	Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 1/19

Merci de nous retourner un exemplaire signé de la 1^{ère} page



DOSSIER D'ARCHITECTURE TECHNIQUE (DAT)

Diffusion interne		Diffusion externe
AUSY : Thierry GENELETTI Marine BARON Luis SEVERINO Nicolas WEBER		DGA : Thierry GOLDER (DGA/SMQ/SDSI) Thierry DEVULDER (DGA/com) Frédéric NGO (DGA/mission Achat)
Rédigé par	Vérifié par	Approuvé par
NOM : Landry RAZAFIMAHAFALY Majid LAHMIDI Pascal MORLAAS-COURTIES	NOM : Thierry GENELETTI	NOM :
DATE : VISA :	DATE : VISA :	DATE : VISA :

Localisation Fichier : \\Neptune\partages\Eboue-TECHNIQUE\VER\MINDEF\141299-DGA-IX_DRUPAL\DOS_TECH\4.Doc-Tech_Internes\4.3.Conception\20160906-NP-AUSY-portails-141299-DGA-lxarm-DAT V4.0.docx



HISTORIQUE		
Date	Version	Motifs
22/04/16	0.9	Rédaction
23/05/16	1.0	Relecture
22/07/16	2.0	Format + Livraison
06/09/16	2.1	Mise à jour Infrastructure BDD et LDAP
22/09/16	3.0	Relecture et montée de version pour livraison
02/12/16 27/01/16	4.0	Chapitre SOLR Prise en compte des remarques/recommandations Connectis issues des réunions suite à l'hébergement des serveurs virtuels.

Version du modèle : 1.0

		Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 2/19

SOMMAIRE

1. OBJET.....	3
2. DOCUMENTS DE REFERENCE.....	3
3. TERMINOLOGIE ET ACRONYMES.....	3
3.1. TERMINOLOGIE.....	3
3.2. ACRONYMES	4
4. ARCHITECTURE TECHNIQUE.....	5
4.1. ARCHITECTURE LOGIQUE ET PHYSIQUE D'UN ECOSYSTEME DRUPAL	5
4.1.1. <i>Architecture logique de l'écosystème DRUPAL</i>	5
4.1.2. <i>Architecture Ecosystème DRUPAL</i>	7
4.1.3. <i>Niveau Physique</i>	8
4.1.4. <i>Niveau Composant Logiciel</i>	9
5. FLUX	12
5.1. SCHEMA SYNOPTIQUE	12
6. BATCH	13
7. PRESENTATION COMPOSANTS TECHNIQUES.....	14
7.1. APACHE SOLR (LUCENE)	14
7.1.1. <i>Présentation</i>	14
7.1.2. <i>Mise en œuvre</i>	14
7.2. POSITIONNEMENT DE DOCUMENTS SUR DIODE	15
8. SUPERVISION.....	15
9. SAUVEGARDES.....	15
10. PRA/PCA.....	15
11. SECURITE.....	15
11.1. SECURITE DE DRUPAL	16
11.1.1. <i>Injection</i>	16
11.1.2. <i>Violation de Gestion d'Authentification et de Session</i>	16
11.1.3. <i>Cross-Site Scripting (XSS)</i>	16
11.1.4. <i>Références directes non sécurisées à un objet</i>	17
11.1.5. <i>Mauvaise configuration et Sécurité</i>	17
11.1.6. <i>Exposition de données sensibles</i>	17
11.1.7. <i>Manque de contrôle d'accès au niveau fonctionnel</i>	17
11.1.8. <i>Falsification de requête intersite (CSRF)</i>	18
11.1.9. <i>Utilisation de composants avec des vulnérabilités connues</i>	18
11.1.10. <i>Redirections et renvois non validés</i>	18
11.1.11. <i>Filtrage d'IP</i>	18
11.2. ACCES DISTANTS	18
11.3. GESTION DES BOITES AUX LETTRES FONCTIONNELLES	19

		Portails Ixarm.com & achats.defense.gouv.fr	Référence 141299-DGA-Ixarm-DAT	Date 27/01/17
			Version : 4.0	Page 3/19

1. OBJET

Ce document est destiné à décrire l'architecture mise en place pour les sites ixarm.com et achats.defense.gouv.fr.

Les sites ixarm.com et achats.defense.gouv.fr s'appuient sur le framework Drupal et l'architecture LAMP associée fournie par l'hébergeur (non défini à ce jour).

Les sites ixarm.com et achats.defense.gouv.fr sont conçus pour :

- Les industriels en relations avec le Ministère de la Défense,
- Les personnels de la recherche travaillant ou souhaitant travailler avec le Ministère de la Défense,
- Le personnel de la DGA.

Il a pour objectif de proposer à ses prospects et clients une expérience cross canal complète et optimale. Le site répond aux exigences suivantes :

- Accessibilité et optimisation des parcours utilisateur adaptés pour chacun des 3 grands terminaux, desktop, tablette et mobile par une conception et intégration en Responsive Web Design ;
- Simplicité d'utilisation et automatisation pour les nombreuses interactions entre les externes et le personnel du Ministère de la Défense.

Ce document décrit l'architecture applicative, logique et physique et les interfaces existantes avec les autres systèmes.



