Dossier d'Architecture Unique

BUILDING TOGETHER
TEAM SPIRIT SOCIETE GENERALE

ITIM – GTS/RET

Ged Data Centric

Cadre de référence	Digital Agence et Big Data
Nom	**Ged Data Centric**
IRT(s)	**A1865**
Trigramme(s)	**GBD**
Criticité métier (STAMP)	**Critique**

Commenté [JMI1]: Correspond à la GED Orchestra existante

Statut : DRAFT

FICHE DE CONTROLE DU DOCUMENT

Caractéristiques du document

Statut	Draft
Réf. Fichier	Modèle DAU - v11 (https://sbc.safe.socgen/docs/DOC-24989)

Création et suivi du document

Assuré dans Jive : https://sbc.safe.socgen/docs/DOC-56916

Intervenants sur le projet

Entité (ou Société)	Domaine de responsabilité dans le projet	Nom

Liste de diffusion

Entité	Nom des destinataires	Objet de la diffusion

CHARTE COULEUR, A UTILISER AVEC MODERATION

EN ROUGE, LES POINTS NON STANDARDS

EN FLUO, LES POINTS NON CLOS AVANT VALIDATION DE LA SOLUTION D'HEBERGEMENT

FICHE DE SYNTHESE DU DOCUMENT

IRT / Trigramme Application	**A1865 / GBD** Ged Data Centric			
Progiciel(s)	**N/A**			
Typologie Architecture	**Big Data**			
D	**I**		**C**	**P**
3	3		2	3
Description de l'Architecture de production				
Site primaire d'hébergement	**Marcoussis Cluster virtuel**			
Site de secours ou secondaire	**Seclin (secours)**			
Modèle d'architecture de résilience	**Rubis (2+1)**			
STAMP	**Critique**			
Plages d'ouverture	**24/24, 7/7**			
RTO	**2h**			
RPO	**< 5 minutes**			
Typologie d'architecture	**Cadre de référence Digital Agence et Big Data**			
Couche métiers	**Composants AWT et Big Data**			
Services d'échanges	**SSOP**			
Serveur d'application	**SpringBoot & PHP/LAMP (hors cadre, pour POC uniquement)**			
Services Données	**Hbase, Elastik Search, HIVE**			
Service ordonnancement	**N/A**			
Zones Cellules Sécurité Réseau (CSR)	**?**			
Systèmes d'exploitation	**Linux Red Hat 7.2 ?**			
Conformité standards et politique	**Durcissement OS :** ☐ advanced ☐premium ☑ premium+ (à partir de l'homologation)			
Offres GTS	**RET : Cloud Interne pour la VM de service** **+ Cluster dédié pour l'architecture Big Data** **ITIM : SSOP**			**…**
Servitudes	**Sauvegarde standard (Inclus offre Cloud GTS)** **Supervision standard Nagios / Patrol**			**…**
Ressources réseaux	**Inclus offre Cloud GTS**			
Poste de Travail	**NDG - IE11 minimum**			**…**
Processus de livraison des packages applicatifs en production	**Package Applicatif Autoporteur (PAAP)** **A voir pour la partie Big Data**			

Dans le paragraphe 1.2.2, le récapitulatif des besoins déclinés par offre et par environnement et par site.

JALONS DU PLANNING		
CVT-I	**05/12/2017**	
CVT-q / -qa	**XX/XX/XXXX**	
CVT-x	**XX/XX/XXXX**	
Installation en développement	**XX/XX/XXXX**	
Mise en Homologation-x	**XX/XX/XXXX**	
Mise en Production	**XX/XX/XXXX**	

TABLE DES MATIERES

1 INTRODUCTION

L'objet de ce document est de présenter :

- Le contexte du projet
- L'architecture applicative choisie pour répondre aux besoins métier
- L'architecture technique et d'hébergement permettant de la déployer
- La réponse aux exigences de sécurité

Ce document décrira également les ressources techniques de l'application GED Data Centric à mettre en œuvre et validée par les différents acteurs (ITIM et GTS/RET) dans le cadre du projet GED Data Centric. Il doit contenir la liste exhaustive des besoins, des choix d'architecture et des ressources matérielles (serveurs, RAM, CPUs, interfaces réseaux données, interfaces stockage et sauvegarde) à mettre en place pour assurer le fonctionnement, la sauvegarde et le secours éventuel de l'application.

Dans une démarche de co-construction ITIM & GTS/RET, ce document couvre un périmètre s'étendant de la conception générale de l'application à l'implémentation de l'infrastructure. Il a vocation à ne décrire que les spécificités du projet qui ne sont pas déjà décrites par ailleurs :

- Le cadre de référence Digital Agence est la référence pour toute information non décrite spécifiquement ici
- La topologie détaillée de l'application est décrite via le PAAP, et ne sera pas reprise ici.

