Direction des systèmes d'information

MISE EN ŒUVRE ET MAINTENANCE DE SITES D'INTRANETS ET DE PORTAILS MÉTIER CNRS

Cahier des Clauses Techniques Particulières (CCTP)

Livret 1/2 du CCTP n°26463

Accord cadre n°26.14.027

ANNEXE FONCTIONNELLE

Objet : Ce document décrit la matrice RACI des responsabilités partagées entre le CNRS et le titulaire pour l'installation et l'exploitation des environnements d'intégration, de recette et production (plateforme CNRS).

1. SOMMAIRE

MISE EN ŒUVRE ET MAINTENANCE DE SITES D'INTRANETS ET DE PORTAILS MÉTIER CNRS 1

1. SOMMAIRE 2

2. RÉPARTITION DES TÂCHES D'INSTALLATION ET D'EXPLOITATION DE LA PLATEFORME CNRS, ENTRE TITULAIRE ET CNRS 3

2.1. Objectifs 3

2.1. RACI de la répartition des tâches de gestion de la plateforme CNRS 3

3. SPÉCIFICITÉS POUR LES ENVIRONNEMENTS D'INTÉGRATION 8

3.1. Objectifs 8

3.2. RACI pour les environnements d'intégration 8

3.2.1. Déploiement Environnement applicatif 9

3.2.2. Maintien en Condition Opérationnelle 9

3.2.3. Installation des applications 10

3.2.4. Cycle de vie des applications 10

2. RÉPARTITION DES TÂCHES D'INSTALLATION ET D'EXPLOITATION DE LA PLATEFORME CNRS, ENTRE TITULAIRE ET CNRS

2.1. OBJECTIFS

L'hébergement de la plateforme (environnements d'intégration, recette et production) est réalisé sur **un cloud privé** (IaaS) fourni par le CNRS.

Le titulaire définit et propose une solution respectant le cadre de cohérence technique (CCT) du CNRS et en définit l'architecture, conjointement avec le CNRS. Cette architecture est composée :

- du socle comprenant l'infrastructure (serveurs, stockage, réseau) et le socle logiciel : Redhat, Apache, PHP, PostgreSQL
- des composants applicatifs comprenant Symfony, DRUPAL, etc. et toutes les personnalisations.

Les installations du socle sont réalisées par le CNRS. Les déploiements applicatifs sont réalisés par le titulaire en environnement d'intégration. Cela permet de mettre au point la configuration et tester l'applicatif et enfin de rédiger les manuels d'installation, les scripts d'automatisation, etc… Le CNRS reproduit le déploiement en environnement de recette pour valider le processus de déploiement produit par le titulaire) puis, si toute la chaine est validée par le CNRS, effectue le déploiement en production.

DRUPAL Core est un composant du socle logiciel mais la DSI du CNRS n'a pas d'expertise de mise en œuvre de DRUPAL, d'où le présent marché de TMA. De plus, le CNRS ne gère pas de container dans sa chaine de CI/CD. Les installations DRUPAL CoRe sont :

- préparées par le titulaire
- automatisées au maximum (forge CNRS, Composer, Ansible, etc…)
- documentées au maximum (toute commande à réaliser doit être listée).
- réalisées par le CNRS avec assistance au besoin d'une équipe de support du titulaire.

Il en est de même pour tous les autres composants applicatifs.

Le titulaire propose et assiste le CNRS pour l'adaptation de ses moyens de **CI/CD** (Intégration Continue et Livraison ou Déploiement Continu) et de sa forge logicielle Koda pour prendre en compte la technologie DRUPAL (ainsi que les composants nécessaires comme Composer) lors des livraisons de code et de configurations, livraisons des tests unitaires, lors de l'exécution de ces tests dans la forge, lors du déploiement de la solution sur les environnements avec tous les composants nécessaires.

Cette chaîne est mise en place conjointement (titulaire et CNRS) en amont de la première livraison de la première version de la première application/portail à déployer, puis est utilisée par le titulaire pour les suivantes.

Nota : les **environnements d'intégration** étant mis à disposition du titulaire pour préparer les déploiements sur les autres environnements (recette et prod) auxquels il n'a pas accès, le titulaire a des activités et responsabilités élevées en environnements d'intégration. Elles sont décrites de manière plus détaillée dans le chapitre suivant.