2. DOCUMENTS DE REFERENCE

	Type	Référence	Version	Date
DR1	CCTP	20151117_NP_SMQ_SDSI_CCTP Marché complémentaire IXARM	1.3	17/11/2015
DR2	Liste de modules	20160629-NP-AUSY-portails-141299-Ixarm-liste_modules	2.1	05/09/2016
DR3	Descriptif d'interface Place et AFP	20151208_NP_DGA_Modèle-S-INF_421-Ed2-Descriptif-interface	1.0	23/05/2016
DR4	Stratégie de tests	20160112_NP_AUSY_Portails-141299-DGA-IXARM-STL	2.0	17/10/2016
DR5	Descriptif d'interface SOLR	20151208_NP_DGA_Modèle-S-INF_421-Ed2-Descriptif-interface SOLR	1.0	27/01/2017
DR6	Descriptif d'interface vers GRID	20151208_NP_DGA_Modèle-S-INF_421-Ed2-Descriptif-interface GRID	1.0	27/01/2017

3. TERMINOLOGIE ET ACRONYMES



3.1. Terminologie

Terme	Description
DRUPAL	CMS (système de gestion de contenu)
MySQL	Système de gestion de base de données relationnel
PHP	Langage de programmation
VMware Vsphere	Système de virtualisation de plate-forme

		Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 4/19

3.2. *Acronymes*

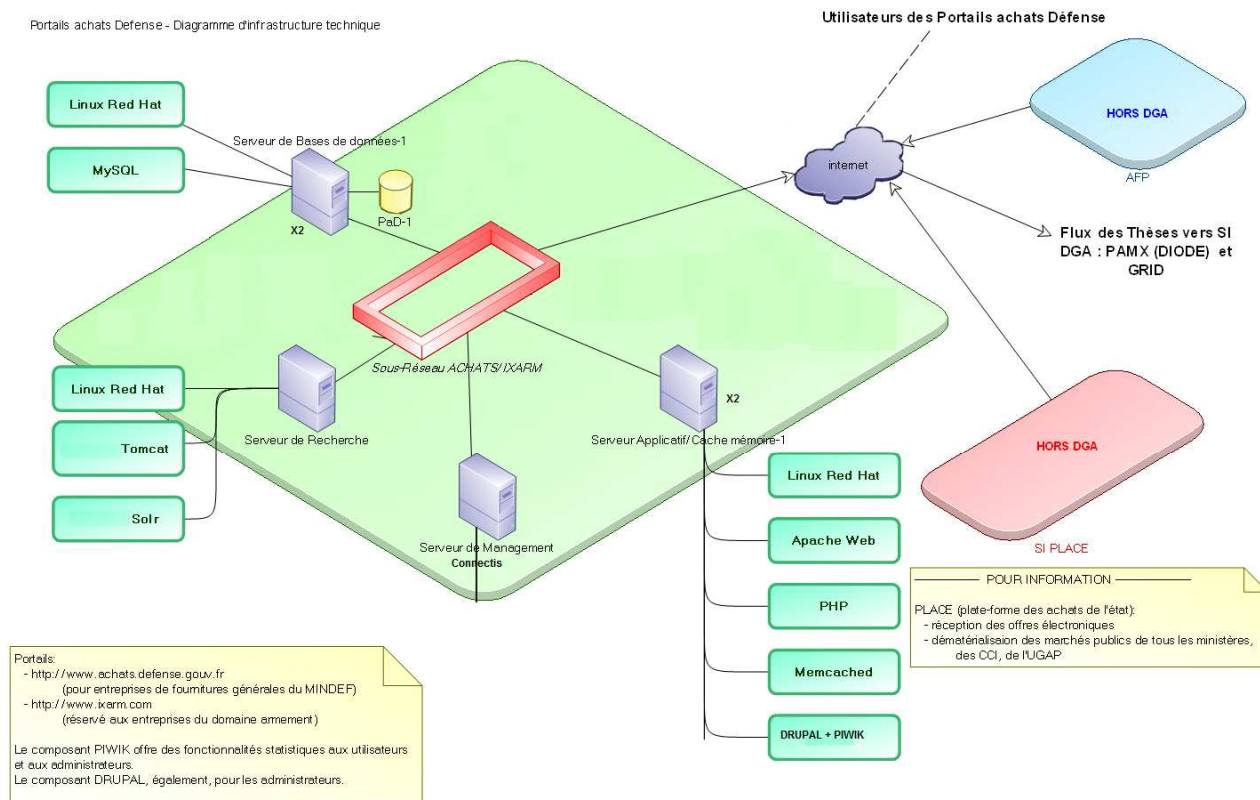
Acronyme	Description
BDD	Base De Données
DRS	Distributed Resource Scheduler
FQDN	Fully Qualified Domain Name
HA	High Availability
PCA	Plan de Continuité d'Activité
PRA	Plan de Reprise d'Activité
SLA	Service-Level Agreement
VIP	Virtual IP adresse
VM	Machine Virtuelle

		Portails Ixarm.com & achats.defense.gouv.fr	Référence 141299-DGA-Ixarm-DAT	Date 27/01/17
			Version : 4.0	Page 5/19

4. ARCHITECTURE TECHNIQUE

4.1. Architecture Logique et Physique d'un Ecosystème DRUPAL

Portails achats Defense - Diagramme d'infrastructure technique

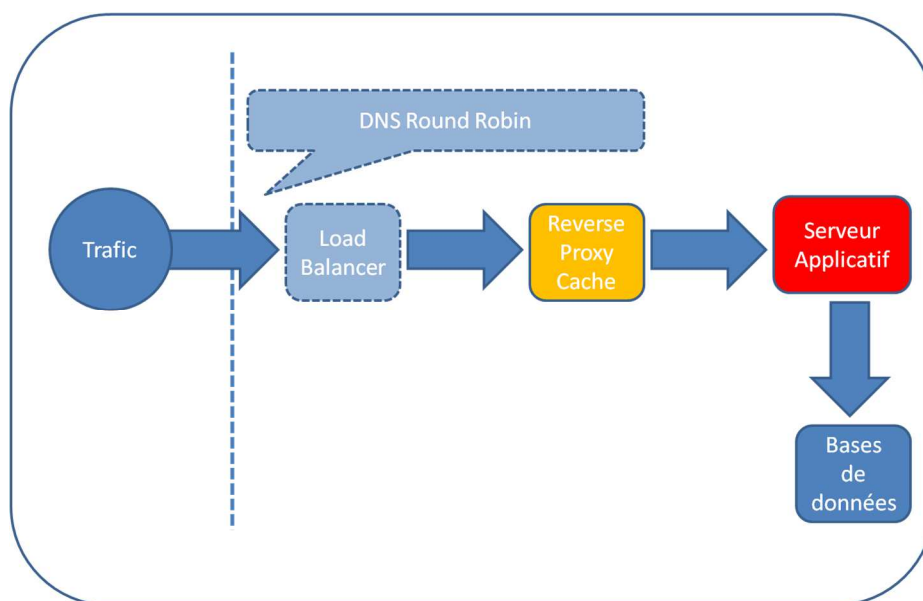


Ce diagramme décrit l'infrastructure technique en termes de réseaux de communication et de ressources matérielles et logicielles

L'utilisation du logiciel « Varnish » (serveur de cache http), dépend du nombre de connexion sur le site. Il sera utilisé si les tests de montée en charge démontrent sa nécessité.