2 GENERALITES

2.1 Contexte et enjeux du projet

Le projet « GED Datacentric » est un POC, qui vise à prouver la capacité d'une nouvelle architecture dite « GED Datacentric » a remplacer la plateforme GED actuelle (GED Orchestra), qui est basée sur le progiciel Documentum Content Server.

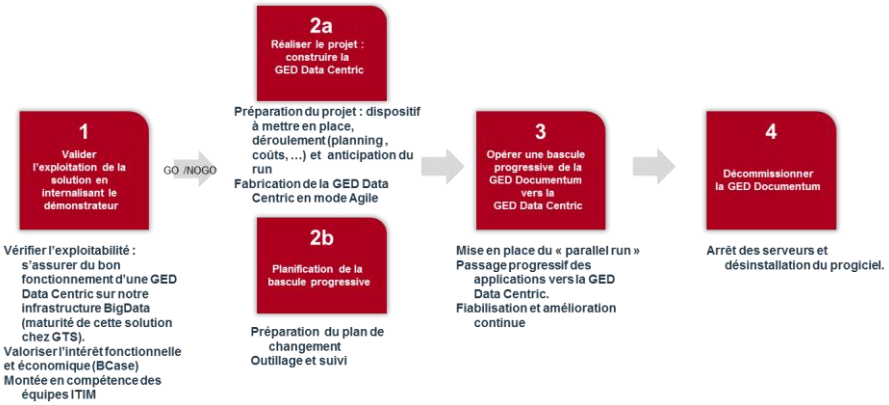
Périmètre :

EXIGENCES FONCTIONNELLES	• **Une couverture quasi-complète** des fonctionnalités actuelles des GED opérationnelles et ce de manière native. • Ces fonctionnalités sont exploitables avec des **technologies modernes** : API natives et catalogue d'API riche, interface d'administration moderne et complète, outils de déploiement..
EVOLUTIVITÉ	• La solution testée s'appuie sur une base documentaire de nouvelle génération (Technologie NoSQL) qui offre une **évolutivité fonctionnelle sans impacts forts** sur l'existant • Grâce à des **fonctions standards**, elle offre aussi des opportunités de **déploiement de fonctionnalités avancées** de type: analyse et contrôle du patrimoine documentaire, accès documentaire étendu, recherche de document, LAD/RAD, historisation native des changements
SCLABILITÉ ET ROBUSTESSE	• La solution testée a prouvé sa **scalabilité logicielle** et sa **performance.** Elle est extensible par des **mécanismes natifs** des technologies Big Data (clusterisation) • Elle offre la possibilité de **réduire le coût total de possession** des documents grâce à l'utilisation d'une infrastructure technique s'appuyant sur des serveurs de moyenne gamme (Commodity hardware moins cher)

Nom de l'application	Ged Data Centric
Code IRT (1)	A1865
Trigramme	GBD
Enseigne	BDDF, CDN et GTPS : RBDF
Métier	
Entité Maitrise d'Œuvre	ITIM/CSM/ADN PPSI : Mathieu Dupitier
Positionnement	Refonte de la GED

2.2 Lotissement / Macro Planning

Le projet est prévu en 4 étapes clés :



3 COMPREHENSION DES BESOINS

3.1 Cartographie fonctionnelle générale

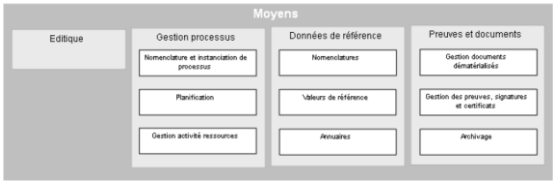


Figure 1: zone "moyens" du modèle fonctionnel « banque de détail »

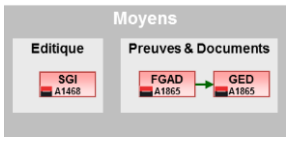


Figure 2: zoom sur les flux

3.2 Niveaux de criticité de l'application

3.3 Niveaux de service

3.3.1 Plage d'ouverture de service et disponibilité

Plages d'ouverture	24h/24h, 7j/7j
Plages de disponibilité	24h/24h, 7j/7j
Interventions	Les interventions se feront le dimanche pour limiter au maximum l'impact client.

3.3.2 Volumétrie et durée de rétention

Préciser s'il s'agit d'hypothèses, de chiffres constatés dedans ou en dehors de votre contexte Société.

Volume de données stockées	Volume de données en augmentation, estimation à 150 To en 2020
Volume de logs quotidien	?
Durée de rétention des logs	?
Nombre de hits / s	200 hits / s (extrapolé des stats de B@D)

3.3.3 Performances

Attente de retour du service synchrone < 1s pour l'injection, la recherche et la restitution.

