REPUBLIQUE FRANCAISE

Shom

Établissement public administratif

Sous tutelle du ministère des armées

CAHIER DES CLAUSES TECHNIQUES PARTICULIERES

ACCORD-CADRE 26AC16

Maintien en conditions opérationnelles et de sécurité du Digital Workplace « Odyssée » du Shom

Table des matières

1. Acronymes - Terminologie 3
2. Présentation générale de l'accord-cadre 4
2.1 Objet du document 4
2.2 Contexte et enjeux 4
3. Description de l'existant 5
3.1 Schéma d'architecture technique 5
3.2 Caractéristiques des VM de production 5
3.3 Lien avec l'Annuaire 6
3.4 Synchronisation annuaire Shom et annuaire de la digital workplace 7
3.5 Lien avec le SSO - Authentification - SSO 7
3.6 Lien Zimbra avec la Messagerie et le Calendrier 8
3.7 Architecture à maintenir 8
4. Besoin global et stratégie de mise en œuvre 9
5. Exigences relatives à la conduite du MCO/MCS et des évolutions 9
5.1 Les acteurs 9
5.2 Dispositif de suivi et de pilotage 10
5.3 Exigences relatives à la gestion de la documentation 10
6. Poste 1 : Montée en compétences 11
6.1 UO du poste : 12
6.2 Livrables attendus du poste 1 12
7. Poste 2 : MCO – MCS et assistance de la solution de digital workplace Odyssée. 12
7.1 Maintenance corrective, évolutive et MCS 12
7.2 Assistance / Support technique 14
7.3 UO du poste 14
7.4 Livrables attendus du poste 2 14
8. Poste 3 : Prestation d'accompagnement sur les modules de travail collaboratif 15
9. Poste 4 : Prestations complémentaires 15
9.1 Prestations complémentaires de déploiement 15
9.2 Prestations complémentaires de maintenance et d'assistance 16
9.3 Prestations complémentaires d'upgrade de version 16
9.4 Prestations complémentaires de formation 16
9.5 Prestations de réversibilité 17
10. Protection des données à caractère personnel 18
11. Numérique responsable 18
12. ANNEXES 19
12.1 ANNEXE I : MODULES DÉPLOYÉS SUR ODYSSÉE 19
12.2 ANNEXE II : STRUCTURE DE L'ANNUAIRE SHOM 21
12.3 ANNEXE III : RÈGLES DE FILTRAGE IMPLÉMENTÉE DANS ODYSSÉE 27
12.4 ANNEXE IV : RECAPITULATIF DES USAGES D'ODYSSEE SUR 1 AN A LA DATE DU 20 JANVIER 2026 28
12.5 ANNEXE V : INFORMATION ET VOLUMETRIE ACTUELLE SUR ODYSSEE 34
12.6 ANNEXE VI : CADRE DE COHÉRENCE TECHNIQUE DU S.I SHOM 37

1. Acronymes - Terminologie

Acronyme	Signification
CCAP	Cahier des Clauses Administratives Particulières
CCT	Cadre de Cohérence Technique
CCTP	Cahier des Clauses Techniques Particulières
CMIS	Content Management Interoperability Service
CMS	Content Management System
COP	Contrat d'Objectifs et de Performance
DCE	Dossier de Consultation des Entreprises
DMZ	Demilitarized zone (zone démilitarisée)
DRH	Direction (Directeur) des Ressources Humaines
DSI	Direction (Directeur) des Systèmes d'Information
EI	Exigence Importante
EP	Exigence Primordiale
EPA	Etablissement Public à caractère Administratif
ESM	Enterprise Service Management
GEC	Gestion Electronique du Courrier
GED	Gestion Electronique de Documents
IT	Information Technology
ITSM	Information Technology Service Management
LDAP	Lightweight Directory Access Protocol
MCO	Maintien en Condition Opérationnelle
MCS	Maintien en Condition de Sécurité
MEP	Mise En Production : déploiement d'une application en environnement de production
MER	Mise En Recette : déploiement d'une application en environnement de recette
MOM	Mise en ordre de marche
OS	Operating System : Système d'Exploitation
OSSI	Officier de Sécurité des Système d'Information
PAQ	Plan d'Assurance Qualité
QVT	Qualité de Vie au Travail
RSSI	Responsable de la sécurité des Systèmes d'Information
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information
SSO	Single Sign On : système permettant d'accéder à plusieurs applications en ne s'identifiant (saisie du login/mot de passe) qu'une seule fois
TIC	Technologies de l'Information et des Communications
TMA	Tierce Maintenance Applicative
UID	User ID : identifiant utilisateur
UO	Unité d'Œuvre
VA	Vérification d'aptitude