4.1.1. Architecture logique de l'écosystème DRUPAL

La composition de l'écosystème technico-fonctionnelle pour Drupal est composée de la manière suivante :



Load Balancer: Système de répartition de charge afin de répartir les réponses à un service sur plusieurs serveurs.

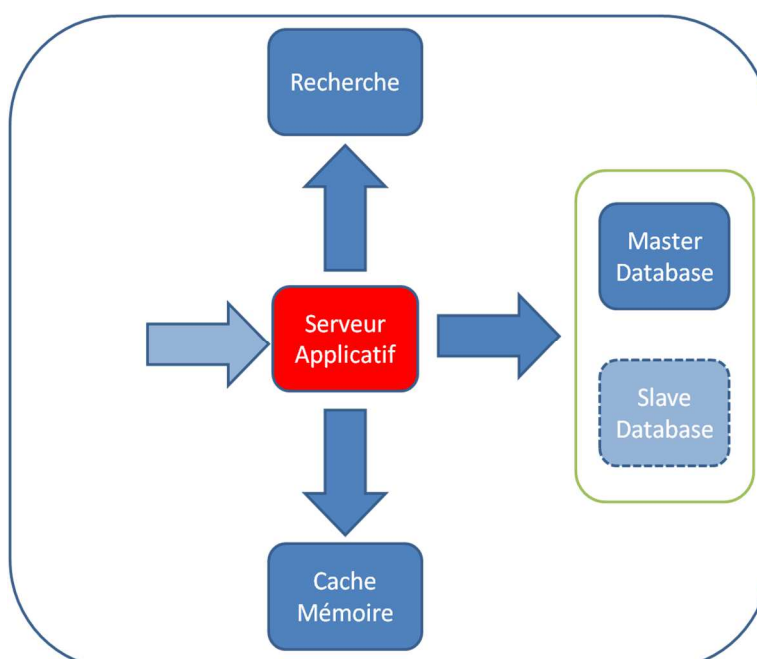
DNS Round Robin: Système de répartition de charge consistant à associer plusieurs adresses IP à un FQDN afin de répartir les réponses à un service sur plusieurs serveurs, suivant un algorithme ordonnancement de type round-robin.

Reverse Proxy Cache : Système de mise en cache de page statique, afin d'augmenter les performances de l'écosystème DRUPAL.

Serveur Applicatif : Cœur de l'écosystème DRUPAL.

Bases de données : Système de base de données de l'écosystème DRUPAL.

Détail autour du serveur Applicatif :



AUSY	DGA	Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 7/19

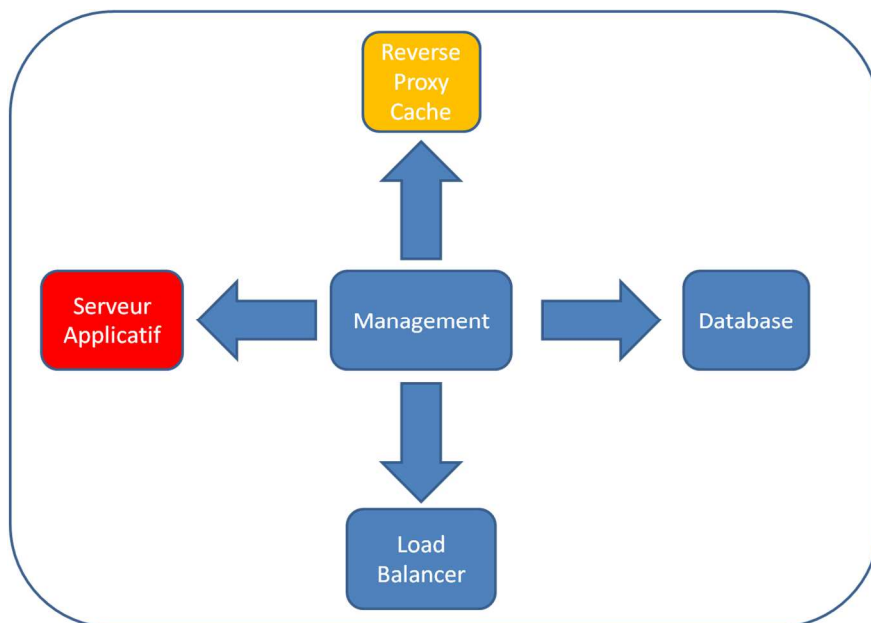
Recherche : Système de Recherche d'élément dans l'écosystème DRUPAL.

Cache Mémoire : Système de mise en cache d'éléments de l'écosystème DRUPAL.

Master Database : Base de données Maître dans un système de base de données en mode réplication.

Slave Database : Base de données Esclave dans un système de base de données en réplication.

En outre, il faut avoir une partie management de l'écosystème DRUPAL :



Management : Système de supervision des éléments constituant un système d'information.