2.1. RACI DE LA RÉPARTITION DES TÂCHES DE GESTION DE LA PLATEFORME CNRS

Le RACI ci-dessous recense l'ensemble des tâches qui l'installation et l'exploitation de la plateforme CNRS et spécifie pour chacune d'entre elles les responsables associés.

R : réalisateur de l'action, A : approbateur/valideur, C : consulté, I : informé

Tâches / Activités	CNRS	Titulaire	Remarques
Conception / Architecture			
Choix de l'architecture technique Drupal	C/A	R	Le titulaire propose une solution respectant le cadre de cohérence et les exigences du CNRS et que le CNRS valide
Définition de l'architecture infrastructure (serveurs, réseau, stockage)	R/A	C	L'infrastructure repose sur des VM (pas de conteneurs).
Sélection et configuration des ressources (CPU, RAM, disque, réseau)	R/A	C	Le titulaire propose des dimensionnements adaptés, qui sont discutés avec le CNRS.
Sélection et configuration des composants de performance (caches proxy et applicatifs).	C/A	R	Le titulaire propose une solution qu'il maîtrise et la configure (le CNRS n'a pas de compétence sur ces composants courants dans les solutions DRUPAL comme Varnish ou Redis). Les load balancer sont gérés par le CNRS.
Installation / Déploiement			
Installation OS et middleware (ex : RedHat, Apache, PHP, PostgreSQL)	R/A	C	Le titulaire est consulté et ensuite potentiellement adapte la configuration et la personnalisation applicative de façon à conserver la compatibilité.
Installation CMS Drupal Core (code source et configuration initiale)	R/A	R/C	Le titulaire propose les configurations, produit les MINST complets ainsi que pour le différentiel etc. et effectue un déploiement en environnement d'intégration. Le CNRS réalise le déploiement en environnement de recette et de production grâce aux composants livrés par le titulaire.
Installation des composants de performance (caches proxy et applicatifs).	R/A	R/C	Le titulaire fournit la configuration ainsi que le MINST. (le CNRS n'a pas de compétence sur ces composants courants dans les solutions DRUPAL comme Varnish ou Redis). Les load balancer sont gérés par le CNRS. Pour le cache applicatif, le titulaire effectue un déploiement en environnement d'intégration. Le CNRS le fait dans les autres environnements.
Déploiement applicatif personnalisé (modules	R/A	R/A	Le titulaire propose les configurations, produit les MINST

contribué, thèmes, intégrations, code applicatif et modules customs)			complets ainsi que pour le différentiel etc. et effectue un déploiement en environnement d'intégration. Le CNRS réalise le déploiement en environnement de recette et de production grâce aux composants livrés par le titulaire.
Déploiement automatisé (ne se substitue pas au déploiement manuel et à la production du MINST) : playbooks ANSIBLE	R/A	R/C	Le CNRS initialise les playbooks ANSIBLE sur la base de l'infrastructure et des MINST livrés par le titulaire. Le titulaire contribue à l'adaptation des playbooks sur les parties applicatives suite à ses évolutions.
Configuration sécurité infrastructure (pare-feu, sécurité réseau)	R/A	I	
Configuration sécurité applicative (Drupal, gestion accès, modules sécurité)	R/A	R/C	Selon les instructions transmises par le titulaire
Supervision / Monitoring			
Monitoring de l'infrastructure (serveurs, CPU, RAM, disques)	R/A	-	
Mise en place des logs applicatifs	R/A	R/C	Le titulaire définit et met en place les logs applicatifs
Monitoring applicatif (Drupal, disponibilité site, logs applicatifs)	R/A	-	
Alertes incidents infrastructure (niveau physique : hosts / réseau / baies de stockage…)	R/A	I	
Alertes incidents infrastructure (niveau virtualisation : VM / réseau virtuel / FW logiciels…)	R/A	I	
Alertes incidents applicatifs Drupal	I	R/C	Si un incident survient, le titulaire le reproduit en environnement d'intégration pour investiguer et le corriger.
Surveillance des publications de CVSS.	R/A	R/C	Le titulaire signale au CNRS et corrige les CVSS de niveau 9 ou plus dans les 24H. Si un correctif rapide n'est pas possible, le CNRS coupera l'application. Pour les CVSS de niveau 7 à 8 : dans les 7 jours et les autres dans les 30 jours. Les maintenances

