intégrer leurs abonnements dans le GAR.
- Le composant de gestion des affectations
- Le composant d'accès aux ressources, permettant de lister les ressources, de les présenter à l'utilisateur final via le Médiacentre GAR et de gérer la continuité du SSO entre ENT, GAR et distributeurs de ressources.
- Le composant WAYF, permettant d'articuler l'authentification auprès des services du GAR (IHM Affectations, Portail GAR et Médiacentre GAR, accès ressource) via la délégation auprès des guichets de l'Education Nationale et des ENT.
- Le portail GAR, regroupant l'ensemble des fonctionnalités d'administration et de suivi du GAR.

Ce découpage en composant fonctionnel permet de spécialiser les fonctions au sein d'un même ensemble cohérent (un module).

Chaque composant expose des services utilisés soit par des acteurs externes, soit par d'autres composants de la solution.

Cette architecture applicative a également été pensée dans une logique d'évolutivité de la solution afin d'intégrer plus facilement de nouveaux composants.

Les différents services composant le GAR sont listés dans le tableau ci-dessous :

REF	DESIGNATION	TYPE	PROTO	MISSION
BCK01	Collecte données ENT	Batch	SFTP	Collecter les données d'identité ENT déposées sur un serveur SFTP (cf DR10).
BCK02	Moissonnage des ressources	Batch	-	Moissonner les fiches ScoLOMFR des entrepôts OAI
BCK03	Batch de pré-affectation	Batch	-	Gérer les pré-affectations de ressources ainsi que les affectations automatiques (cf. DR8)
BCK04	Batch de purge	Batch	-	Purger les affectations et les abonnements (cf. DR16 et DR22)
BCK05	Batch import données ENT-GAR	Batch	-	Intégrer les données ENT du service d' « Import données ENT » dans les bases de données GAR (cf DR19)
BCK06	Batch import table correspondance	Batch	-	Batch d'intégration des tables de nomenclatures BCN dans le GAR (cf DR16)
BCK09	Post moissonnage	Batch	-	Batch permettant d'effectuer les traitements post moissonnage (gestion DCP, activation/désactivation affectations suite à une re-création/suppression d'une ressource) (cf DR17)
BCK10	Post affectation	Batch	-	Envoi de rapport aux distributeurs techniques de ressources (cfDR11)
BCK11	Traitement vignettes	Batch	-	Batch permettant la génération des vignettes GAR à partir des vignettes éditeurs des notices (cf DR9)
BCK12	Post import	Batch	-	Post import
BCK15	Confluence	IHM	HTTPS	Service confluence

REF	DESIGNATION	TYPE	PROTO	MISSION
BCK16	Batch de suppression des comptes support	Batch	HTTPS	Permet de désactiver, et supprimer les comptes support N1 non utilisés et expose un WS de réactivation
BCK18	Pré-Collecte	Batch	SFTP	Collecter les données d'identité RDMEN déposées sur un serveur SFTP au format Delta pour nourrir la Collecte au format Complet (cf <a href="#">DR33</a> ).
BCK19	Batch Décompte d'affectations	Batch	-	Décompte asynchrone en BDD GAR_AFFECT pour le WS Décompte affectations.
BDD01	Bases de données du GAR (Group replication)	SGBD	-	Bases de données du GAR (cf §4.8 Bases de données)
BDD02	Bases de données du GAR	SGBD	-	Bases de données du GAR (cf §4.8 Bases de données)
HTTP	service Nginx Reverse Proxy	Démon	HTTPS/SFTP	Fournir le service de reverse proxy.
IHM01	IHM Affectations	IHM	IHM	Gérer les affectations de ressources pour l'établissement. Accès authentifiés depuis les ENT. L'aide en ligne est hébergé par les serveurs supportant le service HTTP via un montage NFS.
IHM02	Portail GAR	IHM	HTTPS	Portail permettant la consultation des données du GAR (plus d'informations dans le DR13) Accès authentifiés CAS.
IHM03	Page de consentement	IHM	HTTPS	Page de consentement, pour signaler la sortie de la zone de confiance GAR.
IHM04	Médiacentre GAR	IHM	HTTPS	Présenter sur une interface à un accédant connecté via les guichets de l'Education Nationale les ressources numériques par établissement en exploitant les informations fournies par le wsListeRessources. Relayer l'accès à l'IHM Affectations pour les profils responsables d'affectations.
IHM05	WAYF (Where Are You From)	IHM	HTTPS	Rediriger l'utilisateur vers le guichet EN pertinent selon son profil et le service GAR auquel il veut accéder, via redirection directe ou, si nécessaire, présentation d'une interface de choix.
IHM06	Site de communication V2	IHM	HTTPS	Le site de communication gar.education.fr permet de communiquer sur ce qu'est le GAR et son actualité. Il repose sur le CMS WordPress adapté .
IHM07	Jira	IHM	HTTPS	Service JIRA pour la gestion des tickets de support et les demandes de service
IHM08	WAYF Natives	IHM	HTTPS	Interface de choix de l'établissement et du profil, permettant de rediriger l'utilisateur vers le bon guichet ou ENT pour l'authentification depuis la ressource (cf. <a href="#">DR34</a> )
REDIS	Stockage	SGBD	-	Assure le rôle de stockage des identifiants des accédants
SMTP	SMTP	Démon	SMTP	Serveur SMTP pour gérer l'envoi de notifications (cf §5.2.1)

REF	DESIGNATION	TYPE	PROTO	MISSION
<b>SQUID</b>	Proxy sortant	Démon	HTTP/HTTPS	Assure le service de relais des requêtes http/https des services
<b>STT01</b>	Log management	Batch	-	Système de gestion des logs et de statistiques (cf §5.2.2)
<b>WS01</b>	wsListeRessources	Webservice	REST	Lister les ressources disponibles pour un utilisateur. Accès authentifiés depuis les ENT.
<b>WS02</b>	wsGestionDesAbonnements	Webservice	REST	Gérer les abonnements des distributeurs (cf DR6). Accès authentifiés via certificats.
<b>WS03</b>	Accès Ressources	Webservice	HTTPS	Gérer l'accès à une ressource pour un utilisateur. Gérer l'authentification ENT-GAR-Distributeur (cf DR15)
<b>WS04</b>	Service de diffusion des vignettes GAR	Webservice	HTTP	Serveur http permettant de délivrer les vignettes GAR des ressources aux projets ENT (cf§5.2.4)
<b>WS05</b>	WS Liste des établissements	Webservice	HTTP	Service permettant la génération et la mise à disposition de la liste des établissements connus du GAR (cf DR23)
<b>WS06</b>	WS Migration IDOpaques	Webservice	HTTP	Assure les migrations des « uuid » permettant le recalculer un GarPersonIdentifiant identique pour le maintien post-purge année scolaire.
<b>WS07</b>	WS Ressources affectées à l'accédant	Webservice	HTTPS	Lister les ressources affectées à un accédants pour un DTR donné (cf. DR28)
<b>WS08</b>	WS Rapport Affectation	Webservice	HTTPS	Permet aux distributeurs techniques de ressources de lister, changer le statut et télécharger des rapports d'affectation
<b>WS09</b>	WS Interfaçage SUMIT	Webservice	HTTPS	Permet la communication entre JIRA et l'outil du support SUMIT.
<b>WS10</b>	WS Décompte d'affectations	Webservice	HTTPS	Liste les décomptes d'affectations pour un abonnement, un CPR et UAI donnés pour un DCR authentifié.

## 4.2 La solution logicielle

Le diagramme suivant présente l'architecture logicielle de la solution GAR :



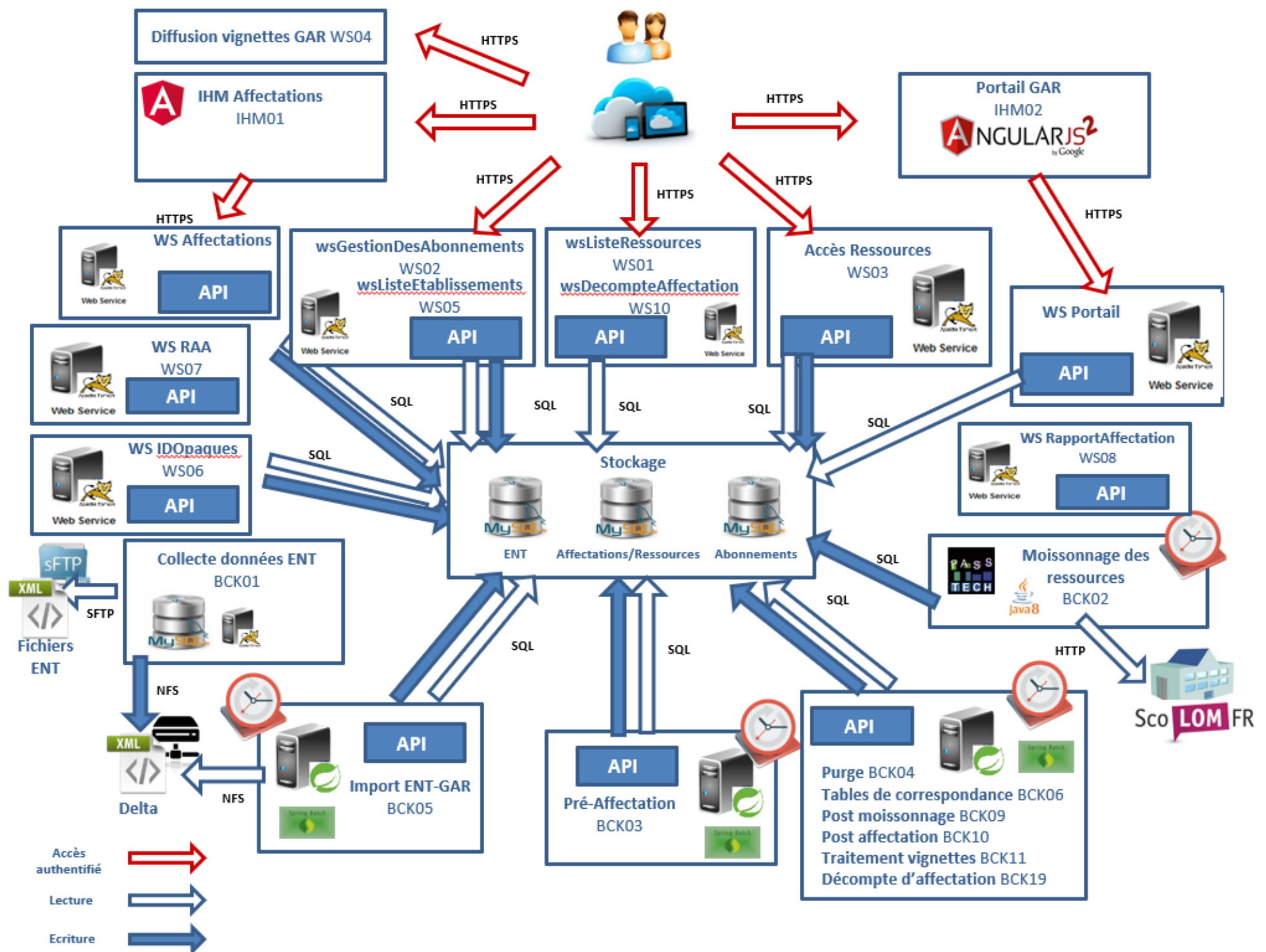


Figure 3 – Diagramme d'architecture logicielle du GAR

## 4.2.1 Socle API

### 4.2.1.1 Définition

Chaque application embarque un socle commun (sous forme de jars), qui permet l'accès aux données GAR dont elle a besoin.

Pour chaque source de données (ENT, Affectations/Ressources, Abonnements et autres), le socle se découpe en 3 modules distincts (donc 3 jars):

- **Module Contract** (Interfaces) :  
Il permet de définir les contrats d'échanges entre les applications et les données GAR. C'est par ces interfaces que les appels au socle sont réalisés.
- **Module Service** :  
Il contient l'implémentation des interfaces du module Contract. C'est lui qui fournit les traitements métiers associés aux contrats d'échanges. Ce module gère les aspects transactionnels. Ce module est embarqué par les applications mais elles n'y ont pas accès directement.
- **Module Data** :  
Il définit les modèles d'objets ainsi que leurs méthodes d'accès, utilisables par les traitements métiers. Cette couche est utilisée par le module Service pour accéder à la base de données. Et comme ce dernier, le module Data est embarqué pour l'exécution des traitements, mais n'est pas accessible nativement par les applications.

Ce découpage permet un cloisonnement plus fin de l'application. Ce qui la rend plus évolutive et plus maintenable. On peut facilement modifier la couche Data ou Service en s'assurant de ne pas impacter le contrat d'échange avec les applications.

Le schéma suivant représente le découpage modulaire pour les 3 sources de données :



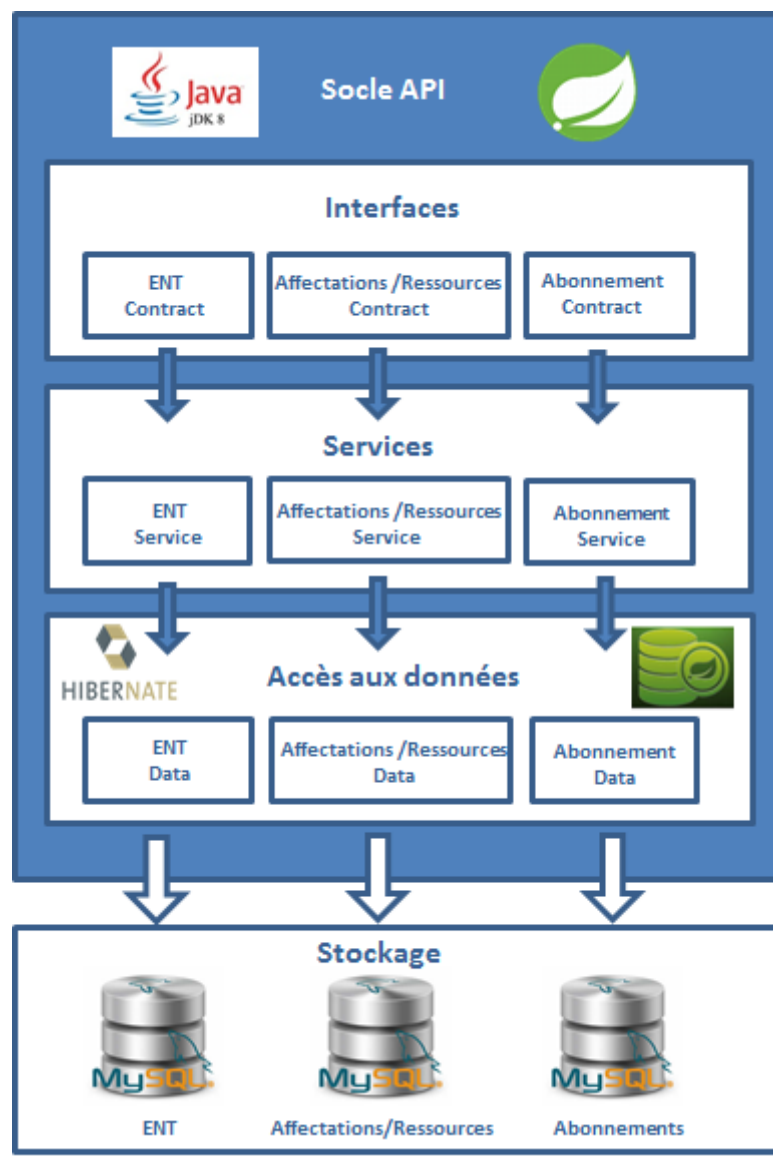


Figure 4 – Découpage des modules

#### 4.2.1.2 Technologies

Ce socle applicatif est basé sur **Spring Framework**. C'est la couche applicative de base de l'écosystème Spring. Elle permet la gestion des interdépendances par injection, l'implémentation de services REST et le câblage des différents modules de la suite logicielle.

**Maven** est utilisé pour la gestion des dépendances et le packaging des projets.

L'accès aux bases de données se fait via la suite d'API **Spring Data**, en particulier **spring-data-jpa**. Basé sur **Hibernate** et **JPA** pour le mapping d'objets et les requêtes, ce module permet l'adressage rapide de bases de données MySQL.

### 4.2.2 Batches

Les différents batches (hors « Log management ») utilisent le framework **Spring Batch**. Il prend en charge le cycle de vie des batches (démarrage/arrêt/redémarrage/erreur/reprise), offre des possibilités de parallélisation, le tout administrable via IHM (Spring Batch Admin).

Ils utilisent les couches d'accès bases de données décrites ci-dessus.

Le scheduler natif de Spring est utilisé pour ordonnancer l'ensemble des batches Spring du GAR.

### 4.2.3 Web Services REST

Réalisés sur base de **Spring Framework**, on leurs adjoint une couche de configuration basée sur **Spring Boot**, qui les rend production-ready (métriques, indicateurs de santé...). Ils utilisent les couches d'accès bases de données décrites ci-dessus.

### 4.2.4 IHM

Les technologies utilisées pour les IHM sont :

- (1) HTML5
- (2) CSS 3 (pure CSS 0.6.0)
- (3) JavaScript (IHM d'Affectation et Portail GAR : Angular version 11 / Médiacentre GAR et WAYF : Angular version 12 / WAYF Natives : Angular 14 / Lanceur de batch : Angular 17)

Les IHM se basent sur des Web Services REST qui fournissent l'ensemble des méthodes métier.

### 4.2.5 Module d'accès aux ressources

#### 4.2.5.1 Lien ENT - GAR

La partie « fournisseur de service » du module d'accès aux ressources du GAR se base sur le serveur open source CAS d'Apereo et l'utilisation de la bibliothèque open source pac4j pour la gestion du protocole SAML2 et OIDC.

Le stockage des informations d'authentification se fait dans une base redis. Le serveur web utilisé est un serveur Nginx, le conteneur de servlets Apache Tomcat.

Concernant le protocole SAML 2.0, les profils suivants sont implémentés au niveau de la partie « fournisseur de service » (cf. DR15) :

- **Web Browser SSO Profile** en utilisant le binding **HTTP Redirect**.
- **Single Logout Profile** en utilisant le binding **SOAP ou HTTP POST**.

#### 4.2.5.2 Lien GAR - DTR

La partie « fournisseur d'identité » du module d'accès aux ressources du GAR se base sur le serveur open source CAS d'Apereo qui permet de gérer au sein du même service les protocoles CAS, OIDC et SAML2 pour les ressources WEB et OIDC pour les applications natives.

Le serveur web utilisé est Nginx, le conteneur de servlets utilisé est Apache Tomcat.

Concernant le protocole SAML 2.0, le profil suivant sera géré au niveau de la partie « fournisseur d'identité » (cf. DR15):

- **Web Browser SSO Profile** en utilisant les bindings **HTTP Redirect** et **HTTP POST**.
- **Single Logout Profile** en utilisant le binding **SOAP**.

En particulier pour l'OIDC :

- dans le cas d'une variante native de ressource, le mode d'accès authorization code flow avec PKCE (Proof Key for Code Exchange) est implémenté,
- dans le cas d'une variante web de ressource, le mode d'accès authorization code flow est complété d'un secret obligatoire et de l'extension PKCE optionnelle.

#### 4.2.5.3 Gouvernance des Métadonnées SAML2

Ce paragraphe décrit la manière dont sont gérés les échanges des fichiers de métadonnées SAML2.

##### 4.2.5.3.1 Métadonnées des projets ENT

Le GAR doit posséder les métadonnées de chaque projet ENT avec lesquels il échange.

La récupération/mise à jour de ces métadonnées est faite via l'URL fournie par chaque projet ENT lors de l'accrochage au GAR (cf. [DR16](#)).

Le mécanisme est décrit dans le document de référence [DR15](#).

##### 4.2.5.3.2 Métadonnées des ressources

L'authentification des ressources auprès du GAR se fait en SP-initiated, le GAR doit donc posséder les métadonnées de chaque ressource implémentant le protocole SAML2.

Comme pour les ENT, la récupération se fait via une url fournie lors de la déclaration des éditeurs (cf. [DR16](#)). Cette URL pointe vers le fichier métadonnées agrégées contenant les métadonnées de toutes les ressources gérées par cet éditeur par le DTR, pour le compte du ou des éditeurs (ou du SP qui gère l'authentification des ressources s'il est commun pour plusieurs ressources).

Le mécanisme est décrit dans le document de référence [DR15](#).

##### 4.2.5.3.3 Caractéristiques communes pour les projets ENT et les ressources

Le service d'accès aux ressources, autant la partie SP pour les projets ENT que la partie IDP pour les fournisseurs de ressource, exploite l'attribut « date de validité » défini dans le fichier de métadonnées pour se mettre à jour vis-à-vis des métadonnées périmées.

La vérification des certificats SSL utilisés pour récupérer les métadonnées se fait en regard des AC packagées et maintenues à jour par CentOS.

En cas de détection d'attaque, il est possible de révoquer rapidement un projet ENT ou une ressource (via demande de service).

Un mécanisme de vérification manuelle de l'auteur de la demande est mis en œuvre pour s'assurer de la légitimité de la personne qui communique les informations au moment de l'accrochage via une demande de support. De plus, les informations communiquées doivent être conformes au PAS (cf. [DR1](#)) et aux politiques de Sécurité Opérationnelle (cf. [DR2](#)) définies.

#### 4.2.5.3.4 Métadonnées du GAR

Le GAR présente également ses métadonnées, via une URL sécurisée, à destination des projets ENT, des guichets d'authentification (ENT EduGAR) et des ressources avec lesquels il échange.

Ces métadonnées du GAR n'ont pas vocation à être modifiées fréquemment pour les raisons suivantes :

1. La relation du GAR avec les différents intervenants se fait en 1-1, l'ajout ou le retrait d'un projet ENT ou d'une ressource au niveau du GAR n'a pas d'impact sur les métadonnées du GAR.
2. Au niveau de l'accès aux ressources, les attributs DCP disponibles pour une ressource ne sont pas déclarés dans le fichier de métadonnées. En effet, la gestion des attributs fournis aux ressources lors de l'accès à celles-ci est portée par le post-moissonnage et par le portail GAR. C'est via ces 2 services qu'est validée la liste des attributs qui sont fournis aux ressources. Il n'est donc pas nécessaire de faire apparaître la liste des attributs demandés dans les métadonnées des ressources. Cette liste ne serait pas prise en compte par le GAR car seule la validation des données DCP via le portail GAR ou le post moissonnage fait foi.

Les seules mises à jour identifiées pour ces métadonnées sont :

- Liées à l'actualisation du certificat.
- Liées à l'action de l'administrateur technique du GAR lorsque l'exploitant ENT ou le point de contact EduGAR le demande via une demande de support.

Des mises à jour de ces métadonnées sont néanmoins publiées fréquemment pour palier le risque de révocation de certificat.

Les métadonnées des partenaires SAML et OIDC du GAR publiées ont une durée de validité paramétrable (positionnée à 7 jours par défaut), en deçà de cette durée un cache des métadonnées est interrogé lors des appels des fournisseurs de ressources pour récupérer les métadonnées.