4.1.2. Architecture Ecosystème DRUPAL

	Processeur/Cores	Mémoires	Vitesse de Disque
Serveur Web	● ● ● ●	● ●	●
Serveur de Recherche	● ●	● ● ●	● ● ●
Serveur Base de données	● ●	● ● ● ●	● ● ● ●
Supervision	●	●	●

Configuration Matérielle minimale :

Architecture des VM de production

2 Serveurs de base de données



CPU : 4VCPU
Mémoire: 8Go
Espace de stockage : 100Go

2 Serveurs Applicatif



CPU : 6VCPU
Mémoire: 4Go
Espace de stockage: 100Go

1 Serveur de Recherche :



CPU : 4VCPU
Mémoire: 6Go
Espace de stockage : 100Go

Architecture des VM de pré-production

Serveur de base de données



CPU : 4VCPU
Mémoire: 4Go
Espace de stockage : 100Go



Serveur Applicatif



CPU : 4VCPU
Mémoire: 6Go
Espace de stockage: 200Go

4.1.4. Niveau Composant Logiciel

Type	OS/Plateforme	Logiciel	Version
Serveur Web Système de gestion de contenu (CMS) Langage Composant Logiciel	Linux Red Hat 7	Apache	Apache 2.4
		DRUPAL	8.1.7
		PHP	7.0.9
		Memcached	1.4.25

		Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 10/19

		PIWIK	2.16.1
Serveur de base de données	Linux Red Hat 7	MySQL	MySQL 5.6
Serveur Recherche	Linux Red Hat 7	Tomcat	7
		JDK	1.7
		Apache SOLR	5.5.1

Composants Système :



Type	Version
OpenSSH	7.2p2
OpenSSL	1.0.2

Composants Drupal :

Type	Version
php-common	7.0.9
php-opcache	7.0.9
php-xml	7.0.9
php-cli	7.0.9
php-pdo	7.0.9
php-gd	7.0.9
php-mbstring	7.0.9
php-mysql	7.0.4
php-imap	7.0.9
php-ldap	7.0.9
php-soap	7.0.9
php-tcpdf	6.2.11
php-pear	1.10.1
php-phpoffice-phpexcel	1.8.1
Curl	7.29.0

Composants Java pour Tomcat :

Type	Version
annotations-api.jar	3.0.FR
catalina.jar	7.0.55
catalina-ant.jar	7.0.55
catalina-ha.jar	7.0.55
catalina-tribes.jar	7.0.55
ecj-4.4.jar	3.10.0.v20140604-1726
el-api.jar	2.2.FR
jasper.jar	7.0.55
jasper-el.jar	7.0.55
jsp-api.jar	2.2.FR
servlet-api.jar	3.0.FR
tomcat7-websocket.jar	7.0.55
tomcat-api.jar	7.0.55
tomcat-coyote.jar	7.0.55

		Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 11/19

tomcat-dbcj.jar	7.0.55
tomcat-i18n-fr.jar	7.0.55
tomcat-jdbc.jar	1.1.0.1
tomcat-util.jar	7.0.55
websocket-api.jar	1.0.FR

Modules DRUPAL : Ils sont décrits dans la liste des modules (cf. [DR2]).

AUSY	DGA	Portails Ixarm.com & achats.defense.gouv.fr	Référence 141299-DGA-Ixarm-DAT	Date 27/01/17
			Version : 4.0	Page 12/19

5. FLUX

5.1. Schéma Synoptique

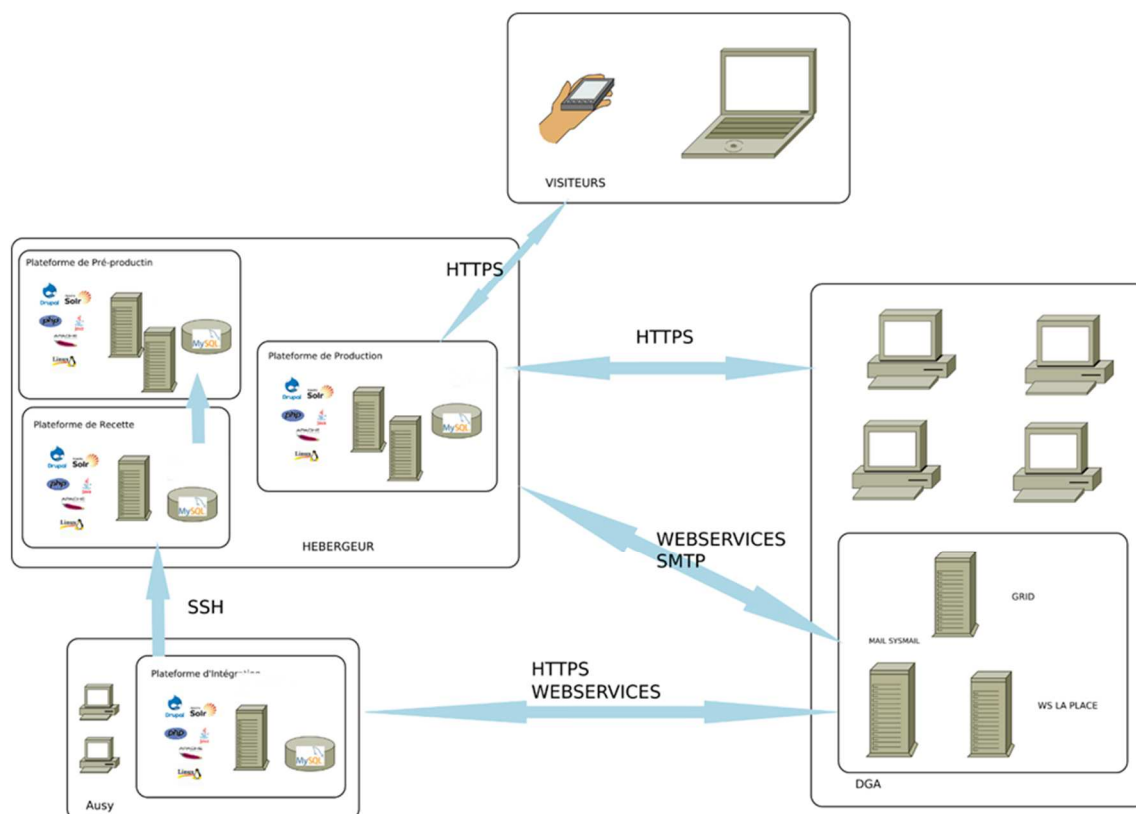
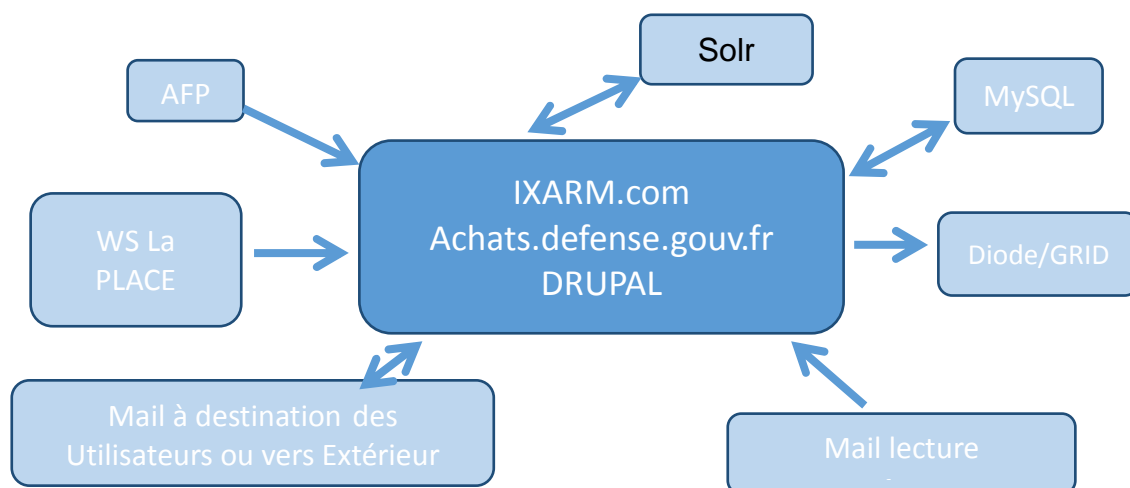