			sont planifiées conjointement en comité hebdomadaire.
Maintenance / Exploitation			
Gestion des sauvegardes (snapshots VM, sauvegardes disques, BDD)	R/A	-	
Maintenance corrective/évolutive infrastructure (niveau physique : serveur, réseau, sécurité)	R/A	I	
Maintenance corrective/évolutive infrastructure (niveau virtualisation : serveur, réseau, sécurité)	R/A	I	
Maintenance corrective/évolutive applicative (Drupal, bugs modules)	R/A	R/C	Le titulaire produit les correctifs/évolutions, les configurations, les MINST complets ainsi que pour le différentiel etc. et effectue un déploiement en environnement d'intégration. Le CNRS réalise le déploiement en environnement de recette et de production grâce aux composants livrés par le titulaire.
Mises à jour OS, middleware (RedHat, PHP, PostgreSQL, Apache)	R/A	R/C	Le titulaire adapte les composants de l'applicatif pour conserver la compatibilité avec les composants du socle.
Mises à jour Drupal (core, modules, sécurité Drupal)	R/A	R/C	Selon les instructions transmises par le titulaire
Déploiement automatisé (ne se substitue pas au déploiement manuel et à la production du MINST) : playbooks ANSIBLE	R/A	R/C	Le titulaire contribue à l'adaptation des playbooks sur les parties applicatives suite à ses évolutions.
Gestion des incidents et support			
Prise en charge incidents infrastructure (niveau physique)	R/A	I	
Prise en charge incidents infrastructure (niveau virtualisation)	R/A	I	
Prise en charge incidents applicatifs Drupal	R/A	R/C	Si un incident survient, le titulaire le reproduit en environnement d'intégration pour investiguer et le corriger.

Communication incidents vers utilisateur final	R/A	I	
Performance & Optimisation			
Optimisation performance infrastructure (serveurs, stockage, réseau)	R/A	R/C	Le titulaire porte notamment la solution de cache proxy (le CNRS n'a pas de compétence sur ces composants courants dans les solutions DRUPAL comme Varnish).
Optimisation performance applicative (Drupal, cache, modules, base de données)	R/A	R/C	Le titulaire porte notamment la solution de cache applicatif (le CNRS n'a pas de compétence sur ces composants courants dans les solutions DRUPAL comme Redis).
Tests et validation performance globale solution	R/A	R/C	Le titulaire rédige et livre les tests. Il effectue des tests de bout en bout en environnement d'intégration. Le CNRS effectue les tests en environnement de recette et de production et valide le produit.

3. SPÉCIFICITÉS POUR LES ENVIRONNEMENTS D'INTÉGRATION

3.1. OBJECTIFS

L'objectif de ce chapitre est de définir le périmètre d'intervention sur les environnements d'intégration entre les équipes du titulaire et l'équipe d'exploitation de la DSI.

Le but des environnements d'intégration est de permettre au titulaire d'intégrer à l'écosystème de la DSI les applications qu'ils développent en dehors des infrastructures de la DSI.

Pour réaliser cette action le titulaire accède aux serveurs via un tunnel VPN IPSEC site à site ikev2 et est totalement autonome (profil root) pour installer, configurer et tester les applications qu'il a développées.

Le titulaire ne doit pas installer autre chose que ce qui est indiqué dans le CCT.

Les objets légitimes sont mis à disposition par le serveur Satellite RedHat de la DSI (packages d'installation).

Les environnements d'intégration permettent :

- D'accéder au service applicatif en mode "Client Web" via le VPN site à site uniquement
- D'accéder au serveur applicatif en mode "administrateur" via le VPN site à site et le bastion CNRS uniquement, en lecture/écriture
- D'accéder au serveur BDD :
    - En mode "Client d'administration SQL" via le VPN site à site uniquement
    - En mode "console d'administrateur" via le VPN site à site et le bastion CNRS uniquement, en lecture/écriture
- De livrer du code applicatif et de tester l'application via l'accès Web
- De tester l'intégration de l'application au SI
    - Connectivité et utilisation du Janus TEST
    - Connectivité et utilisation du WebService XXX
- D'accéder aux proxys mode "console d'administrateur" via le VPN site à site et le bastion CNRS uniquement, en lecture uniquement

Les environnements d'intégration ne permettent pas :

- D'accéder aux services transverses infrastructure en amont des machines de l'environnement
- De donner des accès à internet à un serveur, en dehors des besoins spécifiques et identifiés pour une application.
- Les accès justifiés sont filtrés via le SQUID.
- De connecter l'environnement à un autre Janus que le Janus-test
- De réaliser des tests de charge

3.2. RACI POUR LES ENVIRONNEMENTS D'INTÉGRATION

Le RACI ci-dessous recense l'ensemble des interactions dans les environnements d'intégration et spécifie pour chacune d'entre elles les responsables associés.