3.4 Population impactée

3.4.1 Identification et nombre des utilisateurs

Population	Description	Nombre
CDN	Tous les acteurs réseaux France	10 000
GTPS		
BDDF	Tous les acteurs réseaux France	20 000
Clients finaux	Potentiellement tous les clients BDDF et CDN	10 millions
Total		**10 millions**

3.4.2 Poste de travail utilisateur

L'accès se fera :

- Via le Poste de travail (NDG), au travers du site web PHP/LAMP

3.5 Besoins en mécanisme de sécurité

3.5.1 Authentification / Identification

SAFE

3.5.2 Contrôle d'accès / Habilitation

Rôles RTFE transmis par SAFE sur l'API de login.

L'application étant stateless / sessionless, et es rôles étant nécessaire pour le traitement de toutes les requêtes utilisateurs, ils seront persistés au travers du jeton JWT échangé entre le navigateur et le serveur. Le scellement dans le jeton assurera l'intégrité de ces informations.

Pour les détails concernant les rôles et populations d'utilisateurs, on se reportera aux dossiers d'inscription SAFE et fiche GHABI :

https://sbc.safe.socgen/docs/DOC-57843

https://sbc.safe.socgen/docs/DOC-57854

3.5.3 Imputabilité / Audit

Décrire les attendus TCO

Traçabilité applicative standard – pas de besoin métier exprimés au-delà de TCO.

3.5.4 Non répudiation

Décrire les mécanismes assurant la preuve d'origine et de réception.

3.5.5 Disponibilité

Décrire les mécanismes pour répondre aux besoins du « cut-off » et du RTO ainsi qu'à la sauvegarde dans le cadre du plan de secours, etc.

3.5.6 Sauvegarde / archivage

Snapshot à minima toutes les 24h pour être capable de restaurer les VM et leur contenu, en particulier la base de données HBASE & le données dans ELK.

4 Architecture technique

4.1 Architecture technique

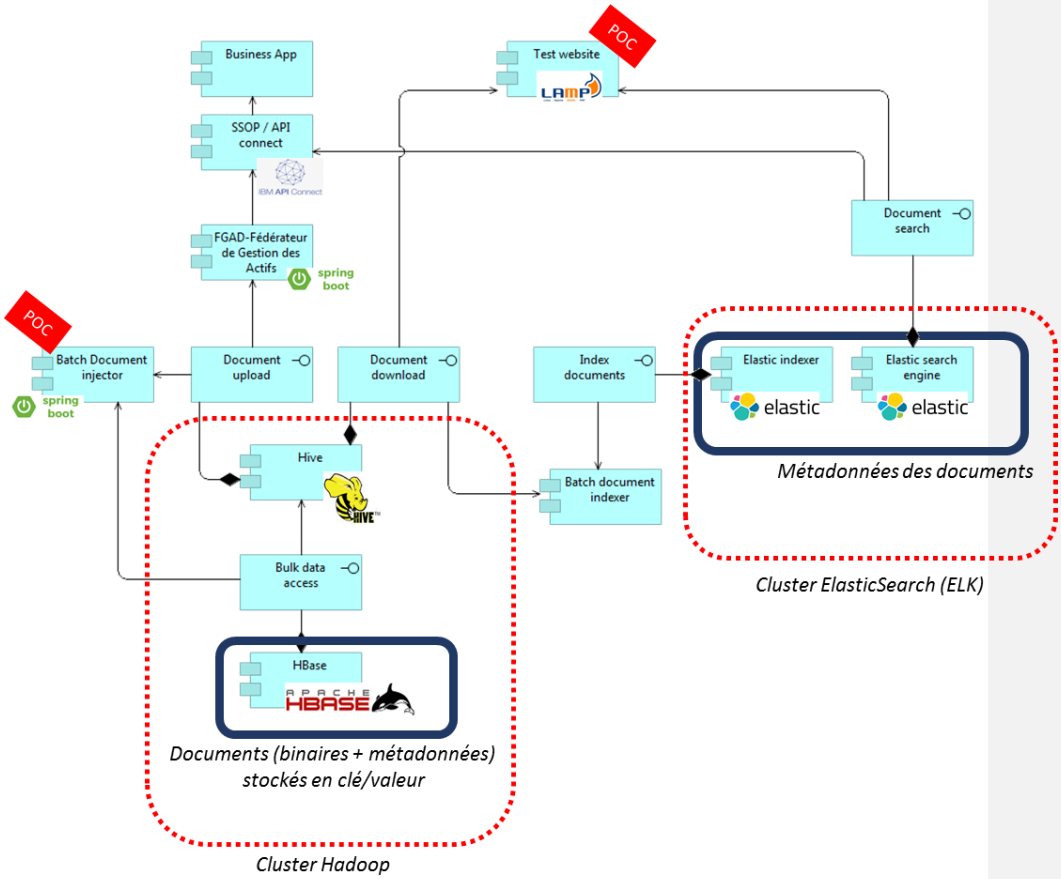


Figure 3: architecture "application layer"