Schéma des flux applicatifs :



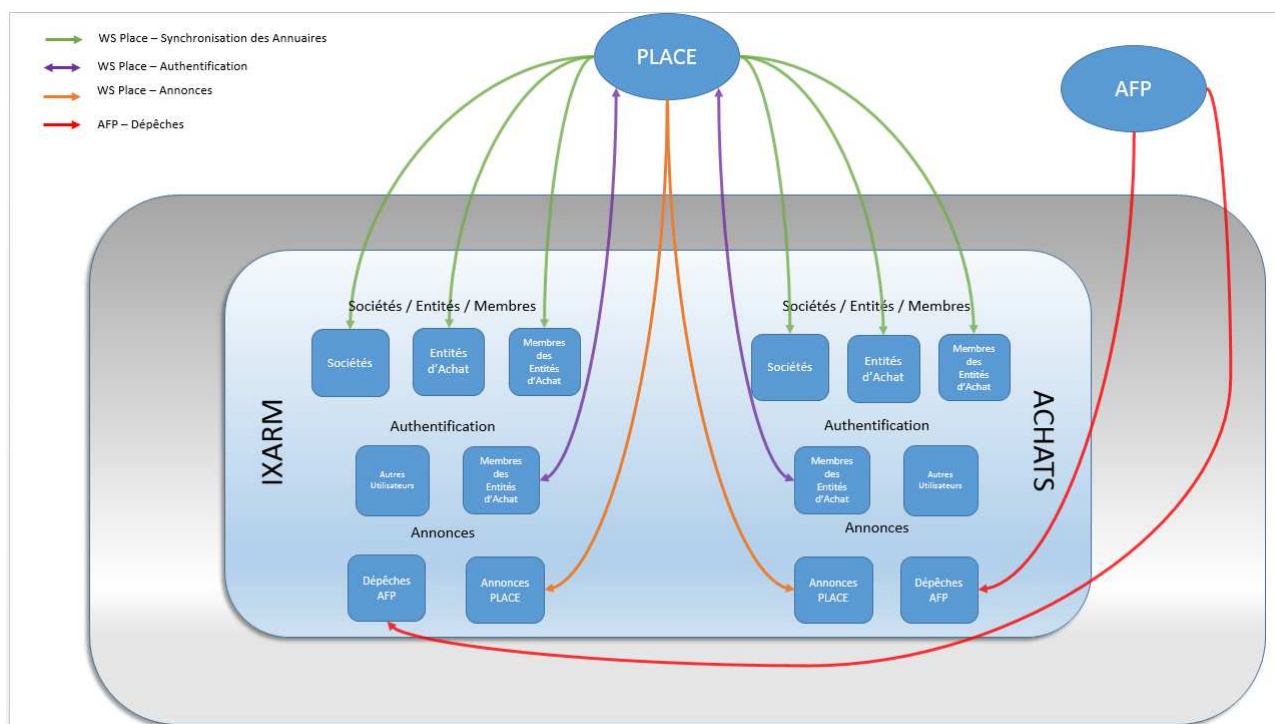


Tableau récapitulatif des flux pour le site :

De	Vers	Visibilité/Protocole	Port
Client	Apache	Internet/Https	443
Drupal	Carte entité	Internet/https et Web Service	80 /443
Drupal	Flux RSS	Internet / HTTPS	443
Drupal	Mail pour les utilisateurs	Internet / SMTP	25
Drupal	WS LA PLACE	Internet/https	443
Drupal	Mail interne	Intranet / SMTP	25
Drupal	Diode / GRID	Intranet/https et webservices	443
Drupal	Piwik statistique	Internet/https	443
Drupal	MYSQL	Interne / TCP	3306

6. BATCH

Les batchs identifiés par le système sont les batchs :



- de récupération des informations de la PLACE. Elles sont récupérées comme suit :

Les sociétés sont créées sur la PLACE, deux Cron Drupal partiel et intégral permettent de les importer vers les deux sites IXARM et ACHAT.