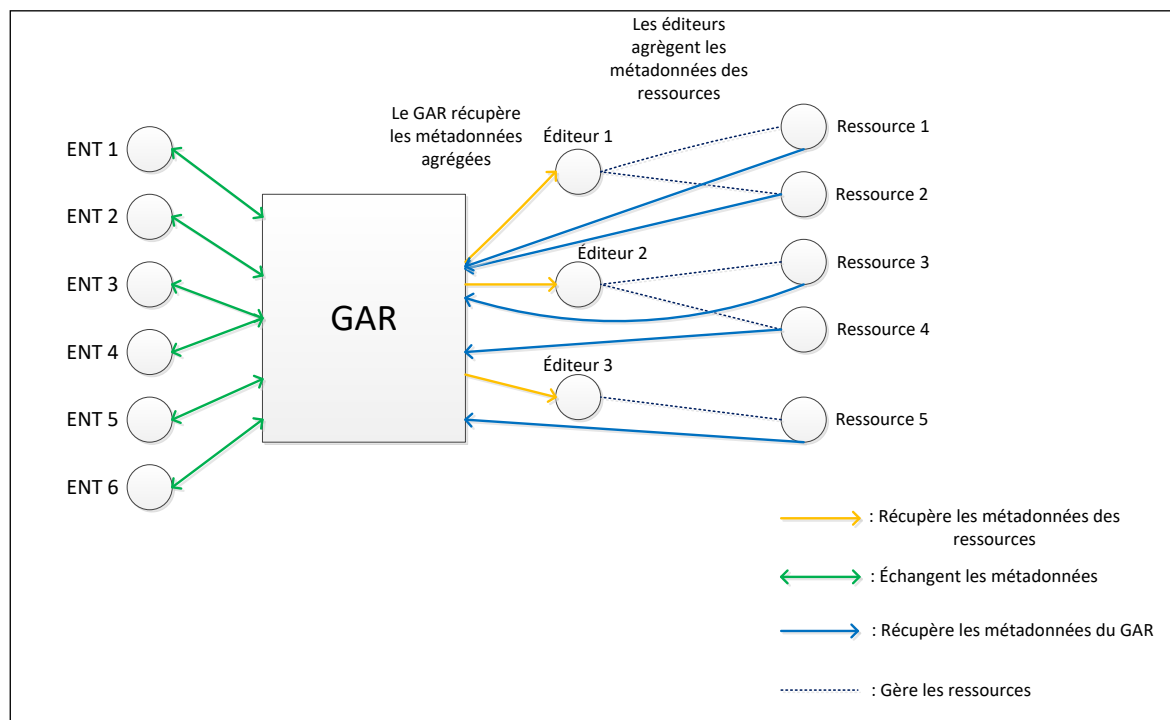
Après cette échéance, les IdP des projets ENT et les SP des ressources devront actualiser la copie locale du fichier de métadonnées du GAR.

La mise en cache des métadonnées des partenaires est réalisée si les contrôles de validité de ces métadonnées sont vérifiés.

Dans le cas où les métadonnées ne sont pas valides ou pas disponibles et présentes en cache :

- un mail sera envoyé au support GAR, au GT et à l'exploitant ENT ou au point de contact EduGAR (pour les guichets d'authentification) concerné pour les informer du problème.
- Un incident sera ouvert et Worldline sera en capacité de forcer la récupération d'une nouvelle version du fichier.
- Au-delà de 7 jours d'invalidité ou d'indisponibilité, les métadonnées seront supprimées du cache.

Voici un schéma présentant l'échange des métadonnées dans le cadre du GAR :



#### 4.2.5.3.4.1 Notifications

Dans le cas où les métadonnées ne sont pas valides ou pas disponibles et présentes en cache, un mail est envoyé au support GAR, au GT et à l'exploitant ENT ou au point de contact EduGAR (pour les guichets d'authentification) concerné pour les informer du problème.

Les adresses utilisées pour l'envoi de notifications sont :

- Pour l'exploitant ENT et le point de contact EduGAR, les adresses de responsables du projet ENT (académique ou non académique en fonction du cas concerné) définies dans la table projet\_ent
- Pour le point de contact EduGAR (pour les guichets d'authentification), les adresses sont fournies par RENATER et celles-ci seront stockées en base de données dans un nouveau champ de la table projet\_ent

Pour le GT, les adresses de contacts indiqués dans les profils de type gestionnaire technique.

## 4.2.6 Module de moissonnage des ressources

Le module de moissonnage est un exécutable Java en ligne de commande, qui peut être appelé directement ou via une tâche planifiée (cron).

Le module, pour fonctionner, nécessite :

- une machine virtuelle Java `jre_11_openjdk`
- un accès HTTP(s) vers l'extérieur pour la moisson des entrepôts OAI
- un accès à un serveur SMTP pour l'envoi de notifications
- l'accès en écriture à un dossier sur le disque pour la génération de logs (exploitation et statistiques)
- l'accès à une base de données MySQL en lecture / écriture pour :
  - lire et mettre à jour les informations de configuration des entrepôts à moissonner
  - sauvegarder les données moissonnées validées
  - lire les tables de référence GAR (pour la validation des données moissonnées)

Le module utilise :

- la brique logicielle OCLC de moisson OAI (version 2.11)
- la bibliothèque Java Hibernate pour assurer la persistance et l'accès aux données.
- la bibliothèque Log4j pour la production de logs

Les données relatives au ScoLOMFR 3.0/4.0/4.1/5.0/6.0/7.0/8.0/9.0 (schéma XSD et vocabulaires) utiles à la validation des données moissonnées sont présentes sous forme de fichiers de ressource fournis avec le module.

La configuration du module s'effectue dans un fichier de paramétrage à l'extérieur du module.

## 4.2.7 Module Import données ENT.

Ci-dessous une présentation de l'architecture des composants nécessaires pour le module d'import des données ENT.

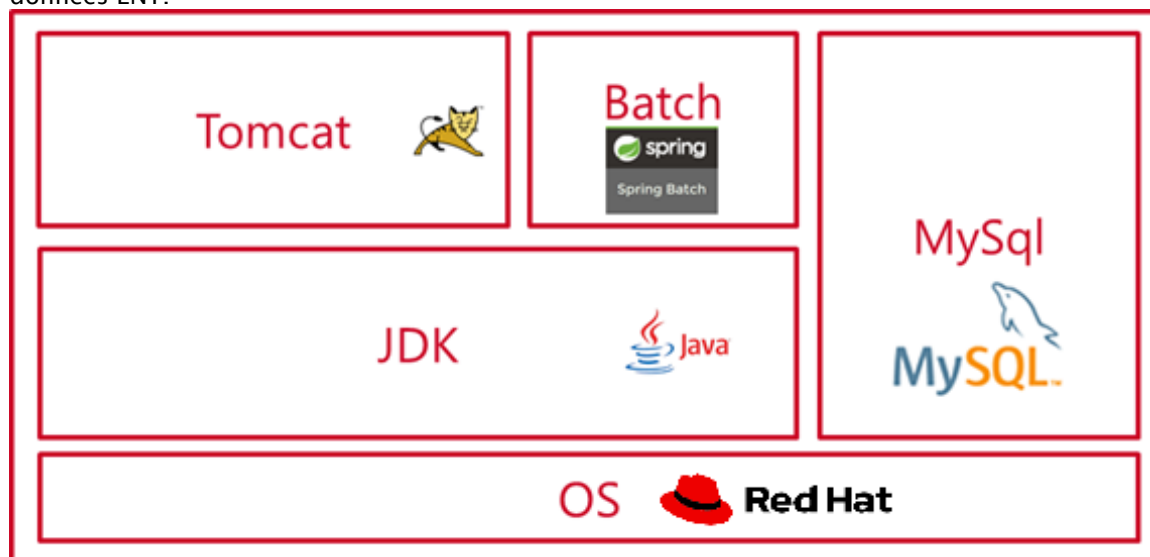


Figure 5 - Architecture des composants de la brique Import ENT

Les principaux composants et leurs fonctions sont listés ci-dessous :

- Conteneur de servlets Tomcat : il assure l'hébergement et l'exécution de la Brique de Collecte des Données ENT (code source compilé, fichiers de paramétrage, ...) qui permet le traitement des demandes de service ;
- SGBD MySQL: il assure l'hébergement des données de la Brique de Collecte des Données ENT, dont le stockage est réalisé par une base de données pour le fonctionnement de la Brique ainsi qu'une base de données par source ENT pour les imports de leurs données.
- Spring Batch : composant technique avec lequel sont implémentés les différents traitements de la Brique de Collecte des Données ENT du GAR ;

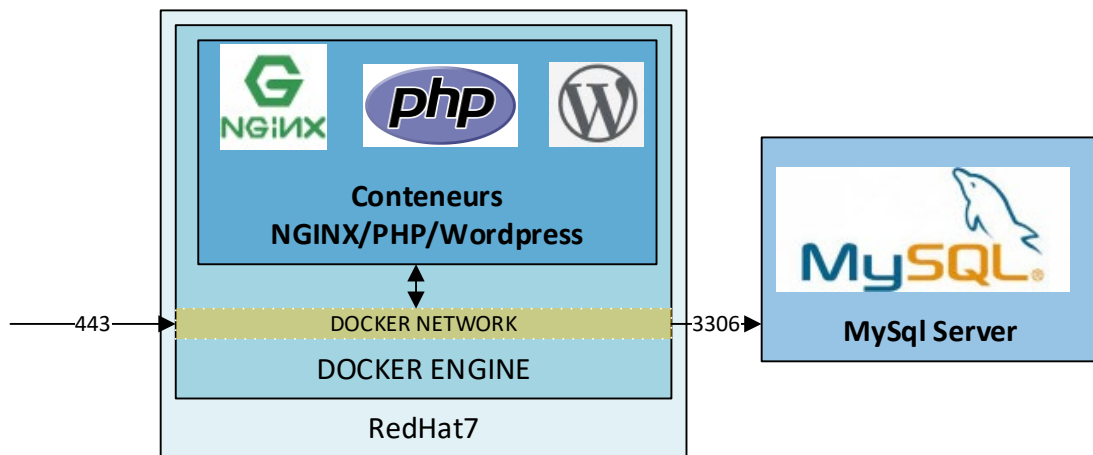
- Serveur de fichier : il assure l'hébergement et le stockage des fichiers utilisés par la Brique de Collecte des Données ENT. Le protocole d'accès aux fichiers recommandé est le NFS.

## 4.3 Site de communication GAR

### 4.3.1 Solution technique

La solution technique repose sur le CMS open source Wordpress. La partie métier repose sur le moteur PHP et s'appuie sur deux types de stockage : un back-end BDD (Mysql) pour le stockage des contributions éditoriales, et un espace disque dédié au stockage des médias et des fichiers de configuration propres aux environnements de déploiement.

Ci-dessous une présentation de l'architecture des composants de la solution.



Versions utilisées pour chaque composant :

Composant	Version	Description
PHP	8.0.29	Librairie PHP
MySql	8.0.26	SGBD
NGINX	1.16.1	Serveur front d'application
Wordpress	6.2.2	CMS
Docker	1.13.1	Moteur de virtualisation (OS- Level)
ClamAV	0.103.5	Antivirus

### 4.3.2 Infrastructure d'hébergement

Deux environnements hébergent le site de communication GAR :

Environnement de qualification (composé d'une machine virtuelle Front et d'un schéma de base de donnée back hébergée sur une autre machine virtuelle).

Environnement de production (composé d'une machine virtuelle Front et d'un schéma de base de donnée back hébergée sur une autre machine virtuelle).



#### 4.3.2.1 Environnement de qualification :

Le site de communication GAR de l'environnement de qualification est accessible via l'URL <https://site2com.integration.test-gar.education.fr>.

Serveur	IP Publique	IP Privée	Port publique	Port privé	Protocole
wiren52s	195.221.81.125	10.35.103.23	443/80	443/80	https/http

#### 4.3.2.2 Environnement de production :

Le site de communication GAR de l'environnement de production est accessible via l'URL <https://gar.education.fr>

Serveur	IP Publique	IP Privée	Port publique	Port privé	Protocole
wpren52s	195.221.81.17	10.43.0.18	443/80	443/80	https/http

## 4.4 Service support GAR (Jira)

Le service support GAR est un outil de ticketing qui permet aux utilisateurs finaux de demander des informations et une assistance à l'utilisation de la solution GAR. Il permet également des échanges entre les gestionnaires du GAR pour la mise en place d'améliorations et de corrections des services. Le service se base sur la solution Jira Service Management.

### 4.4.1 Infrastructure d'hébergement

#### 4.4.1.1 Environnement de préproduction

Le service support GAR de l'environnement de qualification est accessible via l'URL <https://support.pp.test-gar.education.fr/>.

IP Publique	IP Privée	Port publique	Port privé	Protocole
195.221.81.88	10.35.100.228	443/80	443/80	https/http

#### 4.4.1.1 Environnement de production

Le service support GAR de l'environnement de production est accessible via l'URL <https://support.gar.education.fr/>.

IP Publique	IP Privée	Port publique	Port privé	Protocole
195.221.81.11	10.43.0.213	443/80	443/80	https/http

## 4.5 WS Interfaçage SUMIT/Agent GAR

L'interfaçage entre l'application de support académique SUMIT ACA (ITOP) et le support GAR a pour but de mettre en place un système automatisé d'échange de tickets de support sous la forme d'un service hébergé sur un serveur GAR.

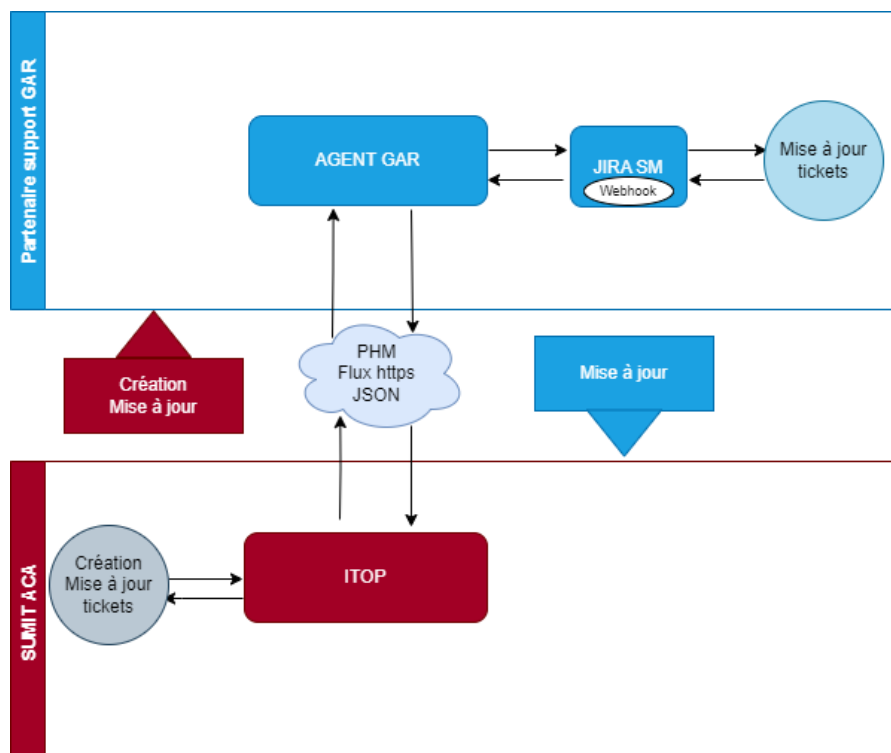
L'objectif de l'interfaçage est l'harmonisation des outils de gestion et de support et aussi celui d'une amélioration du quotidien des académies (partenaires du GAR) dans le suivi de leurs demandes de support.

### 4.5.1 Solution technique

Pour pouvoir utiliser le web service d'interfaçage SUMIT, le partenaire doit fournir une liste d'adresses IP autorisées qui seront configurées.

Une fois toutes les conditions préalables remplies, le partenaire peut faire usage de l'ensemble des méthodes exposées par le service dans le respect des contraintes et règles de gestions en vigueur.

Les spécifications détaillées sont disponibles dans le document référencé [DR35](#).



## 4.5.2 Infrastructure d'hébergement

### 4.5.2.1 Environnement de préproduction

Le service Interfaçage SUMIT de l'environnement de qualification est accessible via l'URL <https://interfacage-sumit.pp.test-gar.education.fr>.

IP Publique	IP Privée	Port publique	Port privé	Protocole
195.221.81.93	10.35.101.232	443	443	https

### 4.5.2.2 Environnement de production

Le service Interfaçage SUMIT de l'environnement de production est accessible via l'URL <https://interfacage-sumit.gar.education.fr>.

IP Publique	IP Privée	Port publique	Port privé	Protocole
195.221.81.27	10.43.0.229	443	443	https

## 4.6 Module migration des idOpaques

Ce WS a pour vocation de permettre à un accédant du GAR de conserver ses identifiants opaques vis-à-vis des ressources quels que soient les changements d'ENT qu'il subit.

Cet identifiant est construit à partir de l'uuid et l'id ressource par un algorithme à sens unique lors des affectations aux différentes ressources.

Sur demande d'un ENT cible via la transmission au GAR d'un fichier de mapping contenant le GarPersonIdentifiant sur l'ENT source et le GarPersonIdentifiant importé dans l'ENT cible, le GAR pourra transférer l'uuid d'un individu de l'ENT source vers l'ENT cible.

Après ce transfert, les affectations faites pour l'individu associeront au GarPersonIdentifiant cible le même idOpaque que celui auquel était associé le GarPersonIdentifiant source pour la même ressource.

Les spécifications détaillées sont disponibles dans le document référencé DR27.

## 4.7 WS Ressources affectées à l'accédant

Ce web service a pour objectif de permettre à un distributeur technique de ressource connu du GAR d'obtenir la liste des identifiants des ressources du périmètre de ce DTR affectées à un accédant identifié par son IDO.

Pour pouvoir utiliser le web service de récupération des Ressources Affectées de l'Accédant (RAA), le DTR doit au préalable :

- Avoir été déclaré dans le GAR
- Et, pour un accès par Access Token
  - Avoir obtenu un Access Token suite à un accès d'un utilisateur à une de ses ressources
- Ou, pour un accès par certificat
  - Avoir un certificat X509 valide (voir DR1)
  - Avoir l'identifiant du certificat renseigné au niveau du GAR

Une fois toutes les conditions préalables remplies, le DTR peut faire usage de l'ensemble des méthodes exposées par le service dans le respect des contraintes et règles de gestion en vigueur.

Les spécifications détaillées sont disponibles dans le document référencé [DR28](#).

## 4.8 WS Rapport d'Affectation

Ce web service a pour objectif de permettre à un distributeur technique de ressources connu du GAR d'obtenir la liste de ses rapports d'affectation delta et complet sur la base de son idDistributeur.

Ce web service permet aussi à un DTR de changer le statut de référence d'un rapport delta et de télécharger un rapport d'affectation delta ou complet sous format xml dans un fichier zip, via le nom du rapport.

Pour pouvoir utiliser le web service de Rapport d'Affectation, le DTR doit au préalable :

- Avoir été déclaré dans le GAR
- Avoir un certificat X509 valide
- Avoir l'identifiant du certificat renseigné au niveau du GAR

Une fois toutes les conditions préalables remplies, le DTR peut faire usage de l'ensemble des méthodes exposées par le service dans le respect des contraintes et règles de gestion en vigueur.

Les spécifications détaillées sont disponibles dans le document référencé DR31.

## 4.9 WS Décompte d'Affectations (et Batch)

Ce web service a pour objectif de permettre à un distributeur commercial de ressources connu du GAR d'obtenir le décompte d'affectations réalisées par public cible, sur chacun des abonnements qu'il administre.

Pour pouvoir utiliser le web service Décompte d'Affectations, le DCR doit au préalable :

- Avoir été déclaré dans le GAR
- Avoir un certificat X509 valide
- Avoir l'identifiant du certificat renseigné au niveau du GAR

Une fois toutes les conditions préalables remplies, le DCR peut faire usage du service dans le respect des contraintes et règles de gestion en vigueur.

Le WS Décompte d'Affectations se base sur les données générées de façon asynchrone par le batch Décompte d'Affectations.

Les spécifications détaillées du WS et du batch associé sont disponibles dans les documents référencés DR37 et DR38.

## 4.10 Simulateur ENT

Le Simulateur est un projet contenant plusieurs applications, l'application Springboard ainsi que l'application Mediacentre.

Le springboard, application mère basée sur la solution ENT open source OPENENTNG permet l'import et la gestion d'utilisateurs et d'établissements.

Le mediacentre est un module imbriqué dans le springboard et permet l'affichage des ressources GAR pour l'utilisateur connecté.

### 4.10.1 Présentation générale de la solution Simulateur

Le Springboard est une application JAVA embarquant de nombreuses dépendances notamment l'ENT-CORE et Vertx qui sont les principales dépendances permettant le bon fonctionnement des autres dépendances intégrées. Il est la brique principale, le portail de l'OPEN ENT NG, celui-ci permettant le lancement et l'intégration de l'ENT et de ses différents modules. Il embarque une interface utilisateur basée sur un template appelé LEO / DYSLEXIC développé en HTML et JAVASCRIPT à l'aide de AngularJS et des librairies front ent-core développées par Opendigitaleducation.

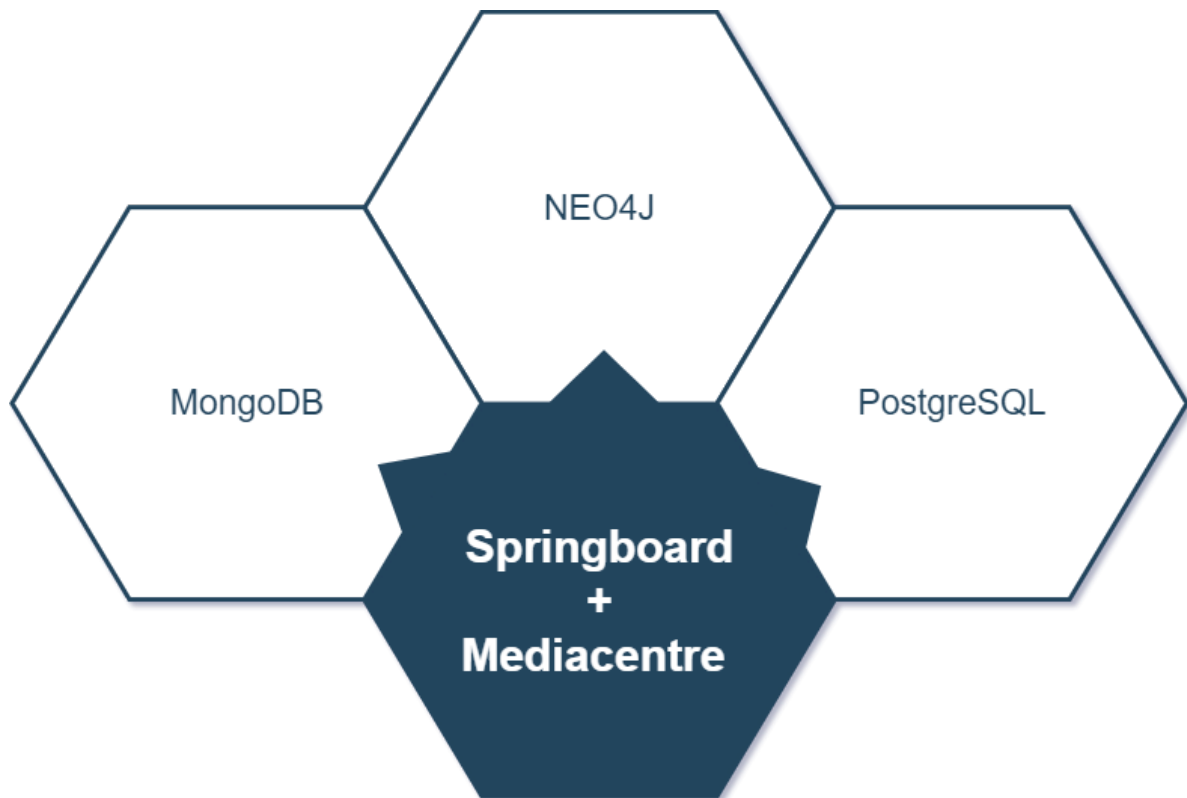
Le Mediacentre est une application Java de type module. Ce module est ajouté aux dépendances du Springboard afin que celui-ci puisse être intégré, interprété et lancé en tant qu'application par le serveur web Vertx.

Il peut être intégré dans le springboard par plusieurs moyens

- Par un repository distant ou local si celui-ci y est publié
- Par un ajout des fichiers java dans le dossier mods du springboard, ceux-là peuvent être récupérés par une décompression d'un .jar-fat généré lors d'un build shadowjar de l'application par gradle.