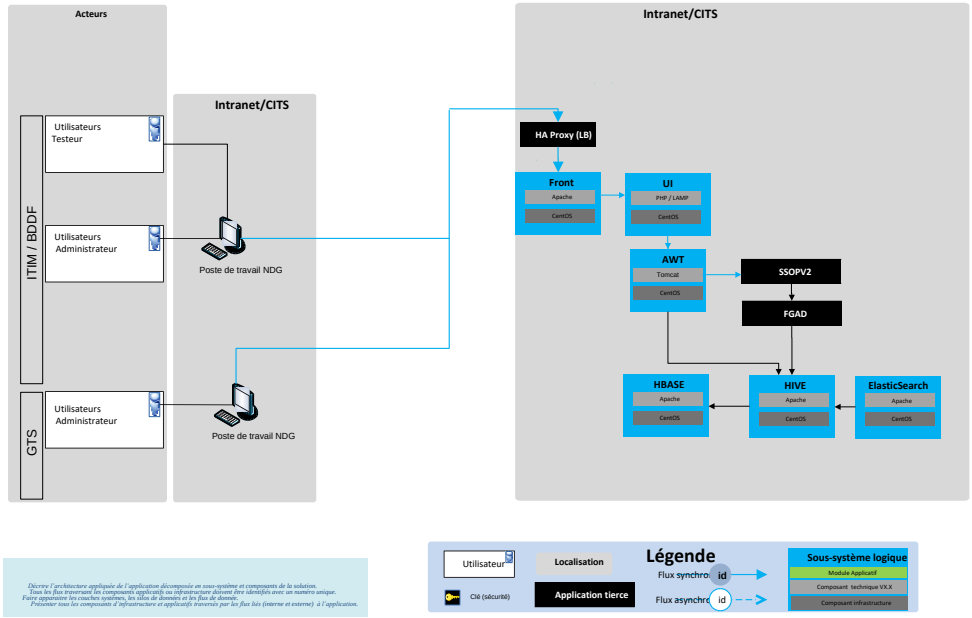


Figure 4: architecture appliquée

4.2 Description des composants

4.2.1 Composants propriétés de l'application GED Data Centric

Composant	Version	Description
HAProxy	A préciser	Ce composant n'est pas représenté mais est suggéré dans le schéma ci-dessus. Il permet une répartition de charge de niveau 4 entre les frontaux http. Les services applicatifs sont entièrement stateless La répartition L4 peut donc se faire sans introspecter le flux, en round robin simple. Note : la dernière terminaison SSL se fait au niveau des frontaux http. Le flux est chiffré en amont et en aval de l'HAProxy.
Apache	2.4+	Le frontal http a 3 rôles : - Authentification de l'utilisateur : la valve SAFE est configurée à ce niveau. Seules les requêtes portant le jeton SAFE d'authentification sont autorisées à traverser le frontal vers le serveur d'application. - Servir les ressources statiques : les ressources ne sont pas déployées sur le frontal, mais il est configuré en mode « proxy-cache » : tout objet de type ressources statique sera servi la première fois par le serveur d'application, mis en cache par Apache, puis servies directement par Apache. - Terminaison SSL : la topologie proposée instancie un Apache par Tomcat, sur la même machine.
PHP/LAMP		IHM Utilisateur final (hors cadre, pour le POC uniquement)
Tomcat/AWT		Permet l'exposition des APIs d'appel de FGAD aux fonctions de GED (HBASE / HIVE / ELK)
HBASE		

Composant	Version	Description
HIVE		
ElasticSearch		

4.2.2 Composants applicatifs sollicités par l'application GED Data Centric

Composant	Description
SSOP	Gateway SOA assurant les rôles décrits dans le cadre de référence Digital Agence (voire section OBA)
SAFE	Système d'authentification

4.3 Description des flux / des échanges

Réf	Description du flux	Emetteur (IRT)	Récepteur (IRT)	Format d'échange	Mode d'accès	Type d'accès	Fréq.	Tiers (*) d'intermédiation	Type (**) d'intégration	Commentaire
1	Echanges entre le navigateur et le frontal http	NDG	BPD (A5139)	HTTPS	Synchrone	Unitaire	TR	HAProxy	Open-Open	Navigation dans l'application Web BPD
2	Echanges entre le navigateur et l'écosystème SAFE	NDG	SAFE	HTTPS	Synchrone	Unitaire	TR	N/A	Open-Open	
2bis	Echanges Apache > SAFE	NDG	SAFE	HTTPS	Synchrone	Unitaire	TR	N/A	Open-Open	Récupération des rôles
3	Apache > PHP/LAMP	Apache	LAMP	HTTP	Synchrone	Unitaire	TR	N/A	Open-Open	
4	Tomcat > HIVE	Tomcat	HIVE	HTTP	Synchrone	Unitaire	TR		Open-Open	
5	ELK->HIVE	ELK (indexer)	HIVE	HTTP						