Les entités d'achats ainsi que les membres des entités d'achats sont importés depuis la PLACE via un Cron Drupal.

Les explications détaillées sont dans le document Descriptif d'interface (cf. [DR3]).

- D'interface avec le serveur d'indexation (fonction de recherche globale sur les deux portails).

		Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 14/19

Les explications détaillées sont dans le document Descriptif d'interface (cf. [DR5]).

- D'interface avec l'application GRID utilisée par la cellule MRIS (l'application GRID n'est pas dans le périmètre contractuel des portails).
Les explications détaillées sont dans le document Descriptif d'interface (cf. [DR6]).

7. PRESENTATION COMPOSANTS TECHNIQUES

7.1. Apache SOLR (Lucène)

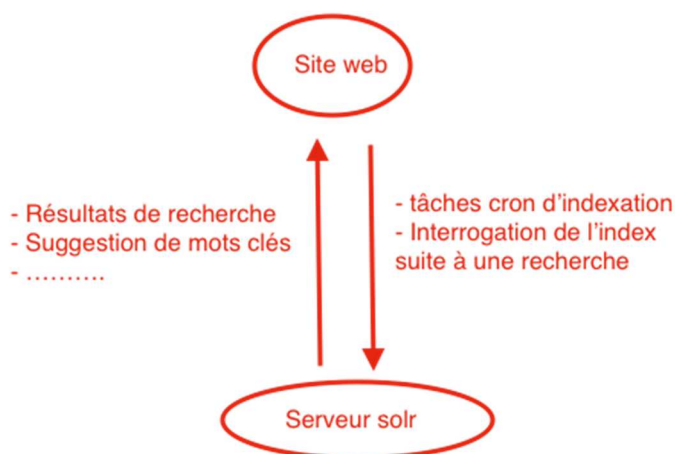
7.1.1. Présentation

Apache SOLR est une solution d'indexation et de recherche full-text. C'est un moteur de recherche open-source très performant permettant l'indexation des contenus textes. Sa puissance vient du fait que le contenu est indexé régulièrement via le planificateur de tâche, ce qui permet d'obtenir les résultats très rapidement lors d'une recherche.

Cette solution, recommandée pour les sites dont le volume de contenu est important, présente les fonctionnalités suivantes :

- Indexation et recherche en fonction de la langue.
- Recherche par mots clés, par phrase.
- Tri par différents critères comme la pertinence, date de modification ...
- Recherche par facettes.
- Mise en évidence des termes cherchés dans les résultats de recherche (highlighting).
- Indexation des contenus stockés dans la base de données.
- Indexation des documents pdf, doc ...
- Interface d'administration.



Le schéma suivant présente l'interconnexion entre le site web, le serveur de base de données ainsi que le serveur SOLR.



7.1.2. Mise en œuvre

La mise en place du moteur recherche SOLR nécessite l'installation des composants suivants :

- Installation du framework JDK de java.
- Installation du serveur de conteneur Tomcat.
- Installation de l'application SOLR.
- Installation des modules Drupal permettant la connexion de Drupal à SOLR.

		Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 15/19

- Configuration des modules Drupal avec les paramètres propres à l'instance SOLR fraîchement installée.

7.2. *Positionnement de documents sur Diode*

Le principe pour le portail est de déposer des documents dans des répertoires du serveur. Ces répertoires sont créés par l'applicatif en fonction des numéros de dossier MRIS.

La sécurisation et l'accès à ces répertoires est géré par l'équipe DIODE pilotée par le projet GRID.

8. SUPERVISION

La supervision est celle définie par l'hébergeur et la DGA.

9. SAUVEGARDES

Les sauvegardes, les purges et l'archivage font partie d'un processus propre à chaque client.

Cependant, une politique minimale est mise en place :

- Sauvegarde initiale de la plate-forme (base de données et site DRUPAL).
- Sauvegarde journalière incrémentale pour la base de données.
- Sauvegarde Hebdomadaire totale pour la base de données.
- Sauvegarde du site web et de la base de données avant chaque livraison.
- Sauvegarde du site web et de la base de données après validation de la livraison.

Une rétention de 7 jours glissants pour les sauvegardes incrémentales est un minimum.

Une rétention de 1 mois pour les sauvegardes totales est un minimum.

Pour les purges et l'archivage, pas de politique minimum, mais seule la capacité du stockage est prise en compte.

Pour une politique particulière de sauvegarde, elle sera définie entre l'hébergeur et la DGA.



10. PRA/PCA

Les Plans de Reprise et de Continuité d'Activité sont ceux définis par l'hébergeur et la DGA.

11. SECURITE

La sécurité repose sur les 3 aspects : intégrité, disponibilité, confidentialité :

- **intégrité** :
Notion d'authentification (Login + mot de passe) : pour le projet le login sera l'adresse email de l'utilisateur et le mot de passe est renforcé.
Cette règle est valide pour tous les utilisateurs du SI sauf ceux identifiés par LA PLACE qui s'occupe de la sécurité des utilisateurs entité d'achats. Pour ces users le mot de passe n'est pas stocké dans DRUPAL il est vérifié au moment de l'authentification via un Web Service en https (certificat à la charge de l'hébergeur) qui interroge LA PLACE.
Le mot de passe : il est paramétrable via l'administration DRUPAL. Les règles de construction (nombre de caractères, majuscules, minuscules, numérique, caractères spéciaux) sont définies par la DGA via le paramétrage.
- **disponibilité** :
Tous les sites de la DGA ont des obligations, ils doivent pouvoir se relancer rapidement.

		Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 16/19

- **confidentialité :**

Masquer les informations sur les briques techniques.

Vider les champs commentaires des sources.

Configurer le système pour enlever les commentaires sur l'OS et les commentaires sur les retours Base de Données.

Tous les flux http doit être proscrits. Seuls les flux HTTPS sont autorisés et les flux sécurisés.