VM	Machine virtuelle. Sauf mention contraire explicite, une VM repose sur l'hyperviseur VMWare.
VSR	Vérification de service régulier

Dans le présent CCTP, les dénominations suivantes sont utilisées :

- « Pouvoir adjudicateur » : personne qui conclut l'accord-cadre avec le titulaire ;
- « Titulaire » : l'opérateur économique titulaire de l'accord-cadre ;
- « *digital workplace* » : plateforme numérique intégrée de travail collaboratif offrant des environnements de communication, collaboration, d'apprentissage, ainsi que des outils de productivité, accessible à distance par l'intermédiaire des TIC. Le *digital workplace* Shom, Odyssée repose sur la solution Jalios Workplace Liberty Edition (offre standard pré-packagée) adossée à un bastion en DMZ Jalios Teamwork, et ses modules associés, de l'éditeur Jalios.
- Dans la suite du document la solution « Jalios Workplace Liberty Edition » est abrégée en « Jalios Workplace ».
- « Socle fonctionnel standard » ou « socle standard » ou « socle » du *digital workplace* désigne la solution standard pré-packagée Jalios Workplace, complétée de quelques modules additionnels (cf. annexe I) ;
- « Fonctionnalités complémentaires » ou « fonctionnalités enrichies » du *digital workplace* désignent les modules complémentaires qui pourront venir compléter le socle du *digital workplace* Shom (cf. annexe I) ;
- « Déploiement » : désigne l'ensemble des opérations d'installation, de paramétrage, de configuration et d'intégration au sein du SI du Shom de la solution Jalios Workplace et de ses modules additionnels.

2. Présentation générale de l'accord-cadre

2.1 Objet du document

L'objet de ce CCTP est de spécifier les modalités de MCO/MCS et TMA de l'environnement numérique de travail collaboratif de type *digital workplace* basé sur les solutions Jalios Workplace et Teamwork.

Le *digital workplace* déployé permet à tous les agents du Shom d'accéder aux applications, aux informations et aux connaissances nécessaires à leur activité quotidienne. Il est le portail applicatif, informatif et un lieu de partage et de ressources pour tous les agents du Shom.

Les différentes exigences du présent CCTP sont numérotées comme suit :

- EP-n : identifie une exigence primordiale

avec n l'index de chaque exigence.

2.2 Contexte et enjeux

2.2.1 Présentation générale du Shom

Le Shom (www.shom.fr) est un établissement public à caractère administratif (EPA) placé sous la tutelle du ministère des armées.

Basé principalement à Brest, il comporte des implantations en région parisienne, à Toulouse, en Polynésie et en Nouvelle Calédonie. Il totalise un effectif de 550 personnes environ.

Sa vocation est de garantir la qualité et la disponibilité de l'information physique maritime, côtière et océanique, en coordonnant son recueil, son archivage et sa diffusion, pour satisfaire au moindre coût les besoins publics, militaires et civils.

2.2.2 Contexte fonctionnel

En 2023, le Shom a modernisé son Intranet et a adopté un Digital Workplace basé sur la solution Jalios. Le marché d'intégration, d'accompagnement fonctionnel et de mise en œuvre intégrait une composante de MCO. Ce dernier arrive à échéance en 2026. Le présent accord-cadre a pour but de répondre aux besoins de continuité de service de manière sécurisée et d'évolution de la plateforme pour répondre aux besoins à venir du Shom.