(*) SER/SSOP, SER/SGE, SER/PRTF, Comporsys/IMSConnect, file MQ, transfert de fichiers, aucun

(**) Il faut distinguer :
1. Les appels de service mainframe depuis le mainframe : CICS-CICS, CICS-IMS, IMS-CICS, IMS-IMS, IMS-Batch
2. Les appels de service mainframe depuis le monde Open (PdT, application Web – par opposition à mainframe) : Open-CICS, Open-IMS

3. Les appels de service web depuis le mainframe : CICS-Open, IMS-Open
4. Les appels de service web depuis le monde Open
5. Les chaînages d'IHMs entre 2 applications Open
6. Les échanges de messages : Open-CICS, Open-IMS, CICS-Open, IMS-Open, CICS-IMS, IMS-CICS, Open-Open
7. Les échanges de fichiers : internes mainframe, Open-mainframe, mainframe-Open, Open-Open

Voir : Topologie, flux, protocole, port, matrice des flux

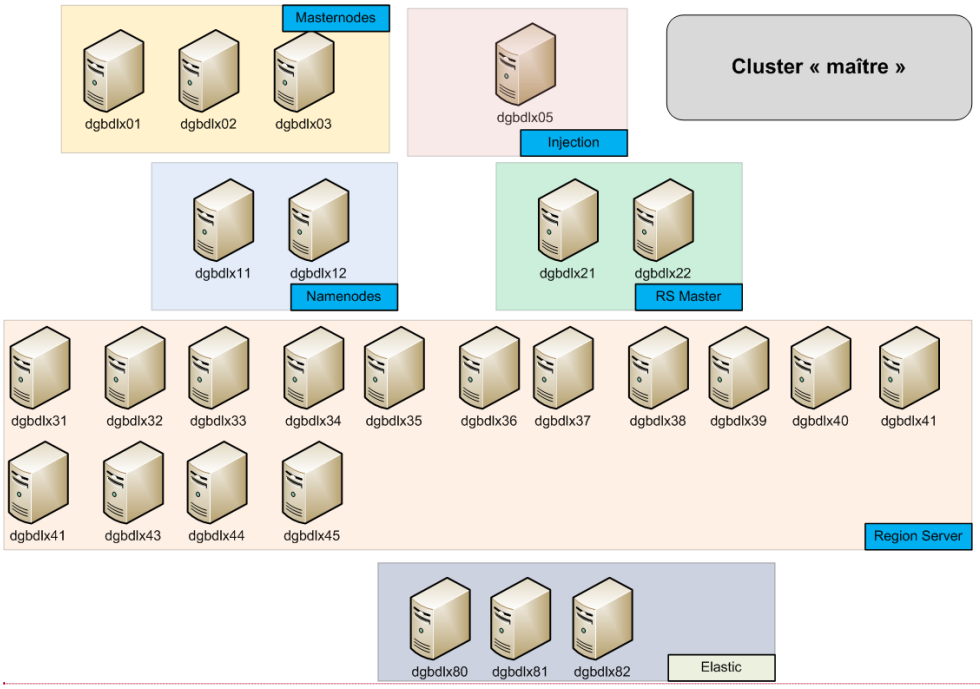
4.4 Stratégie de mise en œuvre des environnements

Nom de l'env	**DB**	**DA**	**DH**	**HOB**	**HOT**	**Prod**
Infrastructure	-	Cloud de Dev		-	-	-
Contributeurs	-	DEV	-	-	-	-