#### 4.10.2 Les composants du Simulateur

Le diagramme suivant présente l'ensemble des composants de la solution Simulateur et les interactions avec les différents acteurs :



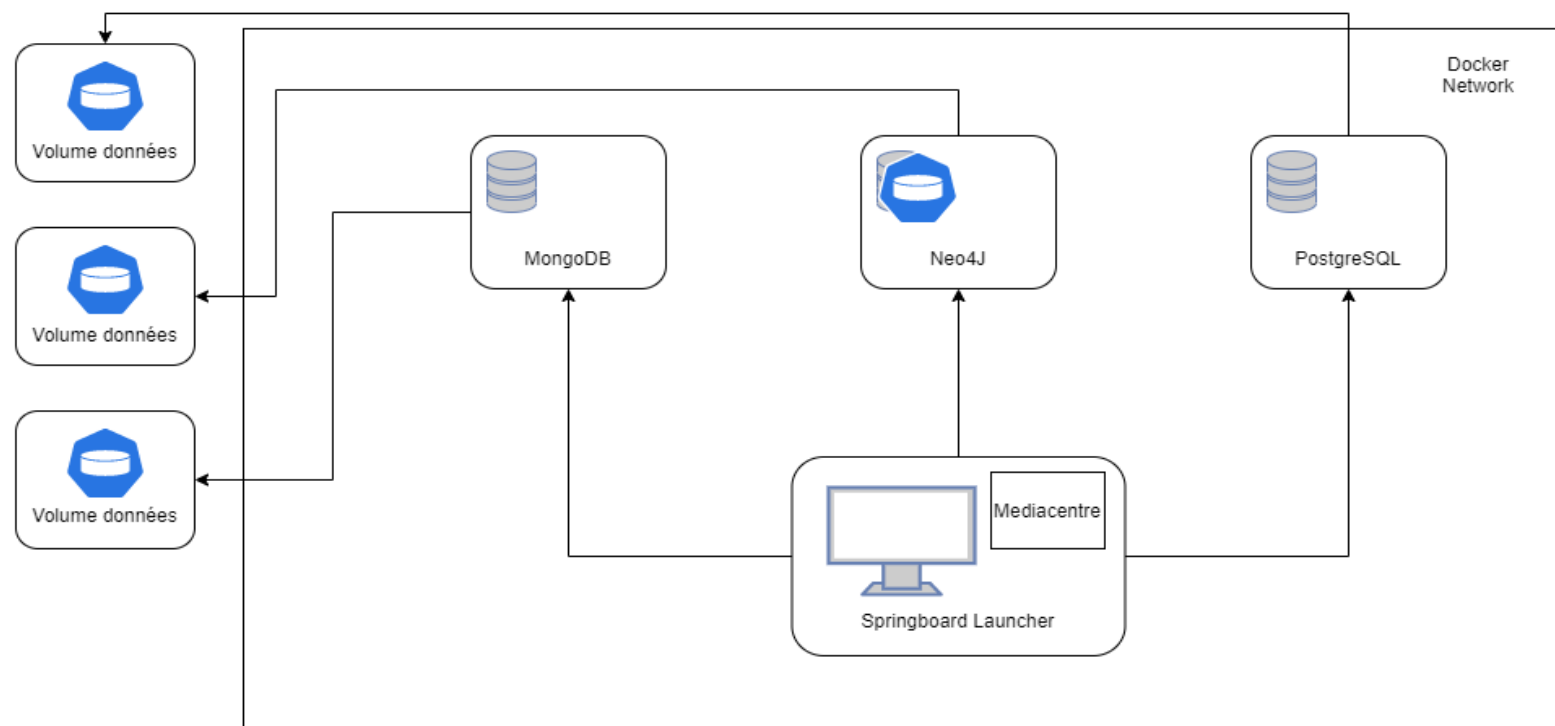


Figure 6 – Diagramme d'architecture de l'image du Springboard lancé avec docker

Base	Moteur	Version	Description
Springboard	Neo4j	3.1	Référence l'ensemble des données utiles du Springboard
	PostgreSQL	9.5	
	MongoDB	3.6	

On retrouve notamment :

- La base de données orientée graph NEO4J. Celle-ci est la base de données principale dont nous nous préoccuperons, car c'est cette base de données qui est utilisée principalement par le Mediacentre et le Springboard.
- La base de données PostgreSQL, celle-ci est nécessaire au bon fonctionnement du springboard et de ses dépendances mais n'est pas spécifiquement utilisée par notre périmètre.
- La base de données Mongoddb, celle-ci est nécessaire au bon fonctionnement du springboard et de ses dépendances mais n'est pas spécifiquement utilisée par notre périmètre.
- Le springboard Launcheur, une image docker permettant le lancement de l'application Springboard à l'aide du serveur web VERTX

#### 4.10.2.1 Technologies

Ce socle applicatif est basé sur **La solution JAVA Open ENT NG**. L'ENT CORE développé par son éditeur opendigitaleducation est la couche applicative de base de l'écosystème Springboard.

**Gradle et Maven** est utilisé par l'application pour la gestion des dépendances et le packaging des projets.

Ils utilisent les couches d'accès bases de données décrites ci-dessus.

#### 4.10.2.2 IHM

Les technologies utilisées pour les IHM sont :

- (4) HTML5
- (5) CSS 3 (pure CSS 0.6.0)
- (6) JavaScript (AngularJS)

#### 4.10.2.3 Bases de données

Les différentes bases de données sont listées dans le tableau ci-dessous.

Base	Moteur	Version	Description
graph.db	Neo4j	3.1	Référence l'ensemble des données du simulateur

Chaque base dispose d'une série de login/mdp selon les environnements et selon les types d'accès (lecture seule, lecture écriture).



#### 4.10.2.4 Architecture applicative

#### 4.10.2.5 OPEN JDK 8

Les nouvelles versions du springboard et du mediacentre seront basées sur la version 8 de Java en intégrant la version open source OPENJDK-8, cette version sera donc utilisée pour les nouvelles versions des applications.

#### 4.10.2.6 SPRINGBOARD

La dernière version utilisée est la version 3.3.9.0.

Le springboard utilise maintenant une application java appelée launcher-service-vertx développée par Opendigitaleducation qui se charge de récupérer les dépendances (modules) nécessaires au springboard brut et se charge de décompiler et de lancer les applications suivant les configurations des applications que nous renseignons dans le fichier conf.properties.

Ce launcher a été conteneurisé à l'aide de docker afin de simplifier son installation et son déploiement.

La dernière version stable du launcher est la 1.0.0

Nous retrouvons dans cette version du springboard la dépendance ent-core 4.12.0.

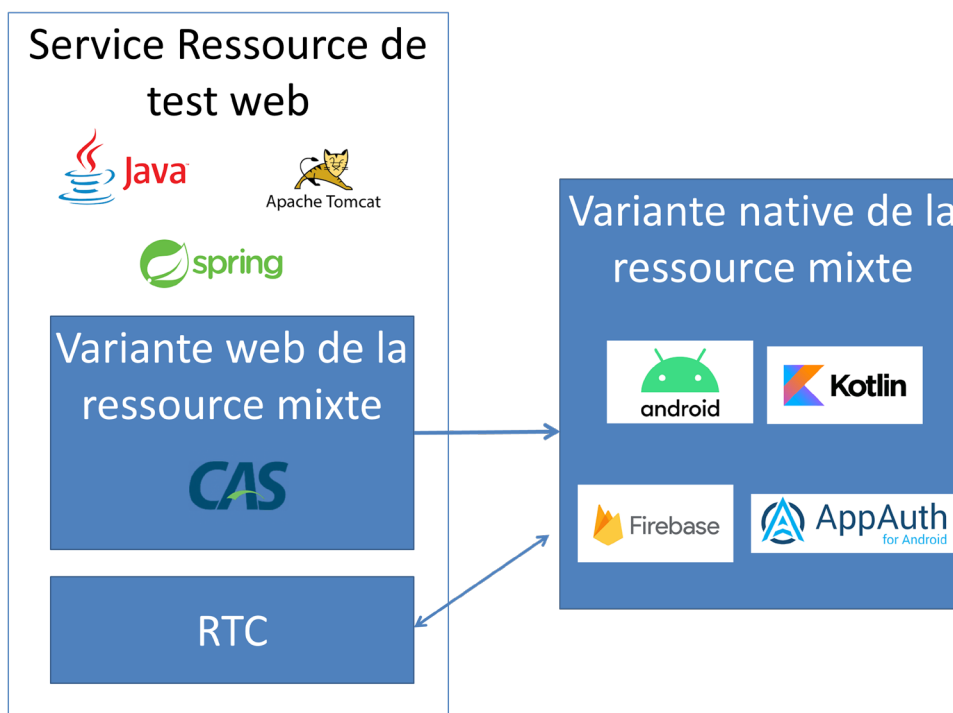
### 4.10.3 Mediacentre

La version du Mediacentre est la 3.2.4

Les dépendances ENT-core et vertx du Mediacentre doit être compatible avec celles du Springboard. En effet les modules à disposition de l'éditeur Opendigitaleducation sont basés sur cette version, si le module doit être compatible avec un il est primordial que l'ent-core du mediacentre soit compatible.

## 4.1.1 Ressources GAR de test et RTC

Dans le cadre de l'accès aux ressources numériques via une application native, la Ressource de test prend la forme d'une ressource mixte, disposant de sa webApp et d'une variante Android, et s'appuyant sur une ressource technique commune (RTC).



Le service ressource de test web est développé en java en s'appuyant sur le serveur CAS Apereo qui implémente les protocoles CAS et OIDC.

Le service ressource de test web utilise les fonctionnalités offertes par le serveur CAS, notamment les vues proposées par celui-ci.

La variante native de la ressource est développée en langage Kotlin pour la plateforme Android. La connexion OIDC au GAR est réalisée avec la librairie AppAuth for Android. L'application est mise à disposition pour téléchargement sur le service d'hébergement Firebase.

Versions utilisées pour chaque composant :

Composant	Version
Java	1.11
Apereo CAS	6.6
Tomcat	9
Android SDK	API 32 (minSDK 23)
AppAuth for Android	0.11.1

Ces services sont déployés sur les environnements de validation et de plateforme partenaires.

## 4.1.2 Interface de lancement des batchs en validation

Une interface permettant de lancer des batchs en validation est disponible uniquement sur l'environnement de validation (cf.[DR36](#)).

Cette interface donne la possibilité de lancer les batchs suivants :

- Pré-affectation
- Post-moissonnage
- Import ENT

Depuis l'interface, l'utilisateur envoie une demande de lancement d'un des batchs. Cette demande est stockée en base de données.

Un script s'exécute régulièrement pour traiter les demandes en cours, et lancer le batch correspondant en gérant la concurrence avec les exécutions automatiques de ces mêmes batchs.

L'interface met à jour le statut des dernières demandes jusqu'à ce qu'elles soient traitées et gère la concurrence multiutilisateur.

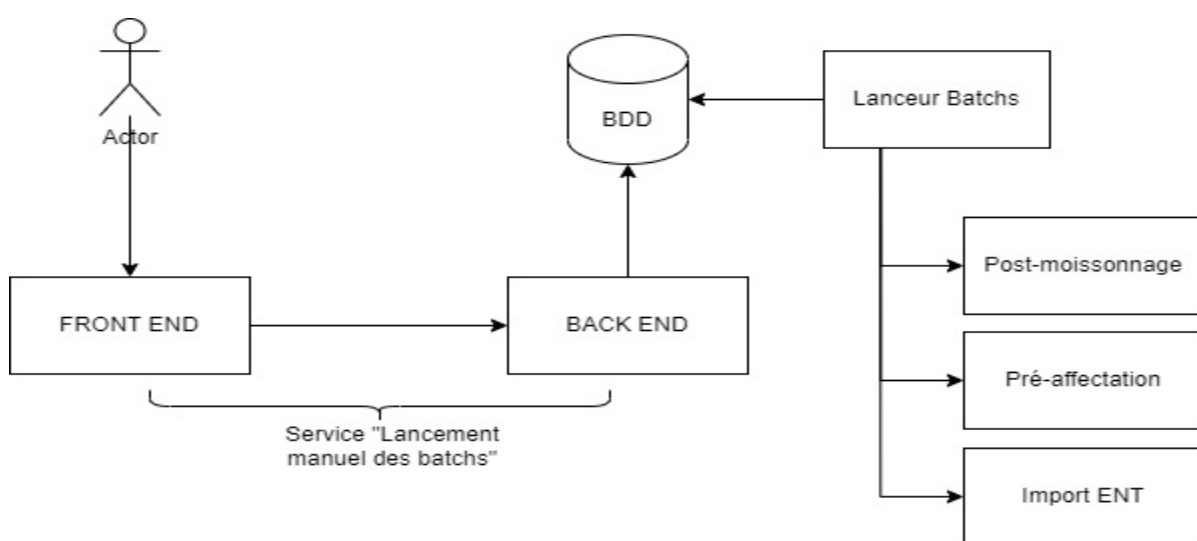


Figure - Service de lancement manuel des batchs

## 4.13 Bases de données

### 4.13.1 Liste

Les différentes bases de données sont listées dans le tableau ci-dessous.

Base	Moteur	Version	Description
ENT	Mysql	8.0.29	Référence l'ensemble des données ENT collectées au sein de la solution GAR
Affectations/Ressources	Mysql	8.0.29	Référence l'ensemble des ressources du GAR et l'ensemble des affectations Ressource/Utilisateur
Abonnements et autres données	Mysql	8.0.29	Référence l'ensemble des autres données de la solution GAR (abonnements, tables de correspondance, ...)
Authentification	Redis	5.6.34	Stockage des informations d'authentification pour le module d'accès aux ressources
Administration	Mysql	8.0.29	Stockage des informations pour l'interface de lancement manuel des batchs Uniquement sur l'environnement de validation
Collecte	Mysql	8.0.29	Stockage de l'ensemble des données ENT utiles pour la brique de collecte des données ENT

Chaque base dispose d'une série de login/mdp selon les environnements et selon les types d'accès (lecture seule, lecture écriture).

Le détail du modèle de données est décrit dans le document [DR14](#).

### 4.13.2 Gestion des connexions

Les services du GAR gèrent des pools de connexions JDBC, paramétrables, pour l'accès à chaque base de données applicative du projet GAR. La librairie open source utilisée est **HikariCP** ; elle permet un réglage fin entre performances et disponibilité.

Pour plus de détail : <https://github.com/brettwooldridge/HikariCP>

### 4.13.3 Règles de nommage

Les règles de nommage suivantes ont été appliquées :

- (1) Nom des bases en majuscule avec '\_' comme séparateur de mots.
- (2) Nom des tables et des champs métier en minuscule avec '\_' comme séparateur de mots.
- (3) Le nom des champs est préfixé par un code rappelant le nom de la table et permettant d'assurer l'unicité de chaque nom de champs dans la base.

Les noms utilisés sont en français.



## 5. Architecture applicative

### 5.1 Version logicielle

Nom	Version	Licence	Commentaire
<b>Système d'exploitation</b>			
Linux RedHat	7.9.9	Red Hat Enterprise Linux	OS utilisé sur l'ensemble des serveurs
<b>Base de données</b>			
MySQL	8.0.29	GPL	
Redis	3.2.12	BSD	
<b>Serveurs web</b>			
NGINX	1.20.1	BSD	
<b>Serveurs d'application</b>			
Tomcat	8 / 9	Apache 2.0	
<b>Serveurs IAM</b>			
CAS d'Apereo	6.3.5	Apache 2.0	
pac4J	4.5.0	Apache 2.0	
<b>Briques logicielles</b>			
Java	1.8 / 1.11	SCSL	
Maven	3.8	Apache 2.0	
Postfix	2.11	IBM public licence	Version maintenue par Redhat dans le cadre de la release CentOS
JIRA	8.22.6		
<b>Front</b>			
Angular	11.0.0, 12.1.3, 14.2.0	MIT/X11	
<b>Back</b>			
Spring Framework	4.3.7	Apache 2.0	
Clamav	0.103.2	GPL-2.0	
spring-data-jpa	2.5.10	Apache 2.0	
Spring Batch	4.3.5	Apache 2.0	
Spring Boot	2.5.12, 2.6.12	Apache 2.0	
<b>Log management</b>			
Logstash	7.17.0-1	Apache 2.0	
Zookeeper	3.4.6	Apache 2.0	
Apache Hadoop	3.10	Apache 2.0	
Apache Spark	2.3.2	Apache 2.0	
Elasticsearch	7.17.0-1	Apache 2.0	
Kibana	7.17.0-1	Apache 2.0	
<b>Sécurité</b>			

OpenSsh	7.4	BSD	Version maintenue par Redhat dans le cadre de la release CentOS
Openssl	1.0.2	OpenSSL License (Licence Apache 1.0) et SSLeay License (licence BSD clause 4)	Version maintenue par Redhat dans le cadre de la release CentOS
<b>Exploitation</b>			
Watchdog		N/A	Produit interne
Collector		N/A	Produit interne

## 5.2 Composants communs techniques

### 5.2.1 Serveurs SMTP

Deux services SMTP sont disponibles sur la plateforme GAR afin de gérer l'envoi des notifications par mail pour les services suivants (cf. [DR8](#)) :

- Batch de pré affectation (cf [DR8](#))
- Batch de post affectation (cf. [DR11](#))
- Brique de collecte des données ENT (cf. [DR10](#))
- Brique de moissonnage (cf. [DR9](#))
- Gestion DCP (Batch + portail GAR) (cf [DR17](#) et [DR13](#))
- Batch d'import ENT-GAR (cf. [DR19](#))
- Batch de suppression des comptes support (cf [DR32](#))

Ces services SMTP sont basés sur Postfix.

Les services sont installés sur 2 VM en mode actif / passif

Configuration :

- Nom de domaine de production : gar.education.fr
- Adresse expéditrice de production : [nepasrepondre@gar.education.fr](mailto:nepasrepondre@gar.education.fr)
- Spool (pour conservation des mails en cas d'erreur temporaire lors de la remise) : 10 Go
- Délai de conservation : 2 jours
- Renvoi des DSN vers un administrateur pour prise en compte et demande de correction auprès de l'acteur concerné

### 5.2.2 Log management

La solution « Log management » permet de collecter les logs de l'ensemble des services du GAR à des fins d'historisation, d'exploitation et de calcul statistiques (Cf. [DR11](#)).

Le schéma suivant présente les briques de services de la solution :

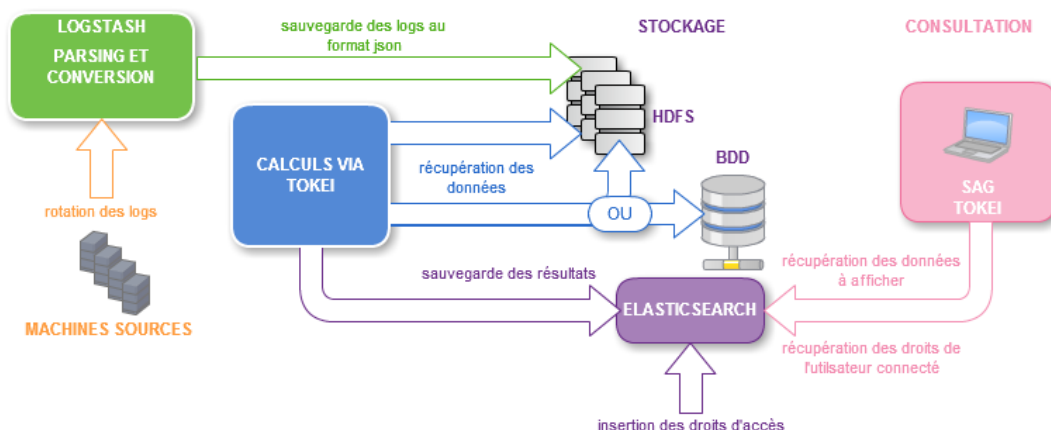


Figure 7 – Briques des services Log Management

Voici le détail de chaque brique logicielle :

- **Logstash** : Point d'entrée des traitements, il va permettre la réception de l'ensemble des logs applicatifs des différents services GAR et va analyser ces fichiers ligne à ligne. Il va ainsi valider leur format, éventuellement enrichir leur contenu et structurer les lignes au format json pour obtenir un format homogène, générique et propre facilement utilisable pour le calcul de métriques.
- **Apache Kafka** : messagerie distribuée, il est le point de sortie de l'ensemble des traitements Logstash. Il récupère les documents json et permet un traitement en parallèle de la donnée. Elle peut alors être exploitée par plusieurs services simultanément. Kafka se base sur l'outil Apache Zookeeper pour la gestion de sa configuration
- **Apache Spark** : outil de traitements parallèles (de type map and reduce), il est chargé d'effectuer les calculs de l'ensemble des indicateurs sur les logs déposés dans HDFS par les précédents traitements. Les calculs sont alors répartis de manière optimale sur l'ensemble des 3 serveurs afin d'optimiser les durées de traitement. Spark permet également de se brancher directement sur les bases de données afin de calculer les métriques d'état de la plateforme (tels que le nombre d'ENT intégrés, le nombre d'entrepôts...)
- **Elasticsearch** : Serveur d'indexation, il est utilisé comme une brique de configuration pour spark (il contient les règles de calcul des indicateurs préalablement définies). Il sert également au stockage des indicateurs calculés.



Le tableau ci-dessous présente la répartition des services Back sur les 5 serveurs utilisés :

	Namenode Serveur #1	Namenode Serveur #2	Datanode Serveur #1	Datanode Serveur #2	Datanode Serveur #3
Kafka/Zookeeper (Distribution de la donnée) <sup>1</sup>			X	X	X
HDFS (Stockage des données au format json) <sup>2</sup>	(namenode)	(namenode)	datanode	datanode	datanode
Elasticsearch (Stockage des configurations et résultats) <sup>3</sup>	X (Master)	X ( Master)	X	X	X
Yarn ResourceManager	X	X			
Yarn nodemanager <sup>4</sup>			X	X	X
Spark (Serveur de lancement des calculs)	X	X	X	X	X

<sup>1</sup> Kafka gère automatiquement la notion de nœud maitre/esclave via Zookeeper. Les données sont répliquées sur 3 serveurs.

<sup>2</sup> Les données (au format json) de HDFS sont dupliquées sur l'ensemble des 3 serveurs datanodes.

<sup>3</sup> Elasticsearch définit automatiquement un nœud maitre. Il le repositionne automatiquement sur un nœud esclave si on le perd.

<sup>4</sup> Yarn est déployé sur tous les serveurs pour réaliser les calculs en parallèle.

Le tableau ci-dessous présente la répartition des services Middle & Front sur les 5 serveurs utilisés :

	Front Serveur #1	Front Serveur #2	Middle Serveur #1	Middle Serveur #2	Middle Serveur #3
Logstash (Parsing des logs bruts) <sup>5</sup>			X	X	X
Kibana (Interface de consultation des logs)	X	X (Failover)			

<sup>5</sup> Logstash est installé sur les 3 serveurs afin d'équilibrer la charge (Load Balancing).

### 5.2.3 Authentification portail GAR

Un service d'authentification centralisé (SSO, acronyme de Single Sign On), basé sur la solution open source jasig, principale implémentation du protocole CAS est mis en place sur le GAR (cf. 1.3 ).

Tous les nœuds qui constituent la plateforme d'authentification sont redondés pour garantir une continuité de service :

- Deux serveurs SSO sont montés en cluster actif-passif (si le serveur actif tombe, le serveur passif prend automatiquement le relais mais les utilisateurs perdent leur session et doivent se ré-authentifier) ;
- Les serveurs SSO sont placés derrière le reverse proxy qui est également redondé en mode actif-passif.

### 5.2.4 Service de diffusion des vignettes GAR

Les vignettes GAR générées (cf. [DR9](#)) sont déposées sur un NFS.