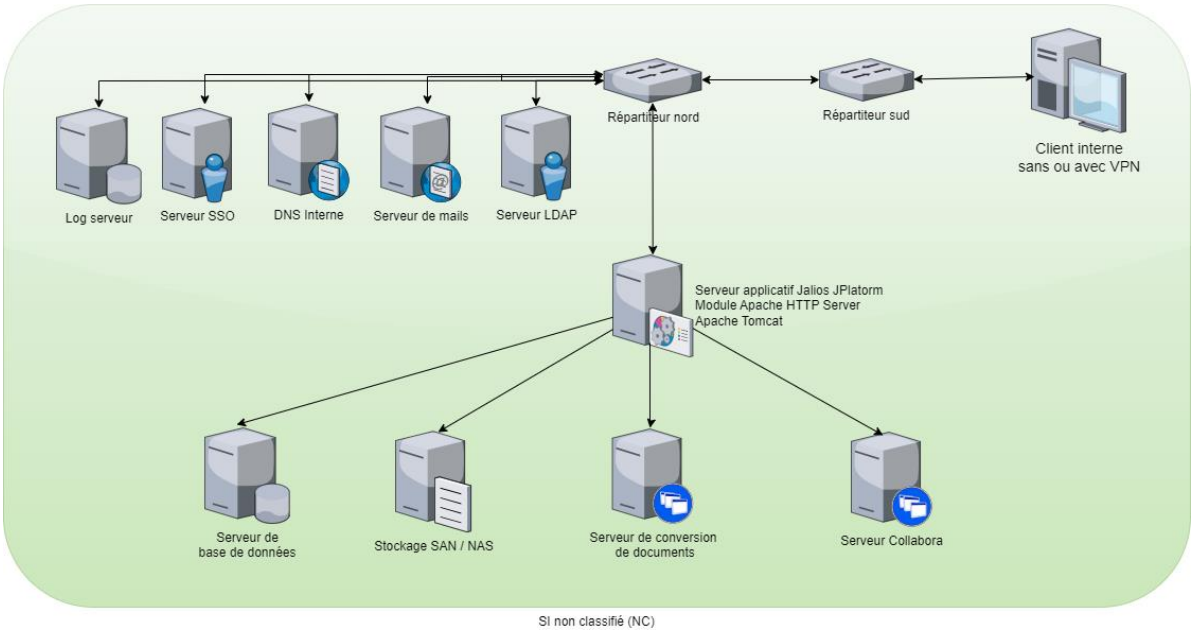
2.2.3 Contexte technique

Pour la réalisation de ses missions, le Shom met à la disposition de ses agents un environnement numérique de travail accessible au moyen de différents outils dont principalement des postes clients fixes ou portables. Par ces moyens, le personnel Shom accède aux applications nécessaires à leur travail soit en local sur leur poste, soit directement sur les serveurs sur lesquels elles sont hébergées, soit en ligne par l'intermédiaire d'un intranet qui fédère une grande partie des ressources disponibles sur le SI.

Le contexte technique dans lequel est intégré l'environnement numérique de travail collaboratif est décrit dans le cadre de cohérence technique (CCT) en annexe VI.

3. Description de l'existant

3.1 Schéma d'architecture technique



3.2 Caractéristiques des VM de production

Le digital workplace Shom fonctionne sur l'application Jalios Workplace Liberty (anciennement Jalios JPlatform) en version 10 SP6. L'upgrade vers la SP8 est actuellement en cours et sera effectif au début de la prestation.

Tableau de caractéristiques des VM de production du digital workplace Shom

VM => Caractéristiques	VM applicative	VM de conversion PDF	VM de base de données	VM d'édition collaborative
Système d'exploitation	Debian Bullseye	Debian Bullseye	Debian Bullseye	Debian Bullseye
Logiciel	Workplace Liberty 10 SP6 Apache HTTPD 2.4.55	Jodconverter 2.2.2-12	PostgreSQL 13.11	Collabora 1.3.7
vCPU	16	4	4	4
RAM en Go	32	8	8	8
Partition système en Go	64	64	64	64
Partition data en Go	500			128

EP-1 Le titulaire assure le MCO, MCS et la TMA sur les VM de l'environnement de production du digital workplace Shom.