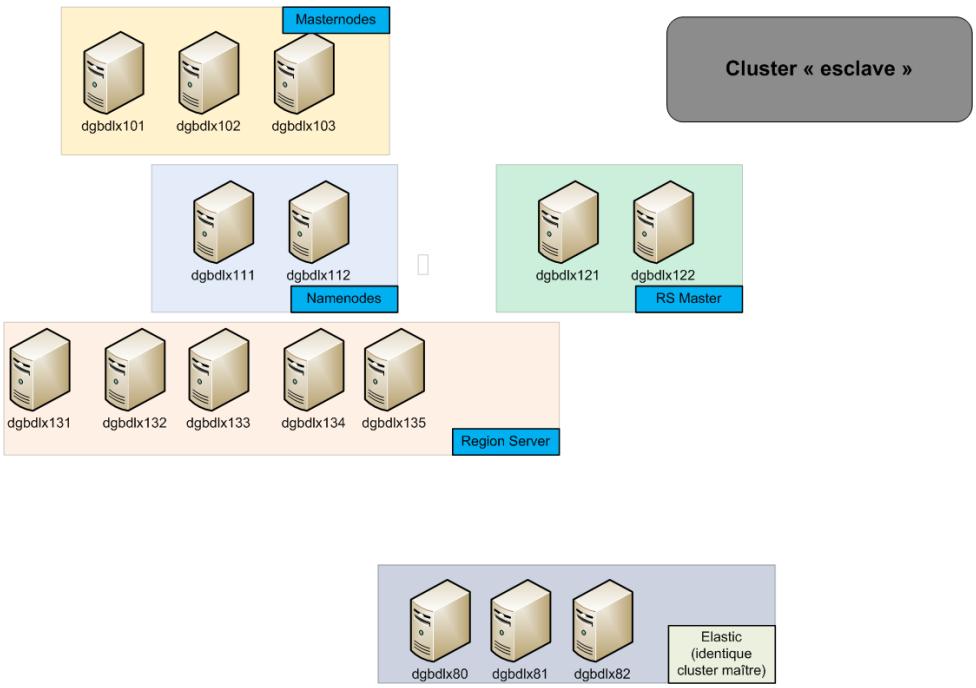
5 ARCHITECTURE D'HEBERGEMENT APPLICATIF

5.1 Description de la solution d'hébergement par environnement

5.1.1 Description détaillée de la production



Commenté [JMI2]: A revoir (pas de mongoDB dans la GED, seulement dans FGAD)



5.1.2 Plan de capacité et perspective d'évolution du besoin en ressources techniques

Environnement	Infrastructure			Composants
	Compute	Storage	RAM	
DA	304vCPU	47940Go	1952Go	1xHAProxy (mutualisé) 1xApache 1xTomcat (AWT) 1xHBASE/HIVE/ELK
DH				1xApache 1xTomcat (AWT) 1xHBASE/HIVE/ELK
HOB (*)		<A compléter>		
HOT (*)		<A compléter>		
Prod (*)		<A compléter>		

Cluster n°1 :

	Mastemodes			Injection	Namenodes		Region server master		Region server													Elastic search			Total
	dgbdlx01	dgbdlx02	dgbdlx03	dhadlx08	dgbdlx11	dgbdlx12	dgbdlx21	dgbdlx22	dgbdlx31	dgbdlx32	dgbdlx33	dgbdlx34	dgbdlx35	dgbdlx36	dgbdlx37	dgbdlx38	dgbdlx39	dgbdlx40	dgbdlx41	dgbdlx42	dgbdlx43	dgbdlx44	dgbdlx45	dgbdlx81	dgbdlx82	dgbdlx83	
Capacité technique																											
CPU (vcore) / thread	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	**208** cores
RAM en Go	32	32	32	32	32	32	32	32	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	**1408** Go
OS - Linux Redhat version	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	
Disques Données en Go	160	160	160	500	60	60	60	60	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000	**37220** Go
Hébergement	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	

Cluster n°2 :

	Master nodes			Namenodes		Region server master		Region server					Total
	dgbdlx101	dgbdlx102	dgbdlx103	dgbdlx111	dgbdlx112	dgbdlx121	dgbdlx122	dgbdlx131	dgbdlx132	dgbdlx133	dgbdlx134	dgbdlx135	
Capacité technique													
CPU (vcore) / thread	8	8	8	8	8	8	8	8	8	8	8	8	**96** cores
RAM en Go	32	32	32	32	32	32	32	64	64	64	64	64	**544** Go
OS - Linux Redhat version	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	CentOS 7.3	
Disques Données en Go	160	160	160	60	60	60	60	2000	2000	2000	2000	2000	**10720** Go
Hébergement	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	MAR	

(*) Attention : à ce stade, il s'agit d'une estimation au regard des informations disponibles :

- Le dimensionnement sera à confirmer en phase HOT
- Chaque demi-infra en production devra être capable d'absorber 100% de la charge
- Le projet prendra soin d'éteindre les VMs des environnements inutilisés pour ne payer que le stockage (e.g. HOB / HOT pendant les phases inter-projet)

Note : voire la section « 3.3.2 Volumétrie et durée de rétention » concernant la volumétrie pour dimensionner les filesystem.