Un serveur nginx gère la diffusion des vignettes GAR sur internet. Ce serveur nginx a accès en lecture au NFS sur lequel sont stockées les vignettes.

Le DNS dédié aux vignettes GAR est accessible sur l'internet sans authentification.

La diffusion des vignettes GAR :

- (1) Est disponible en http et en https.
- (2) Propose la compression gzip (voir header http Content-Encoding)
- (3) Autorise la mise en cache pendant pour 24h (configurable) par le client et les proxys intermédiaires (voir headers http Cache-Control et Expire)

Ce serveur WEB nginx est installé sur deux serveurs loadbalancés

### 5.2.5 Aide en ligne IHM Affectation.

L'hébergement de l'aide en ligne mise à disposition pour l'IHM affectation est positionné sur un montage NFS raccordé aux serveurs porteurs du service HTTP (cf.4.1).

### 5.2.6 Batch de suppression des comptes support

La gestion des comptes utilisateurs support nécessite de supprimer régulièrement les comptes obsolètes dans le SI. Le batch suppression des comptes support est en charge de supprimer les comptes qui n'ont pas d'activité avérée sur le support GAR.

Ce processus de suppression annuel doit s'assurer de ne conserver que les comptes utilisés et de respecter les règles de conservation des données personnelles. Il permettra aussi :

- D'envoyer des mails de notifications vers les comptes des utilisateurs en instance de désactivation/suppression.
- De réactiver un compte utilisateur via un lien dans la notification mail.
- De réassigner les tickets et commentaires Jira associés aux utilisateurs supprimés.
- De supprimer les comptes
- De sauvegarder les informations sur les comptes supprimés

Les spécifications détaillées sont disponibles dans le document référencé DR32.

## 5.3 Stratégie d'ordonnement des services

Le plan batch (cf. [DR21](#)) décrit la stratégie d'ordonnement des batchs sur les différents environnements.

## 5.4 Interfaces du système

Les interfaces d'échanges avec la solution GAR sont de 2 types :

- Webservice REST (https)
- transfert de fichier (sftp)

## 5.5 Design patterns

Voici les principaux design patterns mis en œuvre dans le cadre du projet GAR :

- (1) Factory
- (2) Singleton
- (3) Observer
- (4) Adapter
- (5) Decorator
- (6) Iterator
- (7) Proxy
- (8) MVC
- (9) Template method
- (10) Strategy
- (11) Composite
- (12) Service locator
- (13) Component
- (14) Dependency injection
- (15) Model injection
- (16) Inversion of control

## 6. Architecture technique

### 6.1 Description architecture logique

#### 6.1.1 Introduction

La solution GAR dispose de 5 Plateformes :

- 1 plateforme de production mixant serveurs virtuels et physiques
- 1 plateforme de pré-production. Cette plateforme est iso-production
- 1 plateforme de validation fonctionnelle entièrement constituée de serveurs virtuels
- 1 plateforme de tests partenaires entièrement constituée de serveurs virtuels

Les serveurs virtuels sont hébergés sur notre solution de Cloud mutualisé sous VMWare.

La plateforme de production GAR est hébergée dans notre Cloud mutualisé VMWare du Datacenter Seclin/PMP-Dassault.

Les plateformes de pré-production, validation fonctionnelle, tests partenaires sont hébergées dans notre Cloud mutualisée du Datacenter Seclin/La Pointe.

#### 6.1.2 Zones réseau

Comme présenté dans le schéma suivant, les plateformes réseau de production et de pré-production, validation fonctionnelle, tests partenaires sont construites suivant des architectures trois tiers :

- un réseau frontal de présentation
- un réseau middle de traitement
- un réseau back de données

Des réseaux d'accès à notre backbone data (réseau data front et réseau data middle) permettent l'accès aux ressources de stockage partagée (NFS)

Le backbone data Wordline est constitué de réseaux d'accès et de réseaux de ressources. Les serveurs ayant besoin de joindre une ressource de stockage partagé (NAS) doivent disposer d'une interface dans un réseau d'accès. Les réseaux d'accès sont uniquement autorisés à se connecter aux réseaux de ressources. Les communications entre réseaux d'accès sont impossibles.

Des firewalls Cisco Firepower cloisonnent le réseau frontal vis-à-vis de l'extérieur, solution matérielle plus adaptée pouvant mettre en œuvre notamment des fonctionnalités de filtrage, d'inspection protocolaire, et de prévention d'intrusion.

Le cloisonnement des réseaux Front/Middle/Back est opéré par des firewalls Checkpoint Secure Gateway.

Des technologies de firewalling différentes ont été choisies afin de renforcer la sécurité globale de la plateforme.

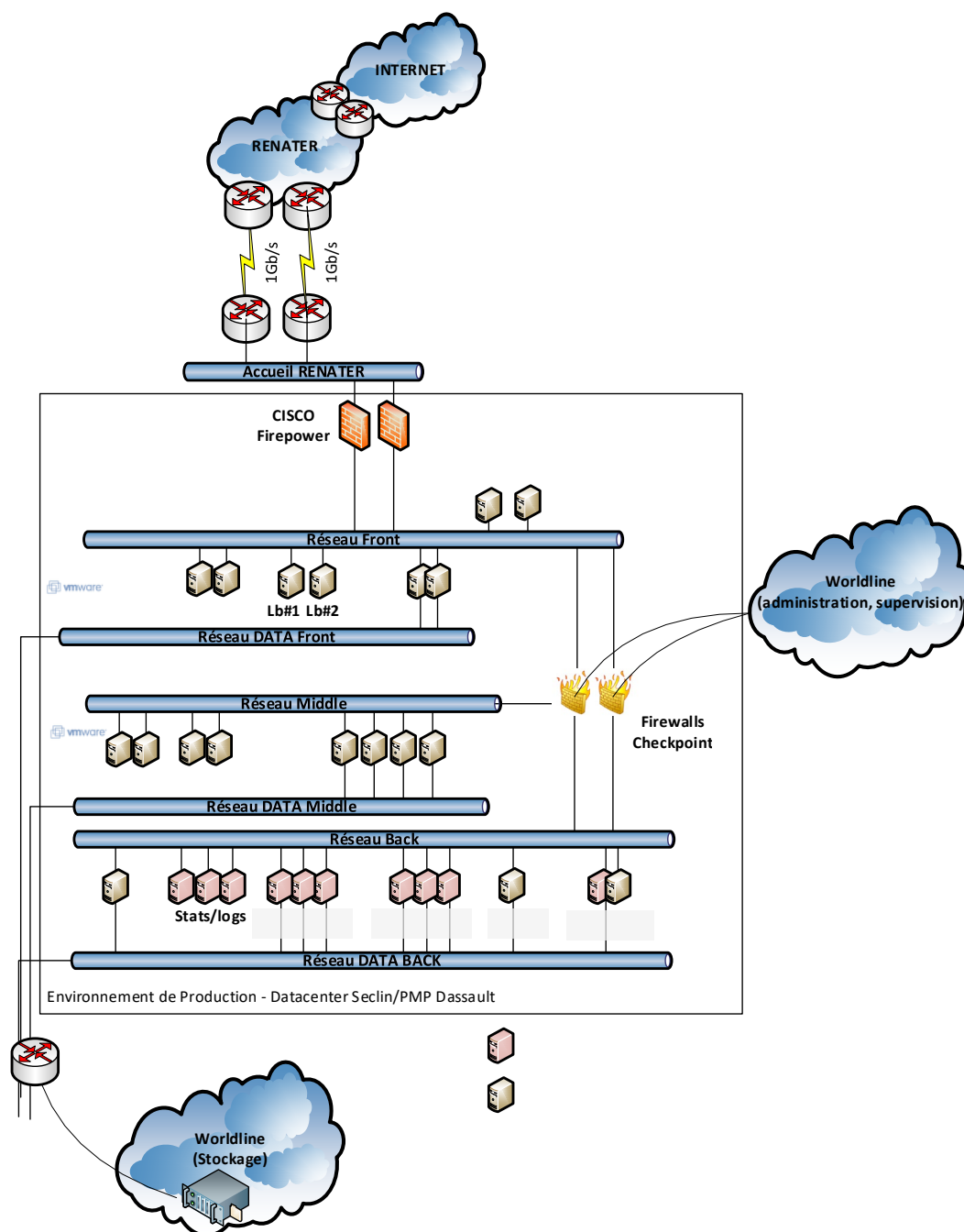


Figure 8 – Schéma d'architecture logique – principe de sécurité

### 6.1.3 Architecture de production

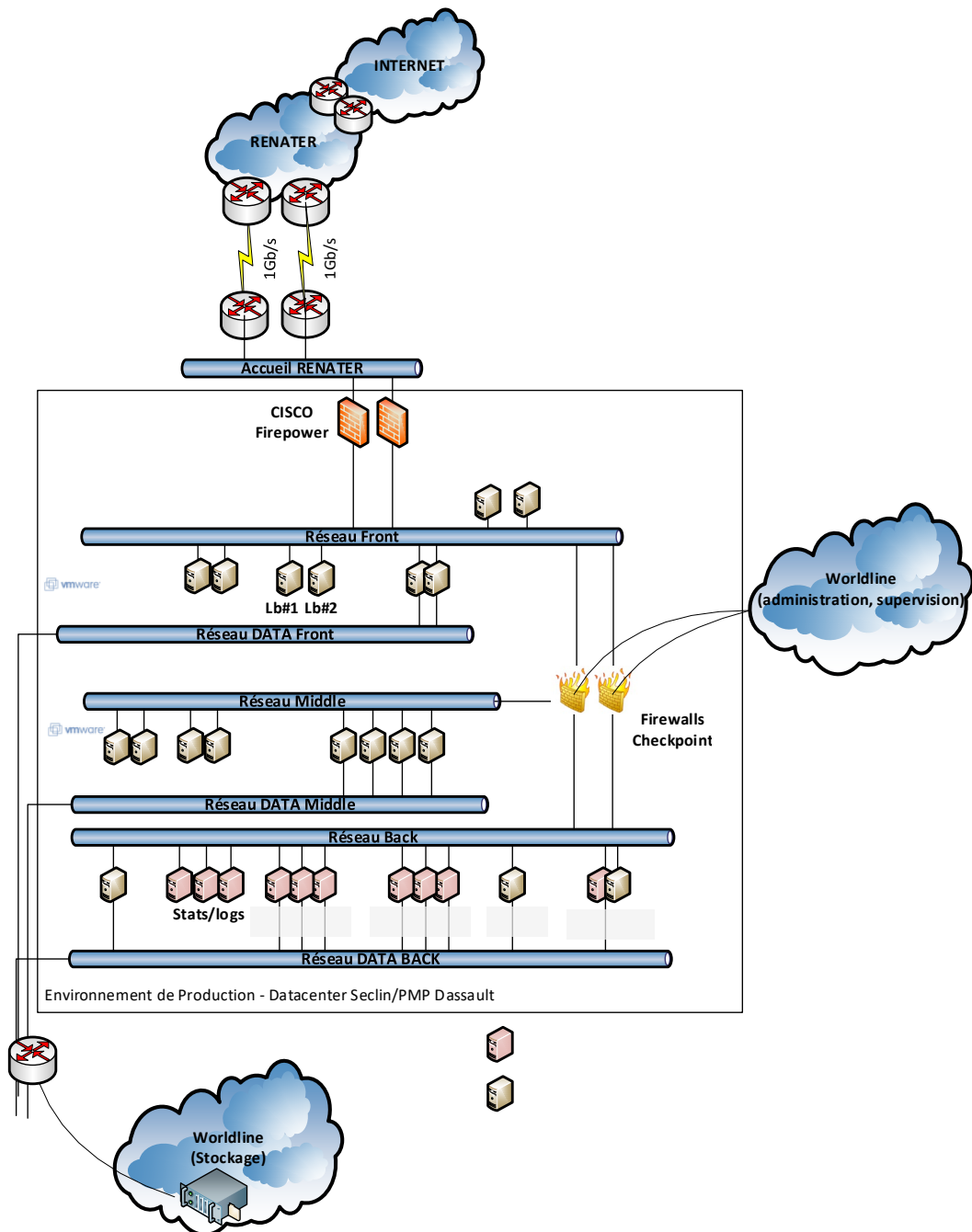


Figure 9 – Architecture de production

La plateforme de production est hébergée sur une architecture logique dédiée au projet GAR. Les réseaux, les serveurs ainsi que les Firewall sont dédiés à cette plateforme GAR.

## 6.1.4 Architecture de pré-production

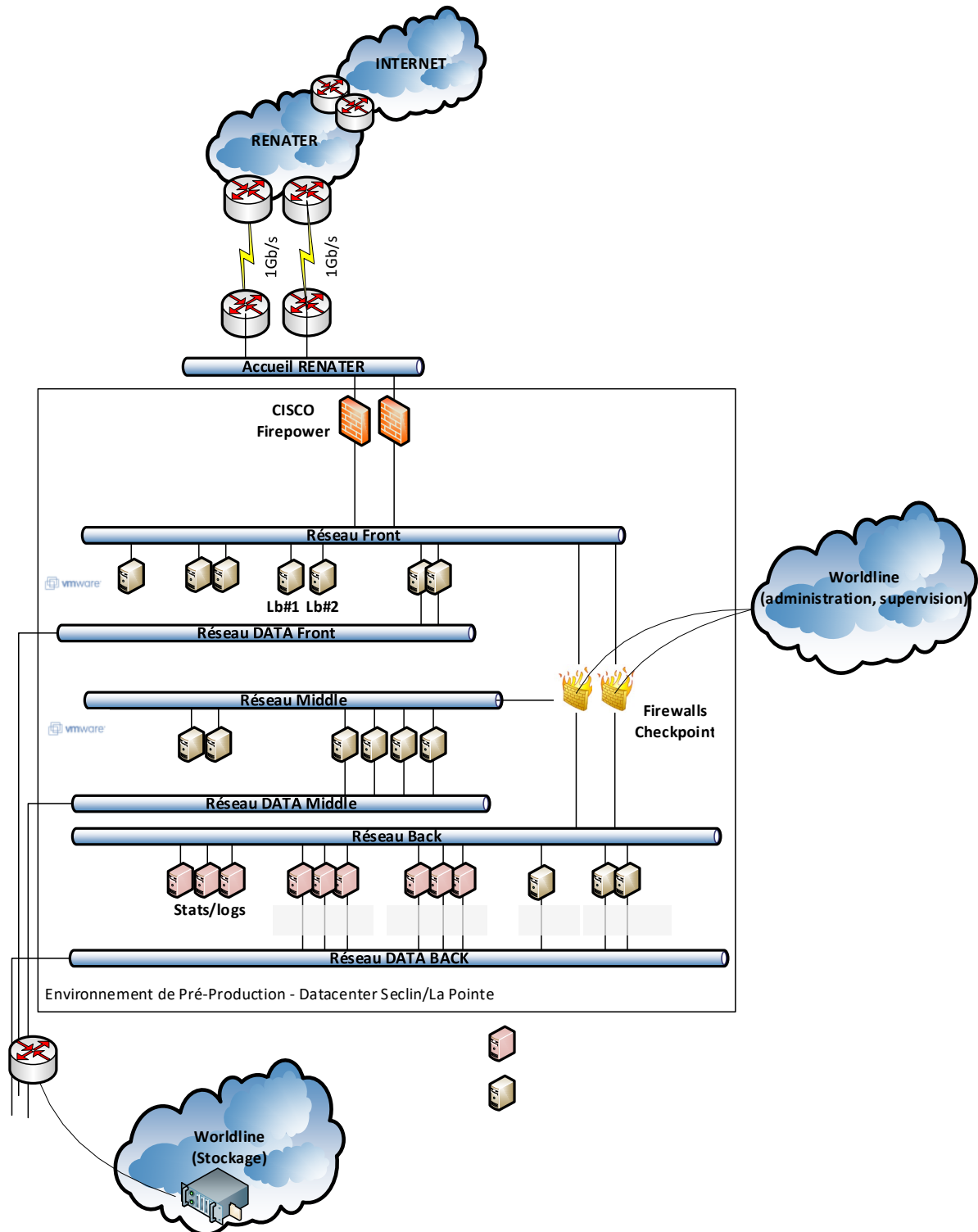


Figure 10 – Architecture de pré-production

La plateforme de pré-production est hébergée sur une architecture logique dédiée au projet GAR. Les réseaux, les serveurs ainsi que les Firewall sont dédiés à cette plateforme GAR.



## 6.1.5 Architecture de validation fonctionnelle/tests partenaires

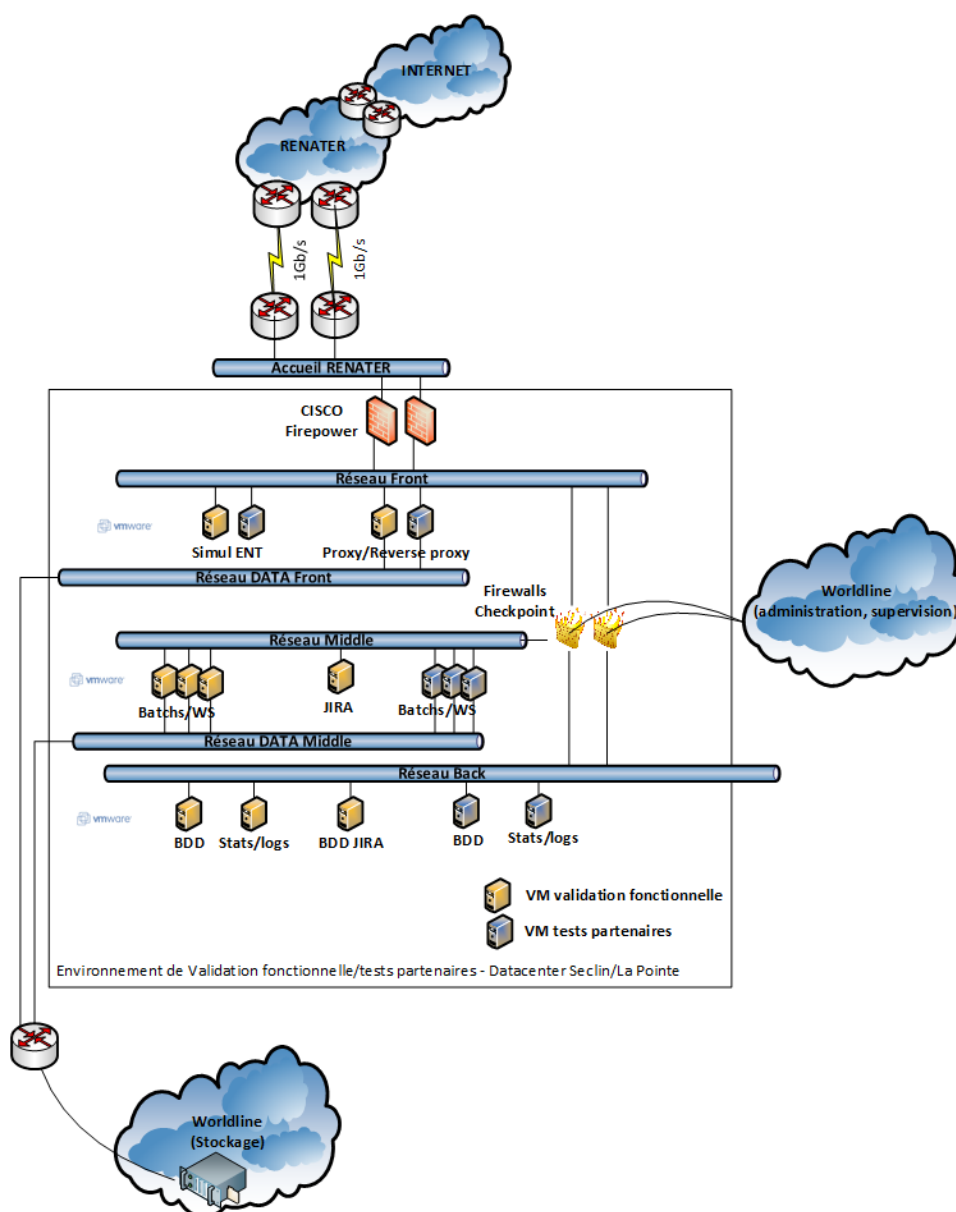


Figure 11 – Architecture de validation fonctionnelle/tests partenaires

Les plateformes de validation fonctionnelle et tests partenaires sont mises à disposition pour de la qualification et la gestion des accrochages. Ces plateformes ne gèreront pas autant de flux que la production ; elles partagent donc la même architecture logique qui sera capable d'honorer le flux de ces 2 environnements ; les Firewalls et Loadbalancers redondés sont donc mutualisés avec la plateforme de préproduction. Les VM hébergeant les services sont quant à elles dédiées soit à la validation fonctionnelle, soit aux tests partenaires.