11.1. Sécurité de DRUPAL

Dans le domaine de la sécurité, la réputation de Drupal n'est plus à faire. Interrogé sur les raisons de cette réputation, il est souvent indiqué que Drupal est sécurisé by design, c'est à dire depuis sa conception même. Autrement dit, dès le départ, Drupal a été conçu avec la notion toujours présente à l'esprit que le système doit être sûr et sécurisé. Les informations de sécurité du corps de DRUPAL sont gérées par une équipe dédiée à la sécurité pour DRUPAL (réf : <https://www.drupal.org/security-team>)

L'OWASP, organisation à but non lucratif dont l'objectif est d'améliorer la sécurité des logiciels, disposant d'une autorité reconnue mondialement en matière de sécurité sur Internet, publie chaque année un Top 10 des failles de sécurité des applications web les plus critiques. Ce Top 10 est largement accepté comme étant un référent sur l'état de l'art en matière de sécurité sur Internet.

Dries Buytaert, le fondateur de Drupal, affirme que Drupal de par sa conception est protégé contre ce Top 10 des failles de sécurité publié par l'OWASP. Regardons en détail comment Drupal, grâce à ses interfaces de programmation (API) si elles sont utilisées correctement, prend en compte chacune de ces plus importantes failles. Ces éléments de réponse proviennent du rapport publié régulièrement sur drupalsecurityreport.org.

Les tests via ZAPPROXY se font en intégration continue comme indiqué dans le document de stratégie de test (STL) au § 7.3.2.

11.1.1. Injection

Une faille d'injection, telle l'injection SQL, OS et LDAP, se produit quand une donnée non fiable est envoyée à un interpréteur en tant qu'élément d'une commande ou d'une requête. Les données hostiles de l'attaquant peuvent duper l'interpréteur afin de l'amener à exécuter des commandes fortuites ou accéder à des données non autorisées.

Drupal contient une API de base de données orientée objet robuste qui rend difficile pour les développeurs de créer sans le savoir des trous d'injection, par la désinfection automatique des paramètres de la requête.



11.1.2. Violation de Gestion d'Authentification et de Session

Les fonctions applicatives relatives à l'authentification et la gestion de session ne sont souvent pas mises en œuvre correctement, permettant aux attaquants de compromettre les mots de passe, clés, jetons de session, ou d'exploiter d'autres failles d'implémentation pour s'approprier les identités d'autres utilisateurs.

Les comptes d'utilisateurs et l'authentification sont gérés par le noyau Drupal. Les cookies d'authentification et le nom, l'ID et le mot de passe d'un utilisateur sont gérés sur le serveur pour empêcher un utilisateur d'escalader facilement une autorisation. Les mots de passe des utilisateurs sont hachés en utilisant un algorithme basé sur le Portable PHP Password Hashing Framework et les sessions existantes sont détruites lors de la connexion et déconnexion.

11.1.3. Cross-Site Scripting (XSS)

Les failles XSS se produisent chaque fois qu'une application accepte des données non fiables et les envoie à un navigateur web sans validation appropriée. XSS permet à des attaquants d'exécuter du script dans le navigateur de la victime afin de détourner des sessions utilisateur, défigurer des sites web, ou rediriger l'utilisateur vers des sites malveillants.

		Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 17/19

Drupal dispose d'un solide système de filtrage du contenu généré sur la page. Le contenu non fiable à destination des internautes est filtré pour éliminer les éléments dangereux par défaut. Pour les développeurs, Drupal dispose d'au moins huit fonctions de l'API pour filtrer le contenu généré et empêcher ainsi les attaques XSS.

11.1.4. Références directes non sécurisées à un objet

Une référence directe à un objet se produit quand un développeur expose une référence à un objet d'exécution interne, tel un fichier, un dossier, un enregistrement de base de données ou une clé de base de données. Sans un contrôle d'accès ou autre protection, les attaquants peuvent manipuler ces références pour accéder à des données non autorisées.

Le système de contrôle d'accès et le riche éco-système des autorisations de Drupal empêchent l'exécution des requêtes non autorisées. Les méthodes de contrôle d'accès sont disponibles via la configuration et le code contribué par la communauté. En outre, la protection contre les attaques sémantiques est mise en œuvre dans le noyau Drupal via l'API des formulaires.

11.1.5. Mauvaise configuration et Sécurité

Une bonne sécurité nécessite de disposer d'une configuration sécurisée définie et déployée pour l'application, contextes, serveur d'application, serveur web, serveur de base de données et la plate-forme. Tous ces paramètres doivent être définis, mis en œuvre et maintenus, car beaucoup ne sont pas livrés sécurisés par défaut. Cela implique de tenir tous les logiciels à jour.

Beaucoup de risques critiques, tels que l'accès au compte administrateur, aux formats de texte, et à des informations privées, sont limités à un seul compte admin par défaut. Les défauts d'ergonomie identifiés qui peuvent mener à une mauvaise configuration sont identifiés par des tests récurrents d'utilisabilité, et des correctifs sont inclus au cœur de Drupal. Une documentation sur les meilleures pratiques pour une configuration sécurisée et la conception d'un site Drupal est fournie et mise à jour gratuitement sur drupal.org. Plusieurs modules contribuent à permettre d'effectuer une revue générale automatisée de la sécurité d'un site, et d'autres proposent de mettre en œuvre des configurations mieux sécurisées.

11.1.6. Exposition de données sensibles


Beaucoup d'applications web ne protègent pas correctement les données sensibles telles que les cartes de crédit, identifiants d'impôt et informations d'authentification. Les pirates peuvent voler ou modifier ces données faiblement protégées pour effectuer un vol d'identité, de la fraude à la carte de crédit ou autres crimes. Les données sensibles méritent une protection supplémentaire tel un chiffrement statique ou en transit, ainsi que des précautions particulières lors de l'échange avec le navigateur.

Les mots de passe de compte sont hachés à plusieurs reprises sur la base du Portable PHP Password Hashing Framework. Plusieurs modules contribuent de Drupal proposent des solutions pour crypter les données sensibles qu'elles soient au repos ou en transit.