5.1.3 Synthèse des ressources techniques

5.1.3.1 Production

5.1.3.2 Homologation bancaire

5.1.3.3 Homologation technique

5.1.3.4 Développement

Référence	DNS physiques	
	DNS applicatifs	
	Zone réseau	
Logiciels socle	OS	
	Robustesse locale	
	Surveillance	
	Sauvegardes	
	Scripts	
Autres	Technologies Java	
	Connecteurs	
	Framework	
	Certificat SSL	

5.2 Services d'infrastructure

5.3 Sécurité et couverture des Risques Opérationnels (dont DICP)

DICP : 3323

D/3 : site principal (Marcoussis/Tigery) + site de secours (Seclin)

I/3 : non traité dans le cadre du POC

C/2 : non traité dans le cadre du POC

P/3 : non traité dans le cadre du POC

5.4 Niveau de service atteint

*Le délai de rétablissement **technique** du service (OLA) de la solution d'architecture de résilience est généralement la somme cumulée des délais suivants : détection, checkpoints de l'ingénieur système en astreinte et délais de redémarrage de chaque composant.*

Ex : suite à un crash serveur, la reprise le délai de remise en service technique est la somme des délais pour que le problème soit automatiquement détecté, que l'ingénieur système valide le problème et pour que le cluster démarre les N services sur le(s) serveur(s) secondaire(s). Cela n'inclut pas les délais pour que les DBA, admin appliquent leurs procédures de contrôles au niveau composant et des BT pour appliquer les procédures de reprise au niveau applicatif.

5.4.1 Par type de panne

Type de panne	Moyen de correction	Délai de remise en service technique (hors contrôle BT)
Panne globale du serveur	Ex : bascule cluster	
Panne de carte réseau publique	Ex : carte réseau redondante	
Panne de carte réseau sauvegarde (ou heartbeat…)		
Panne de carte HBA	Ex : double attachement SAN	Sans impact
Crash du composant logiciel xxxx	A détailler par composant	
Corruption du système	Restauration système / bascule cluster	Ex : En mode « best efforts »
Corruption des données applicatives	Restauration données applicatives	Ex : En mode « best efforts »
Panne baie de disques SAN		

5.4.2 Solution globale

5.5 Architecture réseau

5.5.1 Schéma du réseau

5.5.2 Topologie, flux, protocole, port, matrice des flux

5.6 Identification des SPOFs applicatifs ou physiques

N/A

6 CONFORMITE

Présenter *tous les points de de non-conformité vis-à-vis du cadre de référence Socle Digital Agence*

7 Exercices (preuve) / Ecosystèmes d'hébergement

La démarche pour prouver que l'activité bancaire peut se dérouler sur un site distant est progressive.

Ecosystème d'hébergement = écosystème de données + écosystèmes de flux
- Cf. glossaire et cadrage normatif Résilience (livret Résilience V4)

7.1 Analyse de l'écosystème de flux (premier niveau)

7.2 Analyse de l'écosystème de données (premier niveau)

Sur le périmètre de GTS, la cohérence des données est assurée au niveau le l'écosystème de données.

7.3 Ecosystème d'hébergement [[Catégorie]]

7.4 Définition

7.5 Eléments à prendre en compte pour la procédure de démarrage

7.6 Définition de l'écolience

7.7 Niveau de Preuve atteint

Voir annexe 7.5 et 7.6

Ces exercices correspondent généralement à un modèle d'architecture de résilience reposant sur un dispositif de robustesse, décrit dans le présent DAH.

Preuve exercice **distant**	Granularité	Conditions requises	Impacts utilisateurs
Validation technique	Application		
Exercice faible charge	Ecosystème de données		
Exercice GTS (conditions réelles)	Ecosystème d'hébergement (flux + données)		
Exercice métier (conditions réelles)	Ecolience		
Panne	Au cas par cas		
Test en bulle	Au cas par cas		

Preuve exercice **local**	Granularité	Conditions requises	Impacts utilisateurs
Validation technique	Application		
Exercice GTS (conditions réelles)	Application ou groupe d'applications		
Exercice (conditions réelles)	Ecolience		

8 Exploitation

8.1 Plan de migration

N/A

8.2 Monitoring / Alerting

8.2.1 Monitoring OS & Infrastructure

Offre standard GTS (Nagios ou Patrol selon solution disponible)

Les FS applicatifs ne doivent pas être remplis au delà de 75%, il faut donc :

- Prévoir un seuil « Patrol » pour remonter des alertes liées au remplissage des FS

Le monitoring à implémenter concerne les ressources suivantes :

- Supervision Linux standard : CPU, mémoire, File system, Swap

8.2.2 Monitoring Middleware

Middleware	Elément à superviser	Alerte
HAProxy	Pas de surveillance, mode POC en DEV	
Apache	Pas de surveillance, mode POC en DEV	
Tomcat	Pas de surveillance, mode POC en DEV	
PHP/LAMP	Pas de surveillance, mode POC en DEV	
HDP	Pas de surveillance, mode POC en DEV	
HBASE	Pas de surveillance, mode POC en DEV	
HIVE	Pas de surveillance, mode POC en DEV	
ELK	Pas de surveillance, mode POC en DEV	