## 6.2 Schéma architecture physique

Le schéma ci-dessous présente l'architecture physique globale de la plateforme, intégrant l'intégralité des machines, leur nommage, les scopes réseaux internes à Worldline et les vlans associés :

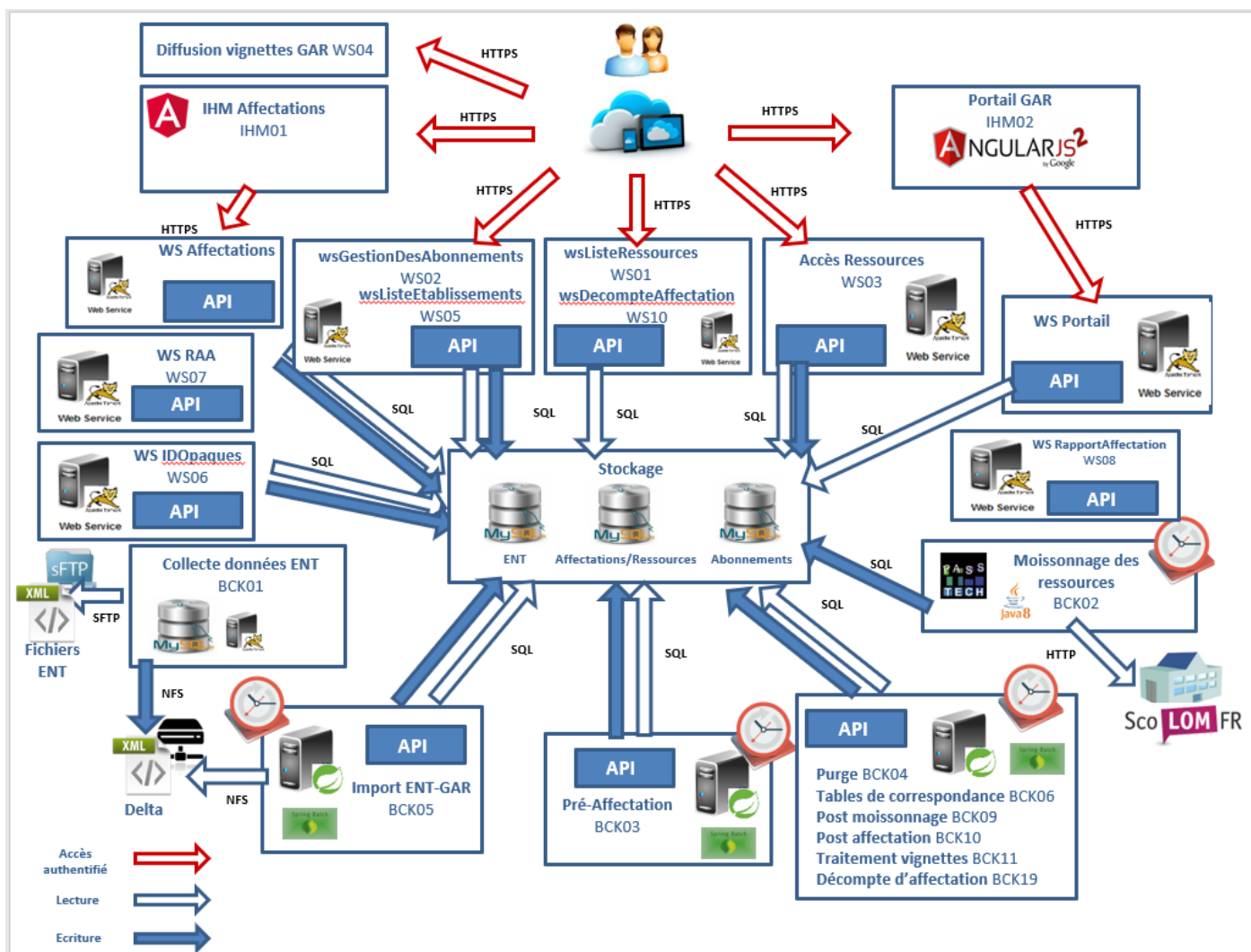


Figure 12 - Architecture physique du GAR

## 6.2.1 Scopes réseaux et VLANs – environnements hors production

### SCOPES ET VLAN RESEAUX - Data Center Seclin/La pointe

ZONE	ENV	RANGE_IP	VIP	VLAN
BACK	PREPROD	10.35.102.0/24	BACK_RENATER_GAR_PREPROD	1090
DATA	PREPROD	10.33.100.0/24	FRONT_RENATER_GAR_PREPROD_DATA	2576
ACCUEIL	PREPROD	10.31.73.64/27	ACCUEIL_RENATER	1186
FRONT	PREPROD	10.35.100.0/24	FRONT_RENATER_GAR_PREPROD	1088
MIDDLE	PREPROD	10.35.101.0/24	MIDDLE_RENATER_GAR_PREPROD	1089
MIDDLE/DATA	PREPROD	10.33.101.0/24	MIDDLE_RENATER_GAR_PREPROD_DATA	2577
BACK	QLF/RCT	10.35.105.0/24	BACK_RENATER_GAR_QUALIF	1094
FRONT	QLF/RCT	10.35.103.0/24	FRONT_RENATER_GAR_QUALIF	1092
FRONT/DATA	QLF/RCT	10.33.103.0/24	FRONT_RENATER_GAR_QUALIF_DATA	2579
MIDDLE	QLF/RCT	10.35.104.0/24	MIDDLE_RENATER_GAR_QUALIF	1093
MIDDLE/DATA	QLF/RCT	10.33.104.0/24	MIDDLE_RENATER_GAR_QUALIF_DATA	2580

## 6.2.2 Scopes réseaux et VLANs – environnement de production

### SCOPES ET VLAN RESEAUX - Data Center Seclin/PMP Dassault

ZONE	ENV	RANGE_IP	VIP	VLAN
ACCUEIL	RENATER	10.92.34.0/27	ACCUEIL_RENATER	395
FRONT	SIT2COM/PROD	10.43.168.0/24	RENATER_GAR_PROD_SIT2COM	1428
FRONT	PROD	10.43.0.0/24	FRONT_RENATER_GAR_PROD	1393
MIDDLE	PROD	10.43.1.0/24	MIDDLE_RENATER_GAR_PROD	1394
BACK	PROD	10.43.2.0/24	BACK_RENATER_GAR_PROD	1395
FRONT/DATA	PROD	10.41.0.0/24	FRONT_RENATER_GAR_PROD_DATA	2630
MIDDLE/DATA	PROD	10.41.1.0/24	MIDDLE_RENATER_GAR_PROD_DATA	2631

Les échanges entre Worldline et Renater ne se font que via des adresses publiques, les translations d'adresses étant implémentées sur les firewalls frontaux ASA.

Le nommage des machines composant la plateforme est construit comme suit :

Le premier digit indique le type de serveur :

- 'l' pour les Loadbalancers
- 'b' pour les BDD
- 'w' pour les machines frontales typées Web (apache)
- 't' pour les machines middle tomcat
- 'z' pour les machines de statistiques
- 'n' pour les serveurs DNS

Le deuxième digit définit le type de plateforme :

- 'p' pour la production
- 'e' pour la pre-production
- 'i' pour la validation fonctionnelle/tests partenaires (qualification)

Les trois digits suivants forment un trigramme identifiant le client, ici 'ren' pour renater

Les deux digits suivants indiquent le numéro de machine, le premier chiffre précisant le numéro de colonne, et le second, le numéro de machine dans la colonne.

Le dernier digit correspond au site, ici 's' pour Seclin

## 6.3 Disponibilité des ressources

L'architecture est conçue de telle sorte que toutes les briques (réseaux, logicielles) soient constamment disponibles :

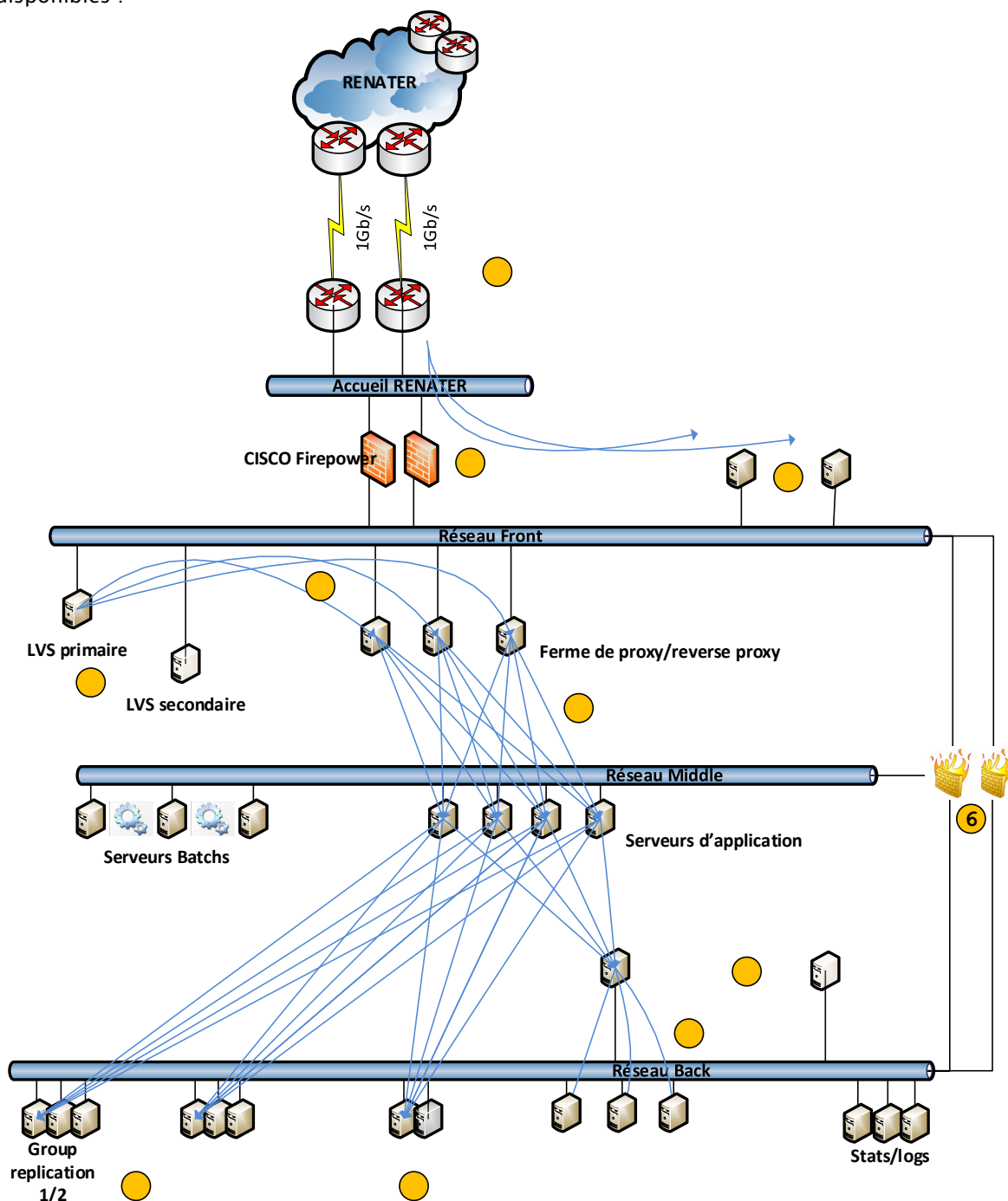


Figure 13 - Disponibilité des services du GAR

- ① La mise en place de l'échange de routes en BGP, avec des poids différents selon le site, nous assure que les plateformes resteront joignables en cas de perte d'une fibre ou d'un routeur. (bascule sur site de secours)
- ② Les firewalls Cisco Firepower fonctionnent en cluster, un master, et un standby. Le master monitore le standby en envoyant des messages keepalive, et inversement. Dès qu'un évènement se produit sur un élément du cluster, panne hardware ou perte d'une interface, l'élément est retiré du cluster. L'élément restant devenant master. Le fonctionnement est configuré en mode Statefull failover avec synchronisation de sessions.
- ③ Les Loadbalancers LVS fonctionnent en cluster. Le loadbalancer master envoie des paquets vrrp au standby. Lorsque le standby ne reçoit plus ces paquets de la part du master, il le considère KO et prend la main.
- ④ Les loadbalancers testent l'accès aux services sur chaque serveur de la ferme, et les retire du loadbalancing en cas d'échec de la connexion.
- ⑤ Les serveurs reverse proxy NGINX testent la disponibilité des serveurs Tomcat. Ainsi, les serveurs Tomcat en échec ne sont plus adressés.
- ⑥ Les Firewalls Checkpoint Security Gateway fonctionnent en cluster. Le firewall master envoie sur chacune de ses interfaces des paquets vrrp au standby. Lorsque le standby ne reçoit plus ces paquets de la part du master, il le considère KO et prend la main. Le master pousse sa table de session au standby, réplication et synchronisation de la table. Dans le cas de machines virtuelles, des règles anti-affinité sont mises en place afin de s'assurer que les 2 éléments du cluster ne soient pas présents sur la même machine physique.
- ⑦ Les machines des clusters BDD « group replication » se surveillent mutuellement. En cas de défaillance du nœud portant le rôle de master au sein de ce groupe, une bascule transparente est déclenchée et provoque l'attribution du rôle master l'un des autres nœuds actifs. Le nœud en défaut est quant à lui écarté du cluster, jusqu'à ce qu'il soit de nouveau opérationnel.
- ⑧ Les requêtes DNS sont équiréparties sur deux serveurs DNS (bind) publics visibles d'internet.
- ⑨ Les accès en écriture aux bases de données (architecture master/failover originale) visent un cluster BDD capable de basculer sur les instances miroir sans dégradation de service

Les principes décrits ci-dessus visent à détecter rapidement les défaillances de services ou de serveurs afin que ces dernières n'impactent pas les utilisateurs qui pourraient être aiguillés vers une ressource en défaut.

Nos mécanismes de surveillances internes détectent aussi ces éventuelles défaillances :

- Oscare détecte la défaillance hardware et le reboot de la VM sera opéré dans les plus brefs délais
- Application Monitor détecte la défaillance d'un service : nos procédures d'exploitation entreront en œuvre afin de redémarrer le service défaillant dans les plus brefs délais

Cette indisponibilité de service ou ressource ne dure que quelques minutes le temps de redémarrage du server ou du service incriminé. Une fois rétabli, le loadbalancer détectera le retour de la ressource et la réintègrera à la ferme de serveurs.

## 6.4 Schéma logique des BdD GAR

Le schéma suivant représente la répartition des instances BdD sur des serveurs physiques dédiés. La notion de groupe réplication est basée sur un ensemble de serveurs. Aucun membre n'a de rôle particulier. Tout membre compatible avec les autres membres du groupe est défini en mode lecture-écriture lorsqu'il rejoint le groupe et peut traiter les transactions d'écriture, même si elles sont émises simultanément.

Une ferme réplication a été positionnée dédiée aux accès en lecture uniquement, les données sont mises à jour par le processus de réplication MySQL (master-slave).

N.B. Un stockage SAN est alloué pour les plateformes de pré-production et de production.

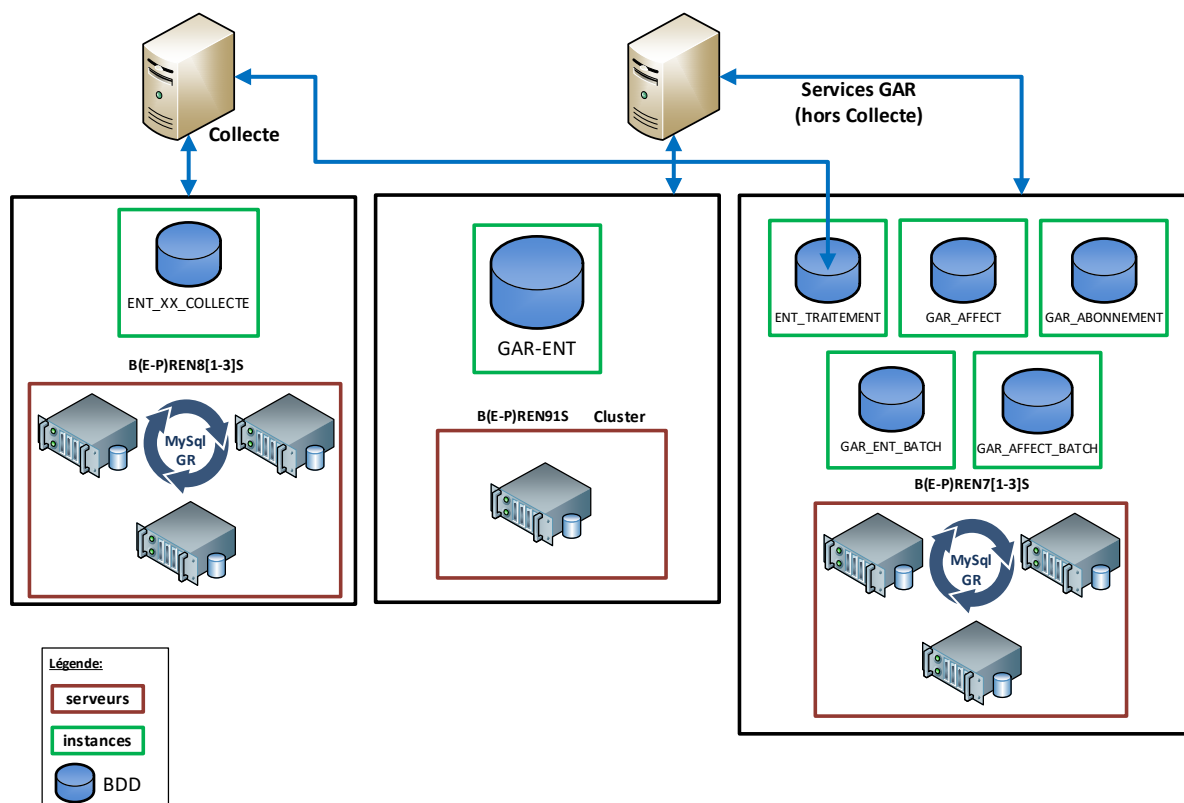


### 6.4.1 Stratégie de répartition des accès Bdd

Les différents services du GAR nécessitent des accès en lecture et/ou en écriture, afin de solliciter au mieux les ressources Bdd, la répartition suivante a été déployée :

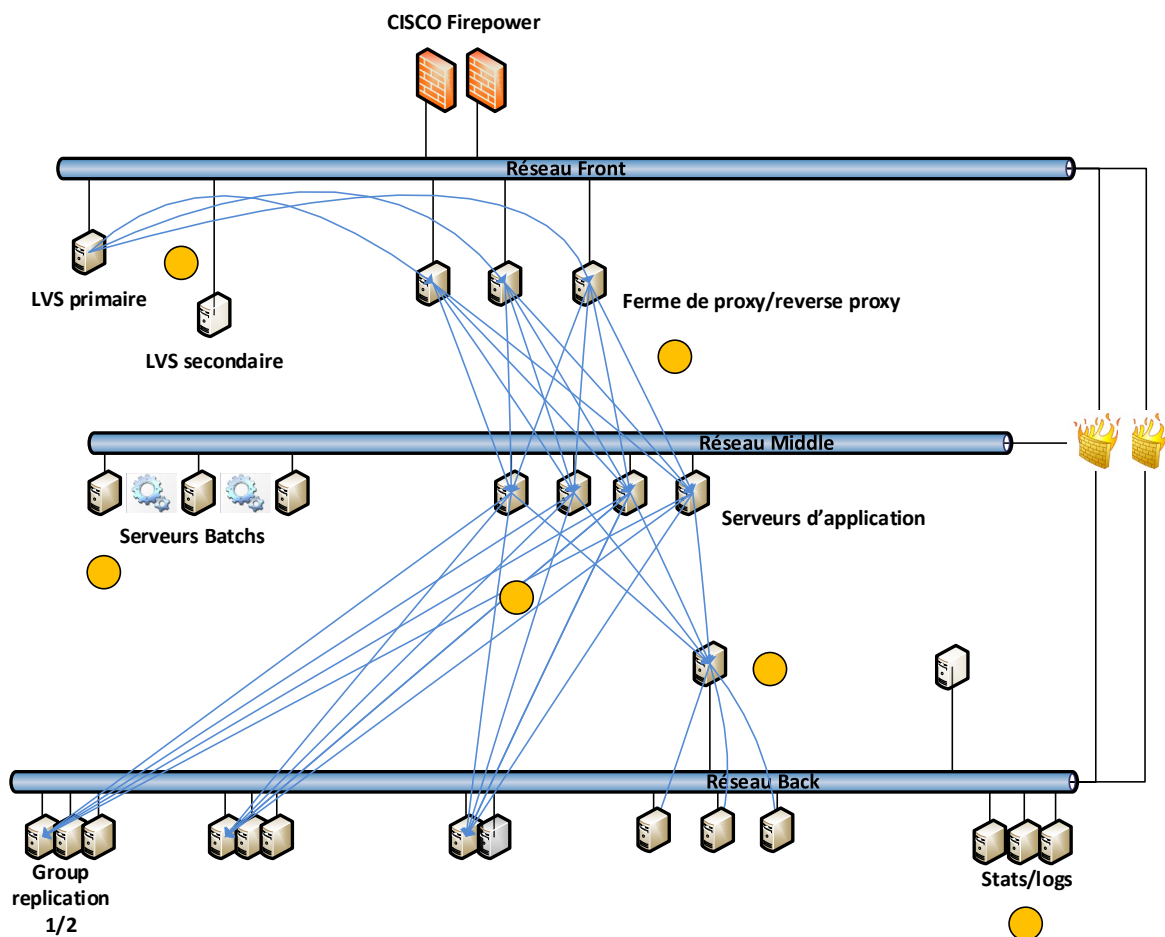
- Les group réplication Bdd portent des instances accessibles en lecture/écriture ;
- Les group réplication Bdd portent des instances en lecture seule

Le schéma suivant indique la stratégie type qui a été positionnée sur les services du GAR.



## 6.5 Scalabilité

Le schéma suivant présente les principes de scalabilité de chaque composant de l'architecture des différentes plateformes :



- ① Les flux http(s) sont gérés par les répartiteurs de charge LVS, ces derniers répartissent la charge vers une ferme extensible de serveurs reverse proxy en mode round-robin. LVS est utilisée en mode Direct Routing : les réponses aux clients se font en direct sans repasser par le répartiteur de charge.
- ② Le flux entre les reverse proxy et les serveurs d'application est géré par la solution reverse proxy (NGINX). Cette solution répartit le flux en round robin vers la ferme extensible de serveurs d'application. Elle garantit aussi le maintien des sessions applicatives sur un même serveur d'application (sticky).
- ③ La ferme extensible de serveurs batch gère l'ensemble des traitements de la solution GAR. La répartition des batchs est gérée par lot. Chaque serveur se voit attribuer la réalisation d'un lot.
- ④ Les accès BDD en écriture se font vers un ensemble de clusters BDD. Certaines bases sont joignables uniquement sur un cluster; d'autres bases sont multi-instances : l'orientation vers le cluster BDD hébergeant l'instance souhaitée se fait au travers d'un hash applicatif.
- ⑤ Les accès BDD en lecture se font au travers de répartiteurs de charge LVS, ces derniers répartissent la charge vers une ferme extensible de serveurs hébergeant des instances esclaves des différentes bases. LVS est utilisée en mode Direct Routing : les réponses aux serveurs d'application se font en direct sans repasser par le répartiteur de charge.
- ⑥ La solution de Statistiques et de logs repose sur la stack ELK (Elastic Search, Logstash, Kibana). Ce stack embarque nativement des mécanismes de distribution pour accompagner la croissance.

## 6.6 Stratégie et architecture pour sauvegardes, restaurations, purges, archivages

### 6.6.1 Sauvegarde des serveurs physiques de Base de données

Le processus de sauvegarde mis en place sur les serveurs physiques de base de données est décrit ci-après. Il se base sur l'outil CommVault qui utilise un agent local à chaque client et permet différents types de backup.

Nous utilisons le processus de Backup qui crée une copie d'un fichier ou d'un ensemble de fichiers et les stocke comme un objet unique pour une période de temps spécifiée sur un serveur de sauvegarde. La copie est ensuite poussée de façon asynchrone sur des bandes. Le processus de récupération du backup des données transfère la copie sur un serveur désigné.

Les serveurs de sauvegardes sont situés dans un datacentre différent de celui hébergeant la plateforme et sont redondés en cas de défaillance. Les bandes sont stockées sur le même site que les serveurs de sauvegarde. Aucun de ces éléments n'est externalisé par défaut mais peut-être envisagé si besoin.

La politique de sauvegarde des instances MySQL prévoit une sauvegarde quotidienne en mode full. Cette sauvegarde est déclenchée à 03H00 du matin. Un dump des instances est réalisé avant la prise de la sauvegarde afin d'assurer la consistance des données

Nous ne sauvegardons pas la configuration système des serveurs. Celle-ci est centralisée dans un repo de fichiers versionnés.

## 6.6.2 Sauvegarde des serveurs virtualisés hors Base de données

Les serveurs virtualisés sont sauvegardés via l'outil VEEAM, qui consiste (pour les serveurs hors base de données) en la prise d'une image de la VM à un instant t. Les sauvegardes sont stockées sur disques. Les équipements de stockage des sauvegardes sont situés sur le même site que le serveur sauvegardé.

La politique de sauvegarde des serveurs virtuels prévoit une sauvegarde quotidienne en mode full. Cette sauvegarde est déclenchée à 03H00 du matin.

## 6.6.3 Sauvegarde des serveurs virtualisés de Base de données

Les serveurs virtualisés base de données sont également sauvegardés via l'outil VEEAM.

La politique de sauvegarde des instances Mysql des bases de données virtuelles prévoit une sauvegarde quotidienne en mode full. Cette sauvegarde est déclenchée à 03H00 du matin. Un dump des instances est réalisé avant la prise de la sauvegarde afin d'assurer la consistance des données

## 6.6.4 Restauration des données

Sur les serveurs virtualisés, seule l'équipe sauvegarde procède à la restauration des données partielles ou complètes, sans distinction du type de données.

Des tests de restauration de données peuvent être demandés.

Les temps de restauration vont être dépendants de la quantité et de l'antériorité des données à restaurer.

## 6.6.5 Tests de restauration des données

Les tests de restauration permettent de valider le bon fonctionnement des restaurations en cas de sinistre.

2 types de sauvegardes sont mis en place sur la plateforme RENATER-GAR :

- Sauvegarde de serveurs virtualisés
- Sauvegarde de bases de données physique

Les tests de restauration consistent en la restauration :

- D'un serveur virtualisé disposant d'une base de données (sous un autre nom de VM provisoire, afin de ne pas perturber le service de production)
- De bases sauvegardées sur bande (dans des schémas temporaires sur un serveur de pré-production, afin de ne pas perturber le service de production)

Les tests se déroulent comme suit et sont tracés dans un outil de ticketing interne. Chaque test annuel fera l'objet d'un ticket de suivi des tests avec le résultat des tests.