EP-2 Le titulaire assure un fonctionnement opérationnel des VM de l'environnement de pré-production du digital workplace Shom.

3.3 Lien avec l'Annuaire

L'annuaire Shom constitue la référence pour toutes les applications qui possèdent un annuaire interne. Les caractéristiques de l'annuaire Shom sont décrites dans le CCT en annexe VI. La structure de l'annuaire Shom, notamment l'usage d'adresses fonctionnelles, et le mécanisme de délégation de fonctions sont décrits en annexe II.

L'annuaire interne du *digital workplace* peut être enrichi et complété de données nouvelles n'appartenant pas à l'annuaire de référence Shom.

EP-3 Le titulaire garantit la continuité de l'interface avec l'annuaire OpenLDAP du Shom. En cas de modification de l'annuaire du Shom (Migration vers un AD par exemple), une prestation complémentaire sera engagée via le poste 5.

EP-4 Les informations suivantes de l'annuaire Shom sont récupérées pour alimenter le *digital workplace* :

- Les personnes et leurs attributs renseignés dans l'annuaire Shom ;
- Les autres « objets » de l'annuaire Shom : fonctions, entités, processus, projets et groupes de circonstance ;
- Les adresses mail fonctionnelles contenues dans les objets de l'annuaire cités ci-dessus ;
- Les alias mail ;
- Dans la branche « Function » : les délégations de fonction.

EP-5 Le mécanisme de délégation de fonctions au Shom n'étant pas standard, le titulaire maintient le développement spécifique permettant de rapatrier les délégations de fonctions dans l'annuaire de la solution Jalios Workplace.

EP-6 Le titulaire maintient le mécanisme de synchronisation automatique entre l'annuaire Shom et celui de la solution Jalios Workplace. Ce dernier permet une tenue à jour de l'annuaire du *digital workplace* en temps différé d'au maximum 12 heures (une nuit). Ce mécanisme est appelable manuellement pour une mise à jour instantanée.

3.4 Synchronisation annuaire Shom et annuaire de la digital workplace

Un script de synchronisation de l'annuaire de la digital workplace se déclenche toutes les nuits. Il récupère un certain nombre d'attributs de l'annuaire Shom pour alimenter les comptes du digital workplace.

Ci-dessous le tableau des attributs récupérés.

Champs JCMS	Attribut LDAP
Compte Utilisateur	uid
Nom	attribut « sn » pour un user
Prénom	attribut « givenName » pour un user
Civilité	Non synchronisé
Organisation	Donnée non présente dans l'annuaire. Valeur déterminée selon l'adresse mail: SHOM si adresse mail en @shom.fr, EXTERNES si adresse mail en @externes.shom.fr STAGIAIRE si adresse mail en @stagiaire.shom.fr
Service	attribut « ou » pour un user
Fonction	Attribut « role » pour un user A distinguer des fonctions présentes dans la branche Fonctions de l'annuaire et pour laquelle il peut y avoir plusieurs fonctions pour la même personne.
Email	attribut « mail » pour un user
Telephone	attribut « telephoneNumber » pour un user
mobile	Non synchronisé
Coordonnée	Non synchronisé
Boite Postal	Non synchronisé
Ville	Non synchronisé
province	Non synchronisé
pays	Non synchronisé
Coordonnées	Non synchronisé
Information	Non synchronisé