11.1.7. Manque de contrôle d'accès au niveau fonctionnel

Pratiquement toutes les applications web vérifient les droits d'accès au niveau fonctionnel avant de rendre cette fonctionnalité visible dans l'interface utilisateur. Cependant, les applications doivent effectuer les mêmes vérifications de contrôle d'accès sur le serveur lors de l'accès à chaque fonction. Si les demandes ne sont pas vérifiées, les attaquants seront en mesure de forger des demandes afin d'accéder à une fonctionnalité non autorisée.

Les accès fonctionnels dans Drupal sont protégés par un puissant système de permissions qui vérifie si les autorisations sont appropriées avant de déclencher une action. Pour les accès aux URL, la vérification d'accès est étroitement intégrée aussi bien dans le menu de rendu et que dans le système de routage système, ce qui signifie que la visibilité des liens de navigation et des pages est protégée par le même système de permissions qui gère les droits d'accès aux requêtes.

AUSY		Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 18/19

11.1.8. Falsification de requête intersite (CSRF)

Une attaque CSRF (Cross Site Request Forgery) force le navigateur d'une victime authentifiée à envoyer une requête HTTP forgée, comprenant le cookie de session de la victime ainsi que toute autre information automatiquement incluse, à une application web vulnérable. Ceci permet à l'attaquant de forcer le navigateur de la victime à générer des requêtes dont l'application vulnérable pense qu'elles émanent légitimement de la victime.

Drupal valide les intentions de l'utilisateur dans les actions effectuées en utilisant les techniques standard de l'industrie. Les actions typiques avec effets secondaires (telles que les actions qui suppriment des objets de base de données) sont généralement effectuées avec la méthode HTTP POST. L'API des formulaires de Drupal met en œuvre des jetons uniques de protection contre les CSRF dans les requêtes POST. Les actions moins importantes (dangereuses) peuvent tirer parti de la génération de jetons et de validation des fonctions fournies par l'API des formulaires tout en utilisant une requête HTTP GET.

11.1.9. Utilisation de composants avec des vulnérabilités connues

Les composants vulnérables, tels que bibliothèques, contextes et autres modules logiciels fonctionnent presque toujours avec des privilèges maximum. Ainsi, si exploités, ils peuvent causer des pertes de données sérieuses ou une prise de contrôle du serveur. Les applications utilisant ces composants vulnérables peuvent compromettre leurs défenses et permettre une série d'attaques et d'impacts potentiels.

Les bibliothèques et framework inclus dans le cœur de Drupal sont (au niveau du système) peu sophistiqués, et de faible risque pour une compromission du serveur ou de l'application.

11.1.10.Redirections et renvois non validés

Les applications web réorientent et redirigent fréquemment les utilisateurs vers d'autres pages et sites internet, et utilisent des données non fiables pour déterminer les pages de destination. Sans validation appropriée, les attaquants peuvent réorienter les victimes vers des sites de phishing ou de malware, ou utiliser les renvois pour accéder à des pages non autorisées.

Les redirections internes au site ne peuvent pas être utilisées pour contourner le système de contrôle de menu et de contrôle d'accès intégré de Drupal. Drupal est protégé également contre la redirection automatique vers des URL hors site qui pourraient être utilisées dans une attaque de phishing.

11.1.11.Filtrage d'IP

La configuration du fichier .htaccess (apache) permet de bloquer ou d'autoriser l'accès à certaines ressources. Pour les organisations ne pouvant modifier la configuration d'un tel fichier, une fonctionnalité (core) donne la possibilité d'interdire l'accès à certaines IP en back office.

L'ajout de modules complémentaires permet d'étendre le filtrage par white-list ou black-list d'IP en back-office.



Ce choix sera confirmé lors de la phase de conception.

Il n'existe pas de logiciel infaillible. La sécurité est moins un dogme qu'un processus continu de veille et d'amélioration. Un logiciel peut être sécurisé un jour pour devenir vulnérable le lendemain. La nombreuse communauté active de DRUPAL apporte dans ce domaine un précieux avantage en détectant rapidement les failles qui apparaissent et en les corrigeant très rapidement.

11.2. Accès distants

L'accès distant aux plates-formes de l'hébergeur, dans le but de livrer, se fera, pour une ou plusieurs personnes d'AUSY dédiées au delivery. Ces personnes accéderont au serveur de pré-production via un certificat x509v3 généré par une autorité de certification reconnue.

Nota : l'accès au serveur de pré-production de la DGA sera filtré sur l'adresse IP d'AUSY.

		Portails lxarm.com & achats.defense.gouv.fr	Référence 141299-DGA-lxarm-DAT	Date 27/01/17
			Version : 4.0	Page 19/19

11.3. Gestion des boîtes aux lettres fonctionnelles

Afin de pallier à l'impossibilité d'uploader des documents pour certains utilisateurs utilisant des postes DGA, il est prévu de permettre l'upload de fichiers suite à l'envoi d'un mail structuré sur une boîte aux lettres fonctionnelle.

Cette boîte aux lettres est administrée et sécurisée par l'Hébergeur.

A la création de son compte, un utilisateur est affecté en automatique du rôle « Utilisateur de la boîte aux lettres fonctionnelle » si le domaine de l'adresse mail fait partie de :

- intradef.gouv.fr
- defense.gouv.fr

L'utilisateur possédant ce rôle peut uploader des documents sur la boîte aux lettres fonctionnelle (le nom de cette boîte n'est pas défini à date).

Les fonctions de lecture et nettoyage de la boîte aux lettres sont décrites dans la SFD 012 – référentiel

- § 7.7.1. Lecture de la boîte aux lettres et stockage des PJ valides (extensions listées dans ce paragraphe) sous formes d'objets « contenus » Drupal.
La description des objets contenus est faite dans la SFD 002 – Contenus §5.1 et § 5.3
La suppression automatique des PJ non utilisées est décrite dans cette même SFD au § 5.5.5
- § 7.7.2. Nettoyage de la boîte aux lettres