#### 6.6.5.1 Test de restauration de serveur virtualisé

La détermination du serveur et de la date de restauration sera laissée au choix de l'équipe Support Applicatif. Elle devra également indiquer le nom du schéma qu'elle souhaite voir apparaître sur le rapport, et le nom de la table dont elle veut avoir un état.

Cette équipe devra indiquer ces informations dans le ticket de suivi qui sera alors transmis à l'équipe Système.

Cette dernière demandera à l'équipe Sauvegarde de procéder à la restauration du serveur virtualisé à la date indiquée, sous un autre nom provisoire.

Une fois la VM restaurée sous un nom provisoire, l'équipe DBA vérifiera la quantité de données présente dans la base, listera les schémas et les tables et fournira les informations à l'équipe Support Applicatif pour vérification.

La VM provisoire sera supprimée par l'équipe Sauvegarde, dès l'instant où l'équipe Support Applicatif aura donné son accord.

#### 6.6.5.2 Test de restauration de bases sauvegardées sur bande

L'équipe Support Applicatif indiquera dans le ticket de suivi le nom du schéma qu'elle souhaite faire restaurer, et le nom de la table dont elle veut avoir un état et transmettra ce ticket vers l'équipe DBA.

Cette dernière vérifiera la place disponible sur le serveur qui hébergera provisoirement les données restaurées, puis elle créera un schéma temporaire sur le serveur de Pré-Production, et procédera à la restauration dans le schéma précédemment créé.

Après la restauration, l'équipe DBA vérifiera la quantité de données présente dans la base, listera les tables et fournira les informations à l'équipe Support Applicatif pour vérification.

Les données restaurées et le schéma provisoire seront supprimés par l'équipe DBA, dès l'instant où l'équipe Support Applicatif aura donné son accord.

### 6.7 Stratégie et architecture pour la supervision du système

La supervision de la plateforme GAR est gérée par plusieurs solutions :

- Notre solution interne OSCARE gère le monitoring système des serveurs (consommation CPU, RAM, Filesystem) et nous permet de remonter des événements en fichier de logs (grep d'un pattern spécifique)
- La solution ICINGA se charge du monitoring des équipements réseaux (ping, consommation CPU, consommation mémoire, états des interfaces). Un alerting est envoyé sur dépassement de seuil préconfiguré ou sur changement d'état.
- Checks supplémentaires pour les firewalls frontaux : check du failover ainsi qu'un check du nombre de sessions.

Notre solution interne « OPS monitor » monitor le service GAR en déroulant un scénario applicatif complet ; elle nous permet aussi de faire des surveillances applicatives ciblées sur chaque brique de la solution (ping applicatif de chaque brique). Cette 2<sup>ème</sup> surveillance est un complément appréciable à la première afin de cibler rapidement l'élément défectueux entraînant une indisponibilité du service globale.

La supervision est détaillée dans le Plan Qualité Gestion des Services GAR (cf. [DR4](#))

### 6.8 Stratégie et architecture pour la métrologie du système

La métrologie de la plateforme GAR est assurée par plusieurs solutions :

- Une vue technique : consolidé par Grafana remonte un certain nombre de métriques systèmes, réseaux, applicatives (nombre de connexions/s, nombre de requêtes/s, ...)
- Une vue service : « OPS monitor » mesure le temps de réponse de différents scénarii applicatifs

Ces 2 solutions nous permettent de piloter les évolutions capacitaires de la plateforme GAR.

## 6.9 Stratégie de gestions des logs

### 6.9.1 Gestion des logs applicatifs

L'ensemble des logs applicatifs des services du GAR sont centralisés sur la brique de service « Log management » (cf §5.2.2).

Les durées de rétention sont définies dans le Plan d'Assurance Sécurité (cf. [DR1](#))

### 6.9.2 Gestion des logs système

#### 6.9.2.1 Principe

Toutes les actions de connexion, d'authentification et d'administration sont tracées, horodatées et par conséquent imputables nominativement. Ces traces sont centralisées sur l'architecture de gestion des traces composée de serveurs centraux nommés LOGS. Toutes les traces gérées par une machine de production sont systématiquement recopiées sur ces serveurs.

Voici la structure des traces collectées :

- La date (JJ:MM:AAAA) et l'heure (HH:MM:SS)
- Le descriptif de l'événement
- Le code retour de l'événement
- L'identifiant de l'utilisateur responsable de l'événement
- La cible de l'événement (fichier paramètre, serveur, application, service, etc)
- Le détail l'action réalisée (la commande passée, le script lancé, etc.)
- Le type d'évènement (modification, suppression, lecture, etc.)

Par exemple, les activités suivantes, liées à l'authentification sont enregistrées :

- Les tentatives d'ouverture de sessions, fructueuses ou non ;
- Les fermetures de session ;
- Les commandes SUDO passées.
- L'utilisation de commande « su - » ;
- L'utilisation du compte ou de l'identification d'un utilisateur privilégié (root);

#### 6.9.2.2 Architecture de centralisation

Le schéma suivant présente l'architecture de centralisation de logs :

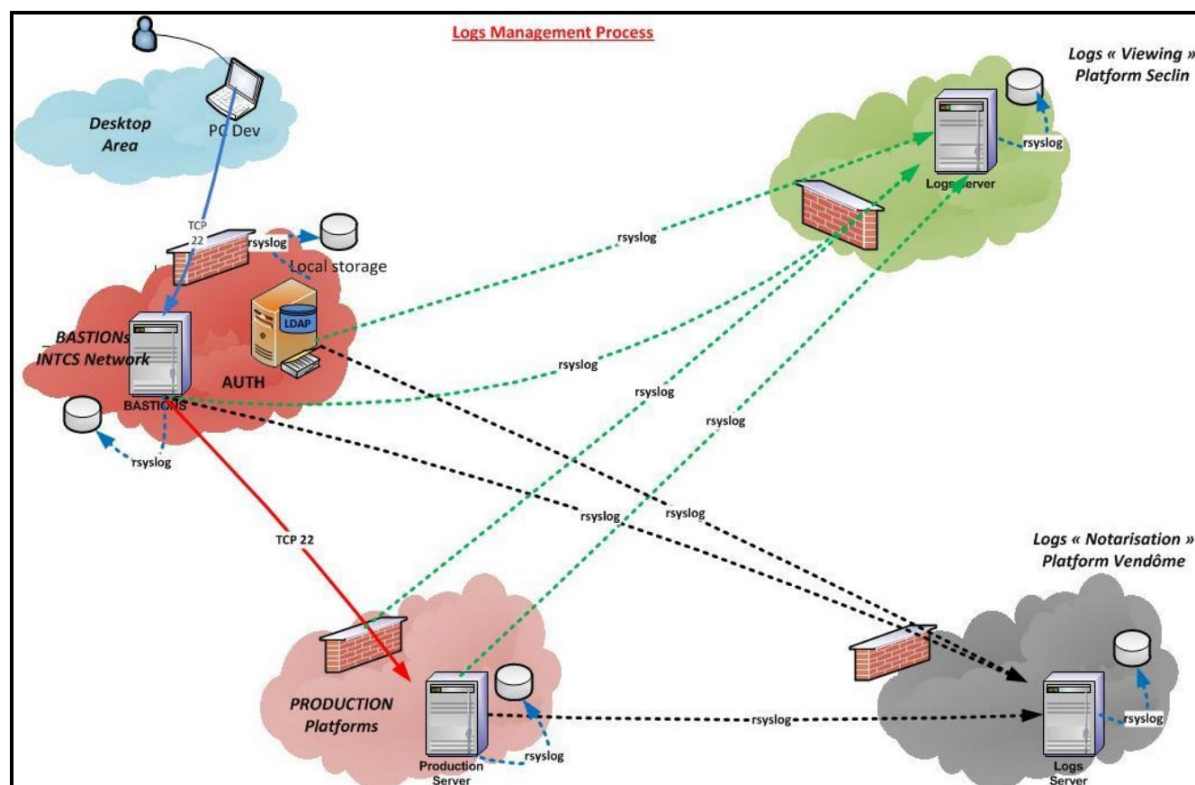


Figure 14 – Architecture de centralisation de logs

L'architecture de centralisation de logs se compose de 2 plateformes indépendantes tant au niveau géographique qu'au niveau de leur fonctions respectives. Les serveurs envoient leurs fichiers de logs en copie « Y » c'est-à-dire aux 2 plateformes simultanément (en plus de leurs copies sur le démon rsyslog en local sur le dit serveur) :

1) Une plateforme dite de « consultation de logs »

Cette plateforme recueille les traces des serveurs de production. Elle permet d'effectuer des opérations de consultation de logs, des traitements automatiques (notamment des opérations de corrélation de logs, des créations de statistiques de connexions par exemple).

Cette plateforme se trouve à Seclin.

2) Une plateforme dite de « notarisation »

Cette plateforme recueille une copie des traces centralisées sur le serveur de consultations de logs. Son rôle est de s'assurer que les fichiers de traces centralisés sont intègres. Dans le cas d'une forte suspicion de compromission du serveur de consultations de logs, des investigations peuvent être menés sur ce serveur pour confirmer et corroborer les résultats obtenus sur le serveur de consultations. L'accès à cette plateforme est très restreint. L'administration des serveurs est sous la responsabilité d'une équipe différente et indépendante de l'équipe de Sécurité Opérationnelle.

Cette plateforme se situe à Vendôme.

Nota : les bastions de rebond situés sur le réseau INTCS est sous la responsabilité de l'équipe Sécurité Opérationnelle. Les différentes équipes intervenant sur le projet GAR se connectent de manière nominative dessus avant de rebondir sur les serveurs du projet GAR. Les traces de sécurité de la plateforme (y compris celles concernant les administrateurs des bastions) sont centralisées vers les plateformes de traces (visualisation et notarisation).

## 6.10 Stratégie de sécurité du GAR

L'ensemble des règles de sécurité mise en œuvre pour le GAR est décrit dans le Plan d'Assurance Sécurité (cf. [DR1](#)) et dans la Politique de Sécurité Opérationnelle (cf [DR2](#)).



## 7.PROCEDURE DE PLAN DE REPRISE D'ACTIVITE

### 7.1 Généralité

L'infrastructure GAR intègre un plan de continuité des services complet incluant le composant Salle Machine (Appelé dans le document Datacenter) pour garantir une disponibilité maximale du service. La construction de ce Plan de Reprise d'Activité est facilitée par notre architecture nativement multi-site présentée en 7.4 et par l'expertise de Worldline à construire des architectures redondées de bout en bout.

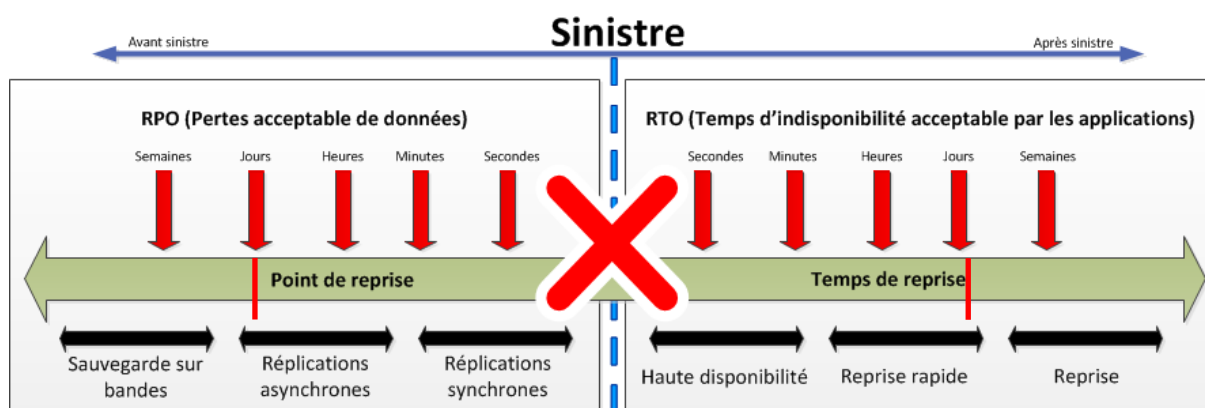
### 7.2 Définition d'un sinistre Majeur

#### **Sinistre Majeur**

Un sinistre majeur représente la perte complète d'un datacenter, suite à un incendie, inondation ou autres problèmes techniques majeurs (perte totale d'alimentation, perte totale de connectivité réseaux, défaut de climatisation).

#### **Adaptation de la solution**

Il est à noter que dans le cadre d'un Plan de Reprise d'Activité plus les points et les temps de reprise sont proches du sinistre, plus la solution technique à mettre en œuvre est complexe et onéreuse.



La solution proposée intègre une réplication de données entre le site de production et de secours. Elle est basée sur une réplication des sauvegardes, associée à une reprise rapide du service en cas de sinistre majeur.

## 7.3 Rappel des engagements

Le Plan de Reprise d'Activité est inclus dans le Plan de Continuité de l'Activité des services du GAR (cf. [DR37](#)). Il permet de pallier la perte du datacenter de production.

Nos engagements de temps de résolution, en fonction de la nature d'un sinistre unitaire rencontré sont décrits ci-dessous.

Nature du sinistre	Engagement	Plan de Continuité d'Activité
<b>Infrastructure PaaS / IaaS / CaaS</b>	< GTR 4h	Inclus dans notre offre
<b>Infrastructure réseau</b>	< GTR 4h	Inclus dans notre offre
<b>Infrastructure électrique/climatisation</b>	< GTR 4h	Inclus dans notre offre
<b>Perte du datacenter de production</b>	<b>24 h</b>	<b>Inclus dans notre offre</b>

Le Plan de Reprise d'Activité est défini par deux définitions fondamentales, établissant la solution technique mise en œuvre pour respecter les délais annoncés.

- Le RTO ou Recovery Time Objective se traduit par la durée maximale d'interruption admissible de service.
- RPO ou Recovery Point Objective désigne la durée maximum d'enregistrement des données qu'il est acceptable de perdre lors d'un sinistre majeur.

**Le Plan de Reprise d'Activité proposé par Worldline établit ces deux facteurs :**

- **RPO : « Fraîcheur » de la donnée de production au maximum de 24 heures**
- **RTO : Le site de secours reprend le service de production à capacité identique après bascule à J+1**

## 7.4 Présentation de nos Datacenters

### 7.4.1 Datacenter de Seclin/La Pointe

Les caractéristiques de notre datacenter de Seclin La Pointe :

- Situé sur le campus de Seclin (Nord de la France) ;
- Construit en 1985 avec extensions et rénovations en particulier depuis 2007 ;
- Installation électrique renouvelée entièrement en 2007 pour permettre une densité accrue ;
- Niveau standard « Uptime Institute Level » : Tier III ;
- Densité moyenne par salle : 1,5 kW/ m2 ;
- 1,5 km le séparent du site jumeau de Seclin/Dassault, permettant des stratégies de réplication de données efficaces.

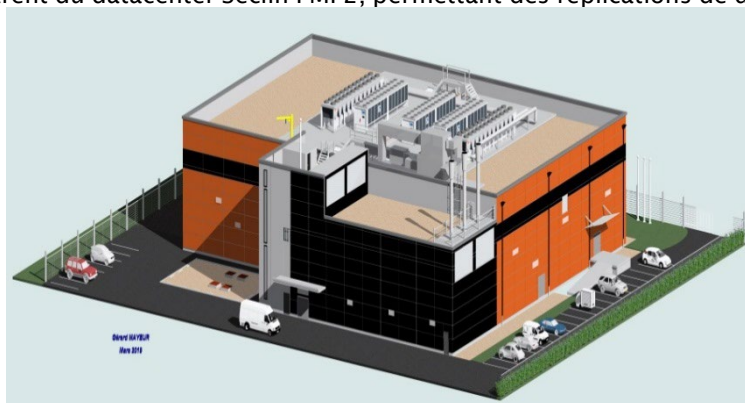


Capacité	<ul style="list-style-type: none"> <li>• 2000 m<sup>2</sup> de salles informatiques disponibles</li> <li>• séparées en 8 zones isolées contre l'incendie</li> <li>• densité prévue 1,5 kW par m<sup>2</sup></li> </ul>
Puissance électrique et secours	<ul style="list-style-type: none"> <li>• Alimentation externe 20 kV par 2 lignes séparées</li> <li>• Redondance composants électriques en N+1 (transfo, tableau principal, onduleur)</li> <li>• Autonomie batterie onduleurs 10 min</li> <li>• Redondance N+1 des groupes électrogènes diesel avec 72h d'autonomie</li> </ul>
Génie climatique	<ul style="list-style-type: none"> <li>• Systèmes d'air conditionné redondés avec échangeur air / fluide caloporteur</li> </ul>
Sécurité	<ul style="list-style-type: none"> <li>• 4 zones à franchir (clôture, accès building, accès salles, accès baies)</li> <li>• Monitoring 24/7 avec équipe locale</li> <li>• Sécurité anti-intrusion externe confiée à une unité de gardiennage mobilisée 24 / 7</li> <li>• Contrôles des accès physiques et logiques par badges et codes</li> <li>• Systèmes détection incendie rapides</li> <li>• Systèmes automatiques d'extinction incendie par zones (gaz inerte)</li> </ul>
Connectivité réseaux	<ul style="list-style-type: none"> <li>• Liens réseaux redondés avec opérateurs différents</li> <li>• Interconnexion Lan en fibre optique avec le datacenter Seclin PMP Dassault</li> </ul>
Efficacité énergétique	<ul style="list-style-type: none"> <li>• PUE valeur 1,78</li> </ul>
Certifications	<ul style="list-style-type: none"> <li>• ISO 9001, 14001, 27001, PCI DSS, DK</li> </ul>

## 7.4.2 Datacenter de Seclin/ Dassault

Les caractéristiques de notre datacenter de Seclin Dassault :

- Situé à Seclin (Nord de la France) ;
- Construit en 2009 ;
- S'étend sur 4350 m<sup>2</sup> ;
- Uptime Institute Level » : Tier III+ avec un taux de disponibilité annuelle > 99.98% ;
- Pour une densité de puissance de 2 kW/ m<sup>2</sup> ;
- 1,5 km le séparent du datacenter Seclin PMP2, permettant des répliquations de données synchrones.



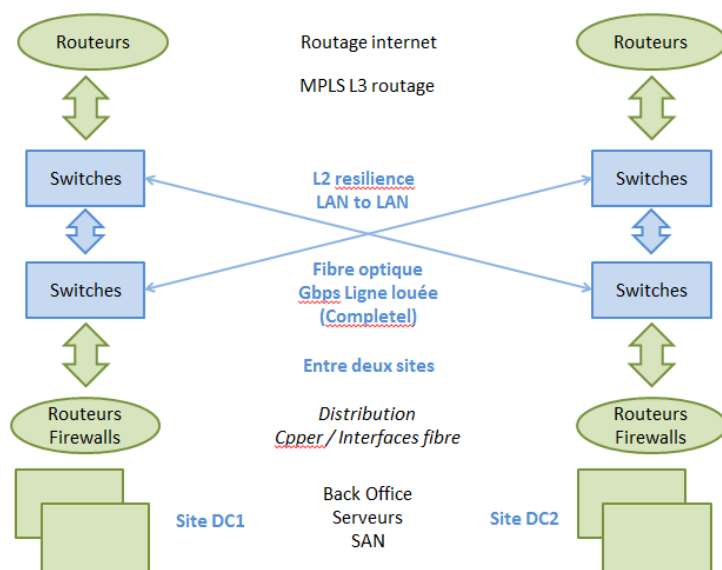
Capacité	<ul style="list-style-type: none"> <li>1200 m<sup>2</sup> de salles informatiques de densité 2KW par m2 divisé en 2 salles avec lutte incendie séparée</li> </ul>
Puissance électrique et secours	<ul style="list-style-type: none"> <li>2 alimentations externes 20 kV par chemin différents</li> <li>Equipements de puissance en redondance N+1 (transfo, tableaux de distribution, onduleurs)</li> <li>Autonomie batteries onduleurs de 15 min</li> <li>Générateurs électriques de secours diesel en N+1 avec 72 h d'autonomie</li> </ul>
Génie climatique	<ul style="list-style-type: none"> <li>Systèmes d'air conditionné en configuration N+1 en salle et en configuration 2N pour les circuits eau glacée et les groupes froids</li> </ul>
Sécurité	<ul style="list-style-type: none"> <li>4 zones de protection physique (clôture, bâtiment, accès salle informatique, accès aux baies)</li> <li>Monitoring 24/7 par équipe sur place</li> <li>Sécurité externe assurée par gardiennage 24 x7</li> <li>Contrôles d'accès par badges personnels et codes</li> <li>Détection rapide départ de feu</li> <li>Extinction automatique à gaz inerte par zones</li> </ul>
Connectivité réseau	<ul style="list-style-type: none"> <li>Liens doublés physiquement et avec opérateurs différents</li> <li>Interconnexion LAN en fibre optique avec le datacenter jumeau Seclin PMP2</li> </ul>
Efficacité énergétique	<ul style="list-style-type: none"> <li>PUE valeur 1,6</li> </ul>
Certifications	<ul style="list-style-type: none"> <li>ISO 9001, 14001, 27001 ,PCI DSS, DK,</li> </ul>

### 7.4.3 Interconnexion de nos deux Datacenters

Les deux datacenters Seclin/La Pointe et Seclin/Dassault sont interconnectés par deux faisceaux de fibres noires de 72 fibres avec des parcours différents dans la zone industrielle. De plus, les datacenters Seclin/La Pointe et Seclin/Dassault ont leurs propres connexions au réseau public avec des opérateurs différents.

Ci-dessous les principes de connexion en place :

- Chaque DC est connecté au minimum à deux autres DCs ;
- Par l'intermédiaire d'un réseau privé MPLS ;
- Avec 10 Gbps de connectivité inter sites ;
- Et 30 Gbps de connexion partagée vers Internet.



Dans cette configuration, les datacenters jumeaux Seclin/La Pointe et Seclin/Dassault, sont équivalents aux exigences du niveau Tier IV de l'Uptime Institute et fournissent une solution de gestion d'un site primaire et de secours.