R : réalisateur de l'action, **A** : approbateur/valideur, **C** : consulté, **I** : informé

3.2.1. Déploiement Environnement applicatif

Tâches / Activités	CNRS MOE	CNRS Resp tech	CNRS Exploitation	Titulaire	Remarques
Demande d'environnement d'Intégration	A	R	I	C	
Déploiement serveurs virtuels	I	A/I	R	I	
Mise à jour automatique des OS	C/I	I	R	I	Les mises à jour automatiques des systèmes d'exploitation déployés dans le SI sont à la charge et de la responsabilité de la DSI. Ces mises à jour automatiques ne doivent pas être désactivées.
Ouverture flux réseau	A	I	R	I	
Gestion des flux entrant/sortant	A	I	R	C	
Vérifications du Service Public OK	I	I	R	I	
Vérifications enregistrement Satellite OK	I	I	R	I	Outils de mise à disposition des dépôts Linux validés par la DSI pour faire les installations.
Accès "administrateur" des utilisateurs (MOE, titulaire) aux serveurs applicatifs ou BDD via Arkea (CyberArk du CNRS)	I	I	R	I	
Vérifications sauvegarde OK	I	I	R	I	
Filtrage	A/C	I	R	I	Autorisation d'accès aux URL d'intégration

3.2.2. Maintien en Condition Opérationnelle

Tâches / Activités	CNRS MOE	CNRS resp Tech	CNRS Exploitation	Titulaire	Remarques
Supervision	C/I	I	A	A/C R	Le titulaire fournira une adresse mail de type liste de diffusion à laquelle seront envoyées automatiquement les alertes de la supervision CNRS.
Ajout ressources matérielles (cpu, mémoire, filesystem, ...)	A/C	C/I	R	A	Accès vSphère requis pour ajout espace disque supplémentaire

Gestion de l'espace disque (suppression de fichiers logs applicatifs)	A/C	C/I	A	A/C R	Alerte du titulaire directement via supervision CNRS
Redémarrage services applicatifs	A/C	C/I	I	A/C R	Alerte du titulaire directement via supervision CNRS
Incidents infrastructure informatique : pb réseau, serveur	A/C	I	R	I	Les MOE font remonter le problème à l'Exploitation pour traitement
Incidents application	A	I	I	A/C R	
Purge des logs				A/C R	Alerte du titulaire directement via supervision CNRS
Montée de version majeure de composants logiciel du socle (RedHat, Apache, PHP, PostgreSQL)	A/C	A/C	R	A/C	Une montée de version majeure demande une compatibilité de tous les composants et le respect du cadre de cohérence technique. Elle peut conduire à une installation applicative (DRUPAL, Symfony… et personnalisations).

3.2.3. Installation des applications

Tâches / Activités	CNRS MOE	CNRS CdPIS	CNRS Exploitation	Titulaire	Remarques
Installation Composants logiciels (Symfony, DRUPAL CoRe, ...)	A	I	I	R	
Installation application	A	I	I	R	Comprend toute personnalisation dans DRUPAL
Mise à jour application	A	I	I	R	
Configuration application (fichiers de conf, ...)	A	I	I	R	

3.2.4. Cycle de vie des applications

Tâches / Activités	CNRS MOE	CNRS CdPIS	CNRS Exploitation	Titulaire	Remarques
Exécution d'un script	A/C	I	I	R	
Modification de fichiers/dossiers	A/C	I	I	R	
Restauration de fichiers	A	I	R	C/I	Demande à adresser à l'Exploitation
Restauration de VMs	A	I	R	C/I	Demande à adresser à l'Exploitation

Contrôle bon fonctionnement de l'application via URL	A	I	I	A/R	
Fourniture et installation des certificats	A	I	R	C/I	Demande à adresser à l'Exploitation
Monitoring de la durée de vie des certificats			R		
Debugging applicatif	A/C	I	I	R	
Dump bdd	A/C	I	I	R	
Logs (consultation)	A/C	I	I	R	