3.5 Lien avec le SSO - Authentification - SSO

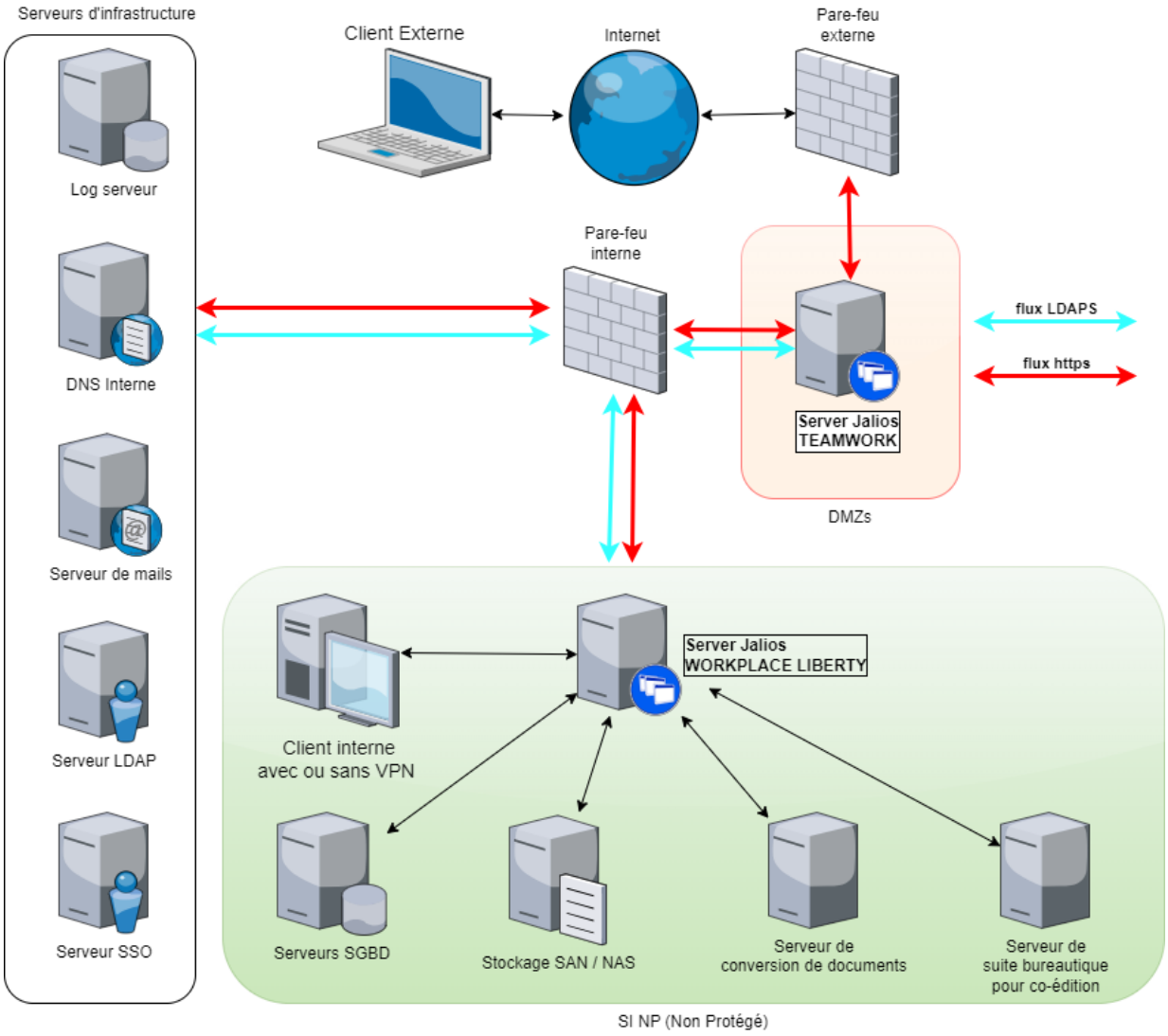
EP-7 Le titulaire maintient en condition opérationnelle le mécanisme de SSO utilisé au Shom (voir CCT en annexe VI) dans le *digital workplace*.

3.6 Lien Zimbra avec la Messagerie et le Calendrier

EP-8 Le titulaire maintient en condition opérationnelle la disponibilité de la messagerie Zimbra et des calendriers dans le Digital Workplace.

3.7 Architecture à maintenir

Le schéma ci-dessous présente l'architecture actuelle sur laquelle se rajoute le produit Jalios Teamwork.