## 7.5 Plan de Continuité des Services du GAR sur plusieurs sites actifs

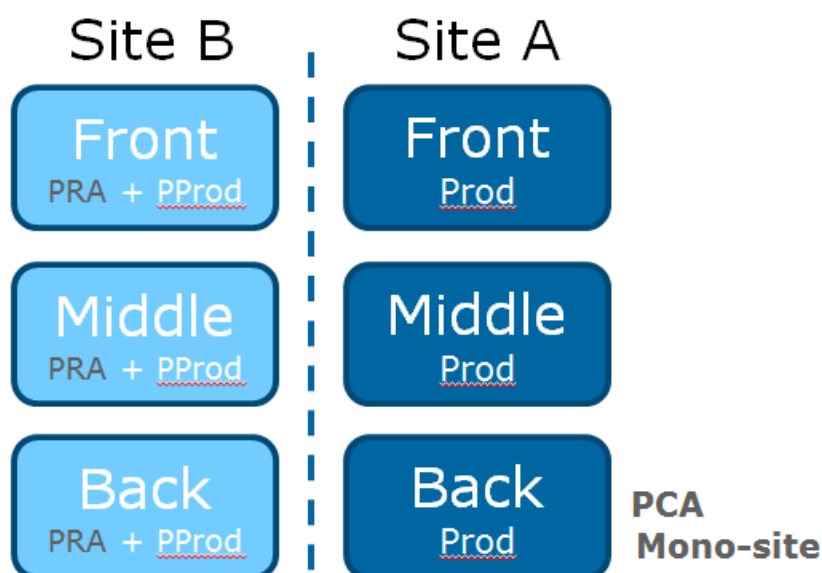
Dans le plan de continuité des services du GAR, une redondance sur l'ensemble des composants techniques permet de garantir un maintien du service malgré la perte unitaire d'un composant. Les mécanismes mis en œuvre sont listés ci-dessous :

Incident	Composants Techniques	Mécanisme de redondance
Mineur	Perte d'une liaison réseau	Protocole BGP Actif/Passif
Mineur	Perte d'un routeur d'aboutement LS	Protocole VRRP Actif/Passif
Mineur	Perte Firewall Front	Cluster Cisco Actif/Passif
Mineur	Perte Firewall Back	Cluster CheckPoint Actif/Passif
Mineur	Perte d'un switch réseau vLAN N2	Double raccordement N2 des serveurs LACP
Mineur	Perte d'un serveur répartiteur de charge	HA VMWare et VRRP
Mineur	Perte d'un serveur VM Front office	HA VMWare et répartiteur de charge LVS
Mineur	Perte d'un Serveur VM Middle office	HA VMWare et répartiteur de charge Modjk
Mineur	Perte d'un serveur base de données	Cluster Group Réplication MySQL
Mineur	Perte d'un serveur base de données	Cluster MySql master/failover

Mineur	Perte d'une alimentation électrique	Doublement des chaînes onduleur d'alimentation des baies du datacenter Classement Uptime Institut Tiers III+
Mineur	Perte de l'alimentation électrique de notre fournisseur Enedis	Groupe électrogène datacenter Tiers III 99.98% de taux de disponibilité
Majeur	Perte complet du DataCenter (Sinistre majeur)	Solution de reconstruction des services de production sur la pré-production via le PRA

### 7.5.1 Description du Plan de Reprise d'Activité

En cas de sinistre majeur sur le datacenter de Seclin/Dassault hébergeant l'environnement de production du GAR, un second datacenter qui héberge l'environnement de pré-production Seclin/La Pointe (appelé site de secours) reprend les services de production. La solution proposée repose sur la présence d'un second site hébergeant l'environnement de **pré-production Seclin/Lapointe** qui est dimensionné à l'identique de la production. Il permet de pallier la survenue d'un sinistre majeur sur le datacenter de **production Seclin/Dassault**.



### 7.5.2 Périmètre et impact du Plan de Reprise d'Activité

- **Périmètre du PRA**

Ce plan de reprise d'activité est applicable uniquement sur l'environnement de production. En cas de perte du Datacenter de production, il est à noter que les statistiques du GAR perdront l'historique des indicateurs. En outre, le PRA ne prend pas en compte les services de Support GAR (JIRA SD, Confluence).

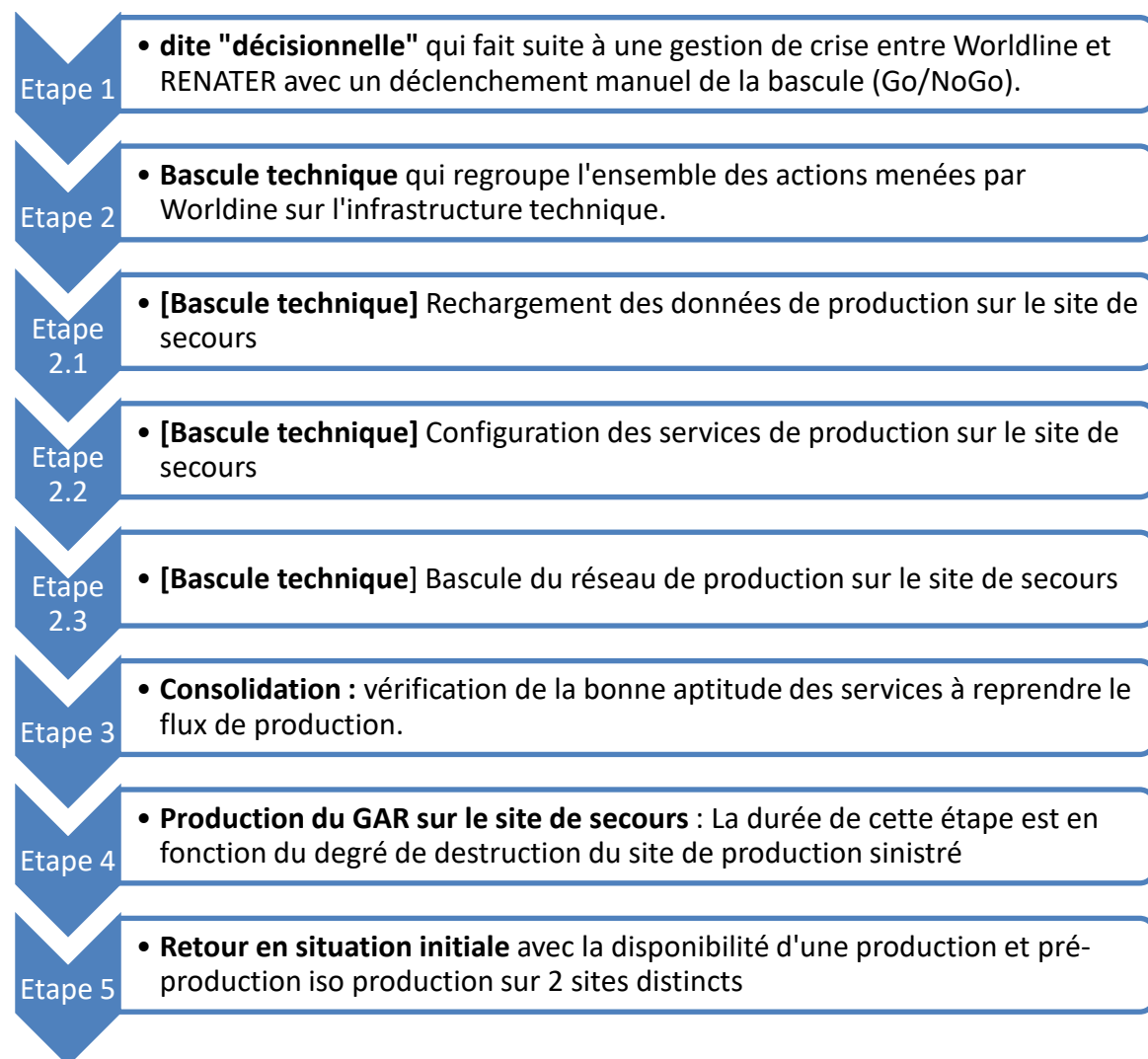
- **Impact du déclenchement du PRA**

Le Plan de Reprise d'Activité lors de la bascule supprime l'environnement de pré-production. Les services et les données de pré-production ne sont plus accessibles et sont remplacés par les services et données de production. Les autres environnements hors pré-production restent disponibles. La nouvelle production est alimentée par les données de production de la dernière sauvegarde, soit la dernière sauvegarde à J-1 à 04h00.

### 7.5.3 Principe du Plan de Reprise d'Activité

#### *Les différentes étapes du Plan de Reprise d'Activité*

Le Plan de Reprise d'Activité est composé de plusieurs étapes pour garantir un retour à la normale des services de production.

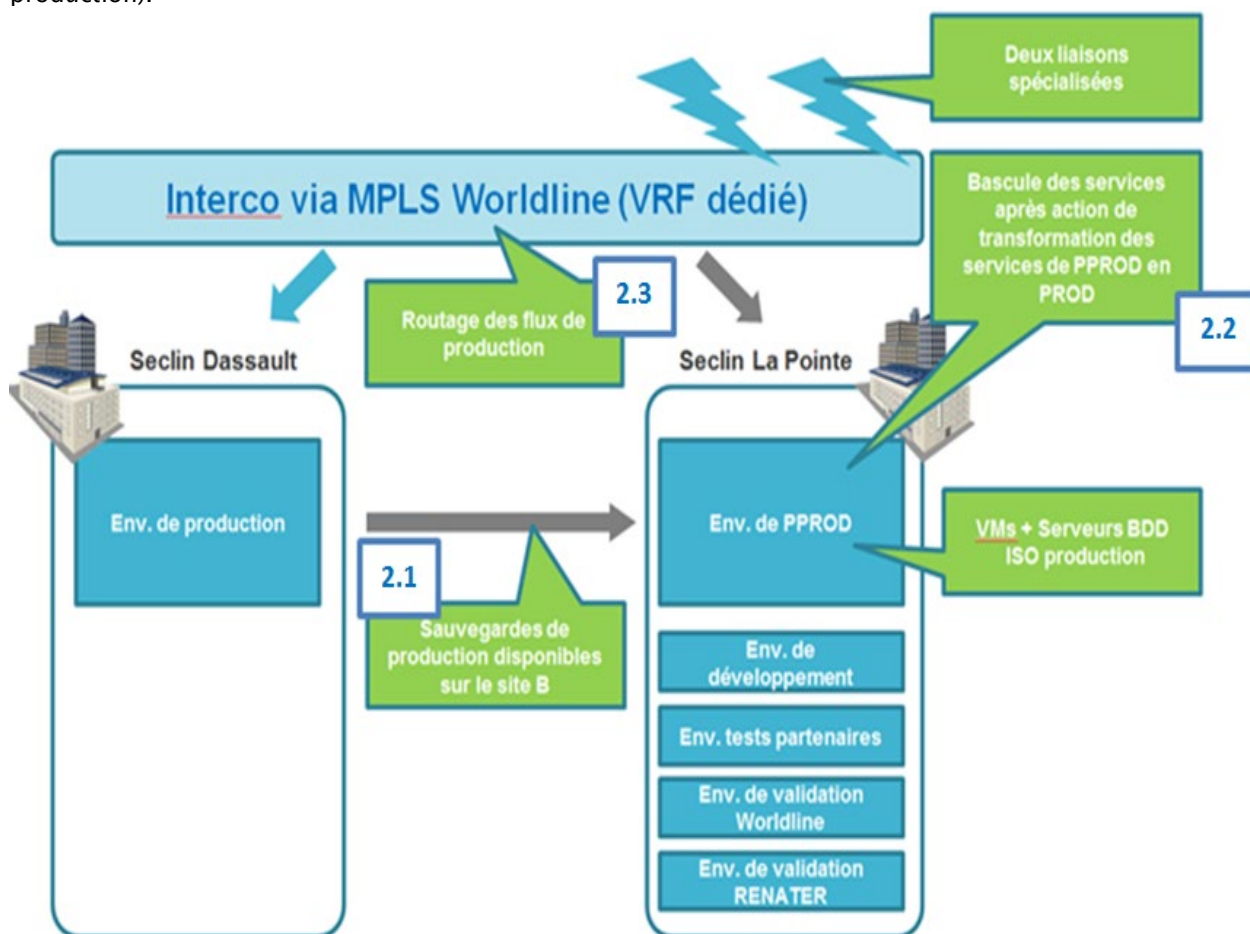




### Schéma explicatif des étapes 2.1, 2.2 et 2.3

L'infrastructure technique permet d'aboutir les deux liaisons réseaux sur nos deux sites Seclin/Dassault & Seclin/Lapointe. Le réseau MPLS Worldline permet de router le flux des liaisons spécialisées vers l'un des deux sites.

Les services de production du GAR sont hébergés sur le site de Seclin/Dassault (Site primaire). Les services hors production du GAR sont hébergés sur le site de Seclin/Lapointe (Site de secours de production).





## 7.7 DESCRIPTION DU PLAN DE REPRISE D'ACTIVITE

### 7.7.1 Etape 1 – Décisionnelle

Dans cette étape, Worldline et RENATER prennent la décision, dans le respect du process de gestion de crise décrit dans notre Plan d'Assurance Qualité, de déclencher le Plan de Reprise d'Activité lors de l'apparition d'un sinistre majeur, tel que la perte du Datacenter avec un arrêt complet du site de production qui héberge le GAR.

Lors de cette réunion de crise, un état des lieux précis de la disponibilité des services et des dates de rétablissement des services non disponibles sur le site primaire sont estimées, afin que Worldline et RENATER puissent prendre la décision d'exécuter la procédure de bascule de l'activité des services du GAR sur le site de secours.

### 7.7.2 Etape 2 – Bascule technique

#### 7.7.2.1 Etape 2.1 – Bascule base de données

##### ***Dispositif d'un système de sauvegarde croisée sur les deux sites***

Le rechargement des données de production sur les serveurs de bases de données de pré-production est facilité par la solution de sauvegarde mise en œuvre. Cette solution est basée sur une suite logicielle de la société Commvault®.

En voici les grands principes :

- Toutes les sauvegardes des bases de données de production sont transférées sur une librairie de sauvegarde située sur le même site.
- Les données sauvegardées sont copiées de façon asynchrone sur une seconde librairie de sauvegarde, située sur le site hébergeant l'environnement de pré-production
- Il est ensuite possible de restaurer ces sauvegardes sur les serveurs de pré-production grâce aux agents/clients déployés sur ceux-ci.

Un environnement CommCell est un regroupement logique des composants logiciels qui protègent, déplacent, stockent et gèrent les données et les informations. Un environnement CommCell contient un serveur CommServe, un ou plusieurs MediaAgents et un ou plusieurs clients.

- **Rechargement des données de production sur la pré-production**

Les serveurs de pré-production ont les mêmes caractéristiques techniques que ceux de production (CPU, RAM, HDD), ils sont en capacité d'accueillir l'usage des services de production. Des tests de restaurations pour estimer les durées de traitements ont été réalisés à cette étape en 7.8.1.1. Une copie complète de l'ensemble des données est effectuée à l'issue de cette étape technique avec une fraîcheur de la donnée conforme au RPO annoncée dans notre engagement.

### 7.7.2.2 Etape 2.2 – Bascule des services

Dans cette étape technique, Worldline livre l'ensemble des configurations, des services et des certificats SSH/SSL pour pouvoir transformer les services de pré-production en service de production. Cette livraison s'appuie sur nos outils de gestion de configuration OPS présents sur nos différents sites.

De manière exhaustive, Worldline procède aux modifications suivantes sur les serveurs de pré-production :

- Livraison de la même version du GAR que la production (si nécessaire, normalement iso production) ;
- Livraison des clefs SSH et des certificats SSL de production sur la pré-production (GitLab/OPS).
- Ajustement des configurations de pré-production :
  - Modification de la configuration des reverse Proxy NGINX au niveau certificat SSL ;
  - Modification de la configuration des serveurs SFTP au niveau certificat SSH
  - Rechargement des metadonnées/d'entity-id sur la pré-production

L'ensemble des configurations des services du GAR sont présentes dans nos outils de configuration OPS/GitLab. Ils doivent être adaptés pour pouvoir reconfigurer la pré-production en production en utilisant les certificats SSL/SSH de production.

Id	Services	Type
1	Accès aux Ressources	Service
2	IHM affectation	Service
3	Batch Import	Batch
4	WS List Ressources	Service
5	Collecte Données ENT	Service
6	Moissonnage	Batch
7	Post import	Batch
8	Post Moissonnage	Batch
9	WS Abonnement	Service
11	Portail GAR	Service
12	Rapport affectation	Service
13	Génération des vignettes	Service
15	Liste Etablissement	Service
16	Pré affectation	Batch
17	Statistiques	Service
18	WS Données d'initialisation	Service
19	Conservation identifiant opaques	Service
20	Page de consentement	Service
21	WS Ressources affectées à l'accédant	Service
22	WAYF	Service
23	Médiacentre GAR	Service
24	Pré-Collecte	Service
25	WAYF natif	Service

### 7.7.2.3 Etape 2.3 – Bascule réseau

Sur l'architecture réseau actuellement en place :

- Les flux de production transitent via le POP Lille1, liaison Eurafibre aboutement Seclin/Dassault.
- Les flux de pré-production/qualification transitent via le POP Paris2, liaison spécialisée Colt aboutement Seclin/Lapointe.

La perte d'un lien, fait automatiquement basculer les flux concernés sur l'autre. Chaque flux rejoint ensuite son firewall nominal. Ce mécanisme de bascule a déjà été éprouvé plusieurs fois, notamment lors d'interventions par les opérateurs télécom lors des bascules des liaisons spécialisées.

Concernant les résolutions DNS, deux serveurs en actif/actif en sont en charge, un Master, sur l'environnement de production (*npren01s*), et un Slave, sur l'environnement de pré-production (*neren01s*). Ils sont répartis sur les deux datacenters pour assurer cette fonctionnalité DNS lors de la perte du site de production.

#### **Passage en PRA**

Suite à la perte complète du datacenter de production, la bascule au niveau des LS est alors automatique.

Dans cette étape de bascule réseau et afin d'honorer les demandes de connexion, les actions suivantes sont nécessaires :

- **Au niveau Routeur**

Modifier le routage du scope d'adresses IPs publiques de production vers le firewall frontal de Pré-production.

- **Au niveau Firewall**

Mettre en place, dans le firewall frontal de pré-production, les translations des adresses IPs publiques de production vers les adresses IP internes des services de pré-production.  
Autoriser les flux sur ce firewall.

#### 1.1. - Etape 3 – Consolidation

À cette étape, l'ensemble des actions techniques sont terminées. Les services de production sont de nouveau disponibles.

Worldline procède à la vérification de l'ensemble des supervisions techniques et métiers des services en production pour garantir la bonne mise en supervision du GAR.

#### 1.2. - Etape 4 – Retour en situation initiale

En fonction du degré de destruction du datacenter sinistré, deux solutions sont envisageables :

- **Solution 1** : Bascule du site de secours vers le site de production initial après remise en état de la production sur le site de production initial ;
- **Solution 2** : Conservation de la production sur le site de secours qui deviendra le nouveau site de production.

#### **Solution 1 de retour arrière**

D'un point de vue technique, la solution 1 se décompose en deux étapes :

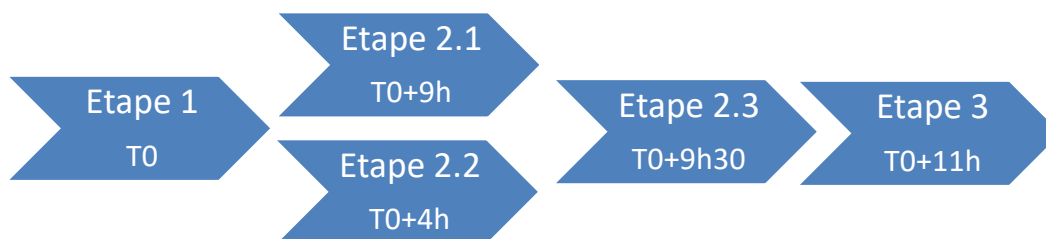
- Etape de reconstruction de la production estimée sur plusieurs mois en fonction du degré de destruction du site sinistré.
- Etape de bascule nécessite une recopie à froid de l'ensemble des données avec un impact sur le service de production estimé à 24 heures (identique à la bascule technique PRA en action et en durée, mais inversée dans le sens site de secours vers production initiale).

### ***Solution 2 de retour arrière***

La solution 2 consiste à pérenniser la transformation du site de secours en nouveau site de production. Dans ces conditions, Worldline devra proposer un planning de construction d'un nouvel environnement de pré-production sur le site sinistré ou sur un autre datacenter disponible dans nos infrastructures en France.

#### **1.3. - Horodatage des différentes étapes**

En prenant comme T0, la décision de bascule de la production vers le site de secours, nous estimons le chronogramme suivant de remise en service du GAR.



#### ***Etape 2 Bascule technique***

- ❖ **Etape 2.1** : Récupération des données de production
  - Temps de rechargement des données J+1 estimé à environ 9 heures
- ❖ **Etape 2.2** : Récupération des services de production
  - Temps de bascule des services de production estimé 4 heures
- ❖ **Etape 2.3** : Bascule du flux réseau de production
  - Temps de bascule réseau estimé à 30 minutes
- ❖ **Etape 3** : Consolidation
  - Temps de vérification et mise en supervision estimé à 1 heures 30

## 7.8 ANNEXES

### 7.8.1.1 Annexe 1 : Durée du rechargement base de données

Les durées de rechargement des bases de données hébergées sur l'infrastructure saison 2, MySQL8, ont été mesurées à l'occasion du test de PRA exécuté au mois de Juillet 2022.

- ❖ Dans le cadre du test de PRA exécuté au mois de Juillet 2022, nous reprenons une sauvegarde des données de production que nous transférons sur la pré-production pour effectuer un rechargement des données iso production. Nous effectuons par la même occasion un test de restauration des données de production sur la pré-production.
- ❖ Les valeurs indiquées ci-dessous sont basées sur les volumétries des données stockées en BDD en date du 11 juillet 2022.

Instance	Récupération des données (HH :MM)	Chargement des données (HH :MM)	Total (HH :MM)
mypren13s	01:54	02:00	03:54
mypren12s	00:25	00:15	00:40
mypren11s	00:32	00:02	00:34
mypren03-04	00:15	00:25	00:40
<b>Total</b>	<b>03:06</b>	<b>02:42</b>	<b>05:48</b>

## 7.9 Volumétrie

### 7.9.1 Hypothèses d'usage de la solution GAR

Voici les hypothèses de volumétrie de la solution GAR :

	2019-2020	2020-2021	2021-2022	2022-2023	2023-2024	2024-2025
Nombre d'accédants *	5 000 000	7 000 000	9 000 000	11 000 000	13 000 000	15 000 000

\* Un utilisateur accédant est un utilisateur intégré dans les bases de données du GAR (élèves, enseignants, autres personnels).

#### **Hypothèse d'interconnexion :**

La majorité des requêtes émises par les ENT pour interroger le Webservice de liste des ressources (cf. [DR7](#)) seront réalisées à travers un pool de connexion https établi par l'ENT client du Webservice.

### 7.9.2 Analyse des besoins réseaux de la solution

Une analyse a été réalisée pour estimer les flux réseaux entre la plateforme GAR et les éléments pouvant la contacter.

Une distinction a été faite entre les flux entrants et sortants de la plateforme.

Les hypothèses générales sont :

- Les échanges d'authentification sont réalisés avec le protocole CAS dans cette estimation ;
- Les transferts de données des ENT pour les imports d'identité sont réalisés en dehors des heures de pointe ;
- Les moisonnages d'entrepôts sont réalisés en dehors des heures de pointe ;
- Les flux d'échange d'abonnements avec les éditeurs ont un poids négligeable.

Les hypothèses de volumétrie sont :

- 3,3 millions d'élèves et d'enseignants accédants ;
- 13 950 gestionnaires (gestionnaires administratif, gestionnaires technique, distributeurs technique et commerciaux de ressources, responsables d'affectation) ;
- 5 100 accès gestionnaires simultanés ;
- 2 accès à la liste des ressources par jour par chaque accédant et une estimation du pic journalier à ~833 requêtes par seconde ;
- 6 accès à une ressource par jour par chaque accédant et une estimation du pic journalier à ~2500 requêtes par seconde ;

Les hypothèses de volume des échanges sont :

- Les requêtes émises par un client http d'une application (ENT, Editeur,) ont un poids de 500 octets ;
- Les requêtes émises par un navigateur web (accès à une ressource) ont un poids de 700 octets ;
- Les redirections HTTP 302 (processus d'authentification) ont un poids de 200 octets ;
- Les réponses liées au flux d'authentification pour validation de l'identité ont un poids de 1Koctets ;
- Le flux renvoyé par le GAR pour lister les ressources est de 3Koctets ;
- Le poids des ressources web (css, js, HTML...) sont de 1.5 Moctets pour l'interface d'affectation ;

Une marge d'incertitude de 30% vis à vis des hypothèses est appliquée sur le total.

	Flux entrant			Flux sortant		
	Poids moyen en octet	Nb requêtes en charge/s	Débit en bit/s	Poids moyen en octet	Nb requêtes en charge/s	Débit en bit/s
accès à l'interface d'affectation	10 000	1	80 000	1 500 000	1	12 000 000
Requête émise par l'ENT pour lister les ressources	500	833	3 332 000	3 000	833	19 992 000
Accès aux ressources	2 900	2 500	58 000 000	1 900	2 500	38 000 000
TOTAL Brut			61 412 000			69 992 000
TOTAL avec marge d'incertitude vis-à-vis des hypothèses			79 835 600			90 989 600

Cette estimation montre que les flux présentés sont inférieurs à 100Mbps/s.