8.2.3 Monitoring applicatif

<Utilisation d'un APM à instruire>

8.2.4 Logs applicatif

8.2.4.1 Production et consommation

Voir section 3.3.2 Volumétrie et durée de rétention concernant les volumes attendus et durée de rétention

8.2.4.2 Purge

Voir section 3.3.2 Volumétrie et durée de rétention concernant les volumes attendus et durée de rétention

8.3 Maintenance

8.4 Liste des droits et privilèges système demandés pour l'installation et le fonctionnement de l'application

8.5 Administration

8.5.1 Administration des composants de sécurité

Décrire l'architecture d'administration de sécurité (type d'outils utilisés, protocoles, procédures de supervision…).
Insérer un schéma décrivant cette architecture.

8.5.2 Principes de gestion des habilitations

A compléter à partir de https://sbc.safe.socgen/thread/28165

8.5.3 Principes de gestion des purges de données

N/A

8.6 Plan de secours

N/A

8.7 Résilience locale : conditions de bascule

<à détailler>

8.8 Résilience distante : conditions de bascule

<à détailler>

Rappel : on aura une résilience distante avec un cluster HDP + ELK sur SECLIN

9 ANNEXE

9.1 Documents de références

Titre	Référence	Localisation
Cadre de référence Digital Agence	Version Jive 69	https://sbc.safe.socgen/docs/DOC-10266
Cadre de référence BIG DATA	<à renseigner>	<à renseigner>

9.2 Conclusion du benchmark (si ceux-ci sont réalisés)

Indiquer les messages principaux et indiquer les modifications au DAH qui ont été induites par les résultats du benchmark.

Faire référence au répertoire de stockage et lister les références (nom, version).

9.3 Glossaire

Terme	Définition
CVT	Comité de Validation Technique (Initialisation / Qualification / eXploitabilité). Plus d'info sur ce site
DAU	Dossier d'Architecture Unique
Preuve	Un test ou un exercice est une action qui consiste en fonction d'un scénario, d'objectifs et de critère préétablis, à évaluer l'efficacité de tout ou partie d'une solution de CA (continuité d'activité), des procédures et plans constitutifs d'un PCA (plan de continuité d'activité). La preuve vue du métier est l'exercice en conditions réelles.
Test (ou dit aussi test en bulle)	Il est réalisé dans un environnement dédié au test avec des données détruites en fin de test. Les intervenants métiers simulent l'exécution de leur activité. Il ne doit pas y avoir d'impact sur la production.
Exercices	Contrairement à un test, un exercice est réalisé, au moins partiellement, en production, sur des données réelles et avec un retour à la situation nominale. Lors d'un exercice, les intervenants métiers exécutent réellement tout ou partie de leur activité. Un exercice hors charge a pour finalité de valider le bon fonctionnement des procédures et de la solution : pas d'utilisateurs métiers, ni échanges de flux Un exercice faible charge (resp. pleine) est réalisé en conditions réelles avec des utilisateurs métiers et des échanges de flux. La seule différence est le volume traité et la période. Généralement, un exercice faible charge est réalisé le week-end (samedi soir, voire dimanche), le pleine charge est réalisé en semaine (cf. méthodologie exercice, les points à analyser sont les conditions de bascule (arrêt de service) et l'impact sur les partenaires : mode dégradé et pic d'activité à la réouverture du service. C'est pourquoi le début et la fin d'un exercice pleine charge sont parfois planifiés en week-end pour limiter l'impact des 2 arrêts de service.
Robustesse	les dispositifs de robustesse permettent de faire face à un incident localisé et ne nécessitent pas d'actions pour jouer leur rôle. La robustesse ne nécessite pas de prise de décision. Le dispositif de robustesse se décline sur les axes organisationnels, moyens, et humains.

	Sur la dimension infrastructure, les solutions se déclinent en modèle de résilience dit de haute disponibilité soit locale soit entre deux sites distants. Par extension, si la haute disponibilité est implémentée sur deux sites distants interégionaux, le dispositif de robustesse est dit nativement résilient car il couvre les 4 risques : composants, perte de salle, perte de site et choc régional.
Résilience	Robustesse + Secours + Preuve
Secours	Les dispositifs de secours nécessitent une prise de décision et une activation. Ils permettent aussi de faire face à un incident de grande ampleur. De même que pour la robustesse, ce dispositif se décline sur les axes organisationnels, moyens, et humains. Sur la dimension infrastructure, les solutions se déclinent en modèles de résilience reposant sur un site de repli distant à froid dont le plan de démarrage est global.

< Fin du document >