L'observation du comportement et de l'adhésion des utilisateurs, ou la remise en cause de nos hypothèses, permettront d'éventuellement augmenter la capacité maximale autorisée. Cette augmentation de débit se fait de manière transparente et ne nécessite pas de construction spécifique. Il s'agit de paramétrage via nos outils d'administration réseau

Le cœur de réseau du GAR traitera un poids de transit de données dans les mêmes grandeurs que les échanges externes au GAR. Un débit de 1Gbits/s semble suffisant pour la croissance de la plateforme.

### 7.9.3 Projections dimensionnement plateforme

Le tableau ci-dessous détaille les projections du dimensionnement de la plateforme GAR (Production et pré production). Le dimensionnement s'appuie sur les hypothèses présentées ci-dessus.

	Nombre de serveurs					
	2020 (5M)	2021 (7M)	2022 (9M)	2023 (11M)	2024 (13M)	2025 (15M)
Loadbalancer	2	2	2	2	2	2
Web	4	4	4	6	6	6
Middle (Application + batchs)	14	14	14	16	16	16
Bdd	9	12	13	14	14	14
Stats logs	11	11	11	12	12	12
Firewall	4	4	4	4	4	4
Dns	2	2	2	2	2	2

## 7.10 Interconnexion avec le réseau RENATER

L'accès aux différentes plateformes GAR se fait au travers d'une interconnexion entre RENATER et Worldline.

Cette interconnexion est opérée par 2 liens 1Gb/s :

- 1 liaison 1Gb/s EURAFIBRE entre notre Datacenter Seclin PMP-Dassault et le POP RENATER LILLE1
- 1 liaison 1Gb/s COLT entre notre Datacenter Seclin La Pointe et le POP RENATER PARIS2 (hébergé chez Telehouse2)

Les Plateformes GAR sont uniquement adressées en adresses publiques attribuées par Renater. La haute disponibilité de cette interconnexion est assurée par le protocole BGP mis en place entre Worldline et Renater.

Renater attribue à Worldline une plage de 255 adresses publiques (/24) sous réserve que Wordline justifie son besoin pour la plate-forme (selon les règles d'attribution d'adresses IP en vigueur au RIPE).

Une partie de ce réseau sera annoncée en BGP par Worldline, en primaire sur le site de Seclin PMP/Dassault pour la plateforme de Production, et en secondaire sur le site de Seclin La Pointe.

L'autre partie de ce réseau sera annoncée en BGP par Worldline, en primaire sur le site de Seclin La Pointe pour les plateformes de Préproduction, Validation fonctionnelle/Tests partenaires et en secondaire sur le site de Seclin PMP/Dassault.

Renater annoncera à Worldline en BGP une route par défaut.

Le schéma ci-dessous décrit l'interconnexion entre Renater et Worldline :

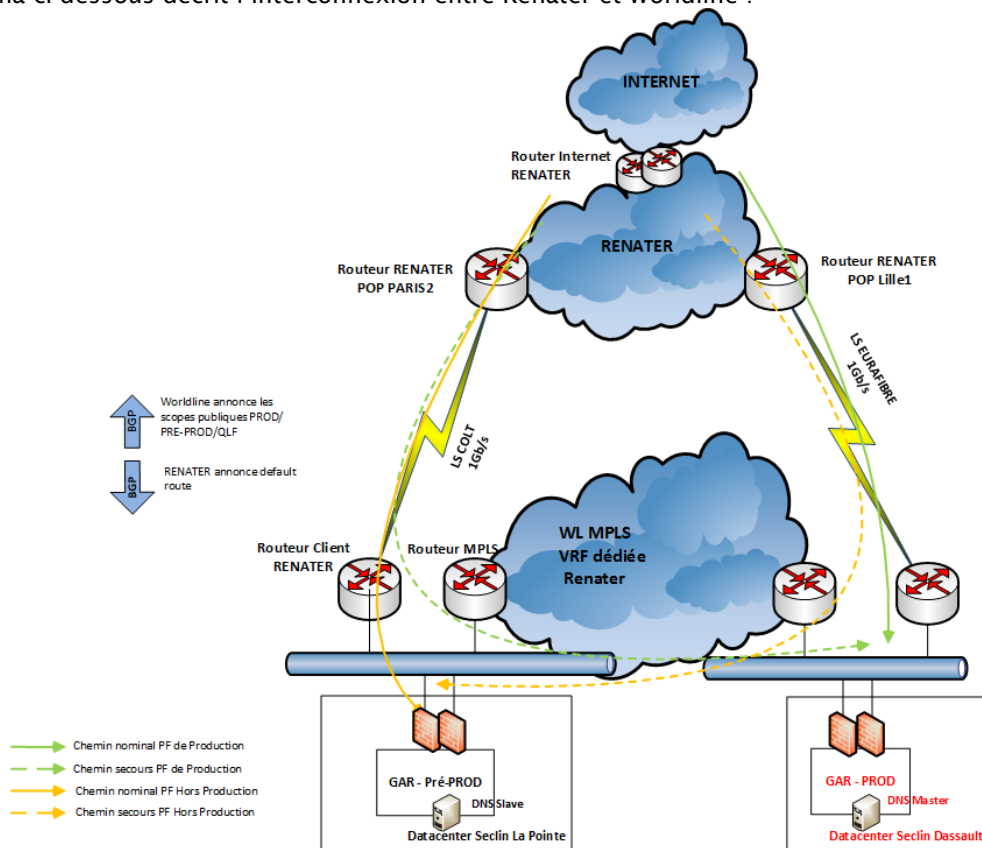


Figure 15 – Interconnexion Renater/Worldline



## 7.11 Référencement IPs publiques

Renater nous attribue une plage de 255 adresses publique (/24), répartie en quatre plages de 64 adresses chacune, une pour la production (/26), une pour la pre-production (/26), une pour la validation fonctionnelle, et la dernière (/26) pour les tests partenaires.

Un fichier de référencement des adresses IPs publiques utilisées sera mis en place par Worldline (cf 8.3 Plan d'adressage des IP publiques).

## 7.12 Stratégie DNS

Renater délègue les zones gar.education.fr, test-gar.education.fr, ainsi que la zone reverse 81.221.195.in-addr.arpa à Worldline.

Deux serveurs DNS dédiés sont installés sur le réseau frontal de production, accessibles tous deux par internet via leurs IPs publiques et sont référencés autoritaires sur les zones déléguées.

Les DNS fonctionnent en mode Master/slave.

La modification des fichiers de zone s'effectue sur le DNS master, le DNS slave télécharge les zones mises à jour sur le master.

## 7.13 Architecture NTP

Worldline met en œuvre deux boîtiers Meinberg Stratum 1, basés, pour l'un à Seclin, et pour l'autre à Francfort. Ces boîtiers sont chacun équipés d'une antenne GPS et d'une antenne DCF. 4 serveurs physiques composent la Stratum 2 et se synchronisent sur la Stratum 1.

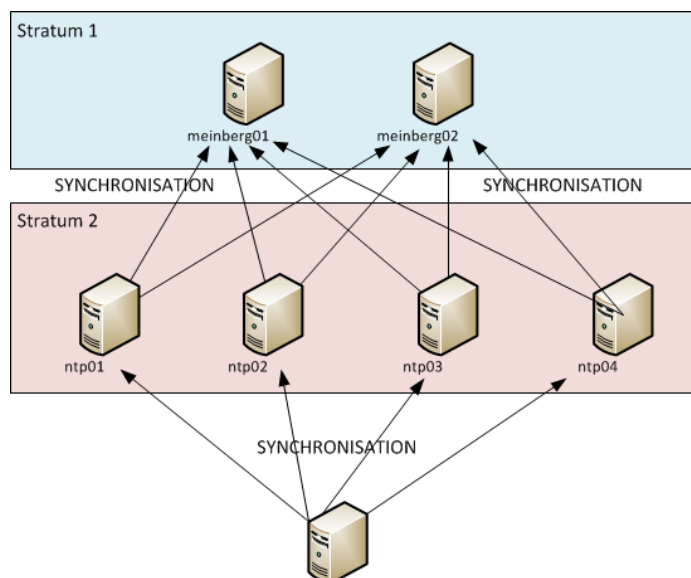


Figure 16 – Architecture NTP

Les équipements finaux sont configurés pour interroger les 4 serveurs de la Stratum 2. L'architecture NTP est PCI ready.

## 7.14 Inventaire plateformes

L'inventaire complet de la plateforme GAR figure dans le document de référence DR30.

## 7.15 Stratégie de mise à jour de composants Redhat/Centos

Le patch management vise à appliquer régulièrement les dernières versions de packages mises à disposition de la communauté Redhat/Centos, sur l'ensemble des environnements d'un projet. Dans cette optique, Worldline met en place sur ses projets (et recommande à ses clients) des planifications de mises à jour mensuelles ou trimestrielles.

À la demande de RENATER, et afin de limiter les indisponibilités et validations fonctionnelles liées à des mises à jour bimensuelles ou trimestrielles, Worldline soumet à RENATER une planification différenciée par zone fonctionnelle.

Les environnements pourraient donc être mis à jour de la manière suivante :

- Trimestriel pour les serveurs Front Virtualisée
- 3 fois par an pour les serveurs applicatifs et de base de données durant les vacances scolaires pour la production :
  - Fin Mars - Début Avril
  - Fin Juillet - Début Août (vacances d'été)
  - Fin Novembre - Début Décembre (vacances de fin d'année)

La période du 15 août au 1 octobre est exclue d'actions de mise à jour afin d'éviter des effets de bord avec la période de pré-rentrée et de rentrée.

Il est à noter que dans le cadre d'une faille de sécurité à appliquer de manière impérative les plateformes hors production seront mises à jour suite à une concertation avec les membres du Comité sécurité (WL/Renater). Pour la plateforme production, la procédure d'eCAB sera engagée pour tracer les opérations de sécurisation.

Vous trouverez pour chaque intervention les impacts des opérations en production (et préproduction) Pour les environnements de PFV et Test Partenaires, il y a une indisponibilité/instabilité des services durant l'ensemble de l'opération à prévoir.

**Tous les trimestres pour la zone Front Virtualisée (nginx, sftp, postfix, loadbalancer) :**

1. Serveur Front - MAJ automatisée en HNO (entre 03h00 et 04h00 hors veille de jour férié) via un outil d'ordonnancement (Webpatching) – sans impact
  - Mardi semaine 1 du premier mois du trimestre : Patch de la Plateforme interne WL
  - Mercredi semaine 1 du premier mois du trimestre : Patch de la Plateforme de Validation Fonctionnelle
  - Jeudi semaine 1 du premier mois du trimestre : Patch de la Plateforme de Test Partenaires
  - Chaque 2ième mardi ouvré du mois : Patch de la Plateforme de Pré-Production (Colonne paire)
  - Chaque 2ième jeudi ouvré du mois : Patch de la Plateforme de Pré-Production (Colonne impaire)
  - Chaque 3ième mardi ouvré du mois : Patch de la Plateforme de Production (Colonne paire)
  - Chaque 3ième jeudi ouvré du mois : Patch de la Plateforme de Production (Colonne impaire)
2. Loadbalancer – Bascule manuelle entre 12h00 et 14h00 afin de valider le fonctionnement – Impact : microcoupure réseau < 1s
  - Chaque 2ième mardi ouvré du mois : Plateforme de Pré-Production - bascule du flux sur le LB patché (slave) afin de valider le fonctionnement
  - Chaque 2ième jeudi ouvré du mois : Patch de la Plateforme de Pré-Production - bascule du flux sur le LB patché (master) retour situation nominale
  - Chaque 3ième mardi ouvré du mois : Patch de la Plateforme de Production - bascule du flux sur le LB patché (slave) afin de valider le fonctionnement
  - Chaque 3ième jeudi ouvré du mois : Patch de la Plateforme de Production - bascule du flux sur le LB patché (master) retour situation nominale

**3 fois par an pour la zone Middle Virtualisée (services GAR)**

MAJ automatisée en HNO (entre 03h00 et 04h00 hors veille de jour férié) via un outil d'ordonnancement (Webpatching) – Impact : perte de session possible

NB : semaine N= la première semaine des vacances scolaires pour au moins 2 zones

- Mardi Semaine N-2: Patch de la Plateforme interne WL
- Mercredi Semaine N-2: Patch de la Plateforme de Validation Fonctionnelle
- Jeudi Semaine N-2: Patch de la Plateforme de Test Partenaires
- Mardi Semaine N-1: Patch de la Plateforme de Pré-Production (Colonne paire)
- Jeudi Semaine N-1: Patch de la Plateforme de Pré-Production (Colonne impaire)
- Mardi Semaine N: Patch de la Plateforme de Production (Colonne paire)
- Jeudi Semaine N: Patch de la Plateforme de Production (Colonne impaire)

**3 fois par an en HNO des serveurs BDD, répli BDD, serveurs DNS\*, des serveurs de stat et serveurs de support**

MAJ Manuelle en HNO (entre 06h00-07h00 et 21h00-22h00 hors veille de jour férié) - Impact : erreur sur les services GAR <1 min, Indisponibilité du support et du portail stats ~1h

NB : semaine N= la première semaine des vacances scolaires pour au moins 2 zones

- Mardi Semaine N-1: Patch de la Plateforme interne WL
- Mercredi Semaine N-1: Patch de la Plateforme de Validation Fonctionnelle
- Jeudi Semaine N-1: Patch de la Plateforme de Test Partenaires
- Mardi Semaine N: Patch de la Plateforme de Pré-Production
- Mardi Semaine N+1: Patch de la Plateforme de Production

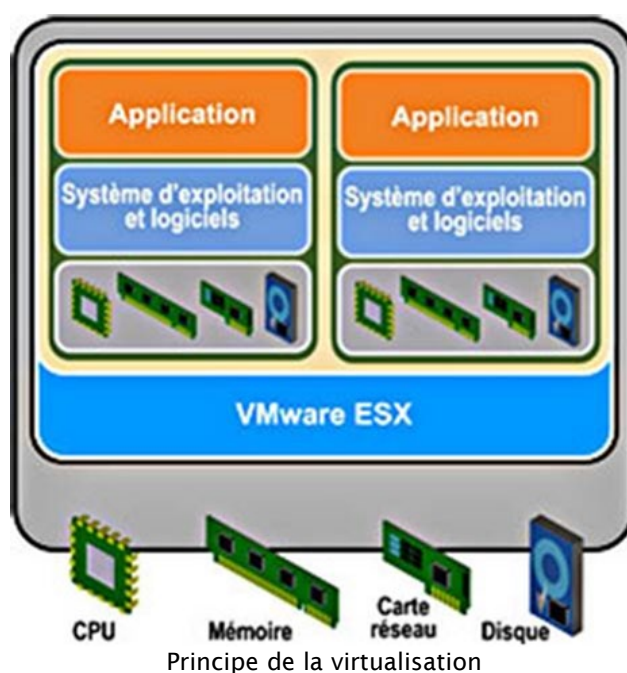
\*les serveurs DNS ne sont présents qu'en production.

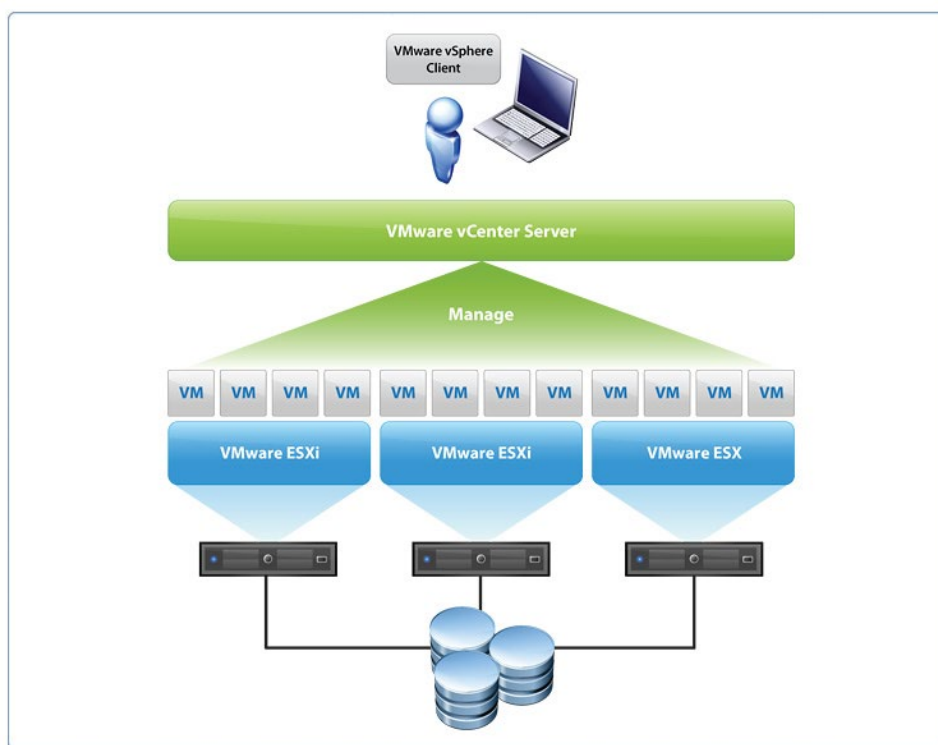
## 8. Annexe

### 8.1 Description offre cloud mutualisé

Notre offre Cloud mutualisée repose sur la Solution VMWare.

La virtualisation nous permet une utilisation efficace et optimale des ressources Hardware fournies par les servers hôtes (ESXi).





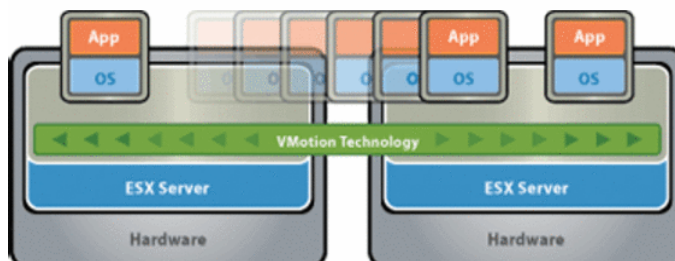
Principe de fonctionnement d'une architecture VMWare

Les ESXi sont composés de serveurs aux capacités RAM et CPU importants (2xCPU 14cores, 512Go RAM).

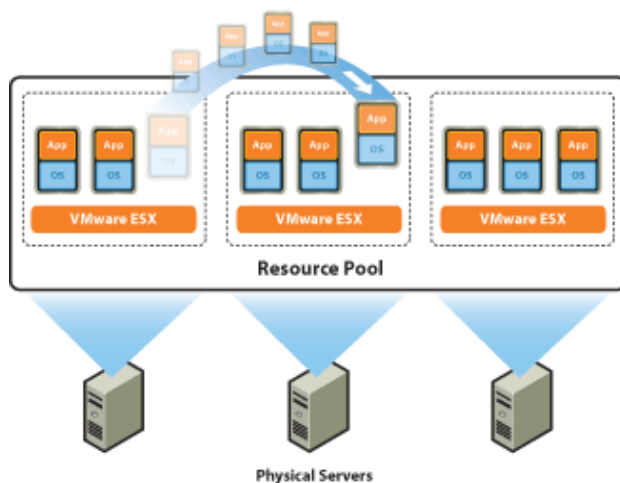
Les datastores sont hébergés sur notre SAN mutualisés ; les images des VM sont stockées sur les datastores. Les ESXi accèdent au SAN via une interface Fiber-channel. Les images étant hébergées sur un stockage centralisé, cela facilite la migration de la VM d'un ESXi à un autre.

Les principales fonctions mises en place qui permettront la souplesse et réactivité de l'infrastructure sont :

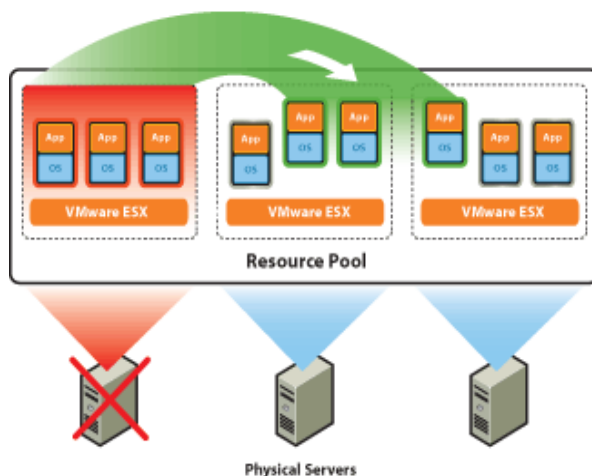
- **vMotion** : permet la migration d'une VM d'un ESXi à un autre sans interruption de service. Ce principe repose sur un réseau privé dédié, ainsi qu'une forte compatibilité hardware entre ESXi ;



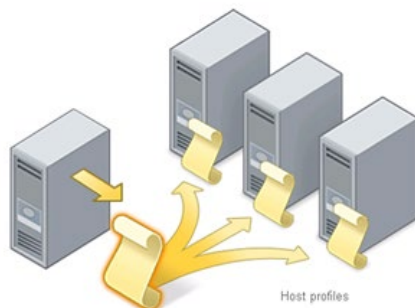
- **DRS** : permet l'automatisation de la répartition des charges sur l'ensemble du cluster. Un calcul est périodiquement fait par le cluster afin de répartir les charges CPU et RAM sur l'ensemble des nœuds du cluster suivant des règles définies par l'utilisateur ;



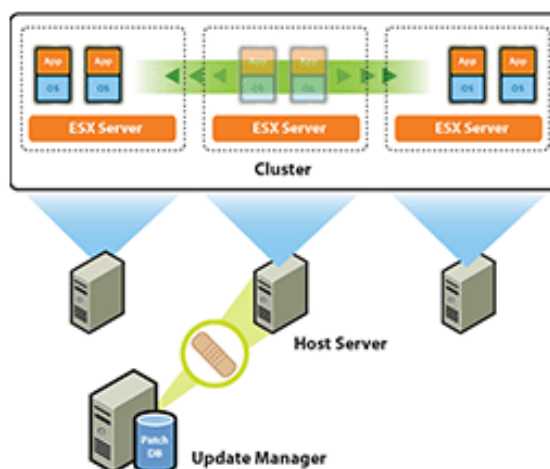
- **HA :** active la haute disponibilité des VM en les réaffectant en cas de panne hardware de l'ESXi. Lorsqu'un ESXi est indisponible, les autres membres du cluster reprennent la gestion des VM crashées ;



- **Host Profiles :** garantit la conformité de l'ensemble des hosts composant le cluster VMware ;



- **VMware Update Manager :** permet la mise à jour des ESXi afin de garantir le plus haut niveau de sécurité des hyperviseurs



***Toutes ces fonctionnalités VMWare sont activées sur notre offre Cloud Mutualisé, l'environnement GAR en bénéficie donc.***

### 8.1.1 ESXi

ESXi est un hyperviseur avec une empreinte réduite (>150Mo) et durcie, ce qui le rend particulièrement robuste dans un environnement de production. Il est à traiter comme une Appliance. Les paramétrages en dur sont restreints, la quasi-totalité étant déportée sur Virtual Center.

### 8.1.2 Virtual Center

Le Virtual Center Server est une application hébergée sur Windows dans une machine virtuelle. L'avantage de placer cette VM dans le cluster est de pouvoir bénéficier des fonctionnalités de souplesse, de redondance et de performances apportés par le cluster HA/DRS. Virtual Center est nécessaire à la construction du cluster, ainsi qu'à sa gestion, mais n'est pas critique. Aucune des VMs hébergées au sein du cluster ne seront impactées si le Virtual Center est indisponible. Également, HA (High Availability), ou le redémarrage des VM en cas de panne, fonctionnera sans problème sans la présence du VC Server.

## 8.2 Matrice de flux

La matrice de flux est définie dans le document de référence [DR24](#).

## 8.3 Plan d'adressage des IP publiques

Le plan d'adressage est défini dans le document de référence [DR25](#).