Le logiciel Teamwork accueillera dans le courant de l'année 2026 des espaces collaboratifs ouverts sur l'extérieur sur un niveau de sécurité NP (Non Protégé). Cette évolution sera effective dès la notification du marché.

Des espaces collaboratifs internes au Shom sont gérés par Workplace Liberty.

Une liste à jour des espaces collaboratifs utilisables sur Jalios Workplace Liberty et Jalios Teamwork sera créée sur Jalios Workplace Liberty fin 2026. Elle constituera la seule interface existante entre Jalios Workplace Liberty et Jalios Teamwork.

Les données fournies par Teamwork au socle principal (Jalios Liberty) permettant la mise à jour de la liste des espaces collaboratifs seront communiquées par Teamwork sous forme de service web.

EP-9 Le titulaire assure le MCO, MCS et la TMA sur l'application Jalios Teamwork.

EP-10 Le titulaire assure le MCO, MCS et la TMA sur l'interface entre Jalios Teamwork et Jalios Workplace Liberty.

A date le Shom dispose de 700 licences liberty, 250 Collabora et 200 licences Teamwork.

4. Besoin global et stratégie de mise en œuvre

Afin de répondre au besoin de continuité de service sécurisée et d'évolution d'Odyssée, l'accord-cadre est décomposé en 4 postes.

Poste	Intitulé
1	Montée en compétences.
2	MCO – MCS et assistance de la solution de digital workplace Odyssée.
3	Prestation d'accompagnement sur les modules de travail collaboratif.
4	Prestations complémentaires (Réversibilité, upgrade de version non contenue dans le MCS, évolutions sur les modules spécifiques Shom et/ou l'intégration de nouveaux modules spécifiques Shom, formation, intervention sur site …)

5. Exigences relatives à la conduite du MCO/MCS et des évolutions

5.1 Les acteurs

5.1.1 Équipe du titulaire

EP-11 Le titulaire désigne un responsable de la prestation, interlocuteur privilégié du gestionnaire de configuration d'Odyssée au Shom (cf. 5.1.2) pour l'ensemble des prestations. Le responsable sera le garant, coté titulaire, du bon déroulement de la réalisation des prestations. A ce titre, il aura pour responsabilité de :

- définir les charges propres au titulaire, le planning et l'organisation des différentes étapes de chaque prestation ;
- suivre l'état d'avancement des prestations ;
- proposer ou prendre les mesures nécessaires pour que l'avancement soit cohérent avec les objectifs des prestations (en concertation avec le gestionnaire de configuration d'Odyssée) ;
- veiller au bon déroulement de toutes les prestations ;
- coordonner les équipes coté titulaire ;
- alerter le gestionnaire de configuration d'Odyssée en cas de difficulté(s) ;
- animer les comités de pilotage de suivi de la prestation.

EP-12 Le titulaire met en place une organisation afin de répondre aux exigences des prestations de MCO, MCS et TMA.

5.1.2 Équipe Shom

L'équipe du Shom est composée :

→ d'un gestionnaire de configuration d'Odyssée, responsable côté Shom ;

→ d'un pilote technique de la Division du système d'information du Shom. Il sera l'interlocuteur privilégié pour la gestion des accès à l'infrastructure Shom et les opérations techniques.

5.2 Dispositif de suivi et de pilotage

EP-13 Le titulaire met en place un dispositif de pilotage et de suivi de réalisation des prestations.

EP-14 Ce dispositif de pilotage et de suivi comprend notamment un Comité de pilotage, constitué a minima :

- Pour le titulaire, du responsable de la prestation.
- Pour le Shom, du gestionnaire de configuration et du pilote technique de la DSI. Ce comité de pilotage se réunit au moins 1 fois par an et autant que de besoin selon l'activité de TMA.

Les réunions de ce comité de pilotage projet se déroulent en distanciel par des moyens de télécommunications adaptés (réunion téléphonique, visioconférence).

EP-15 Chaque réunion donne lieu à la rédaction d'un compte rendu synthétique par le titulaire dans un délai de 3 jours ouvrés. Il est transmis au Shom par mail pour approbation. Le Shom dispose alors de 5 jours ouvrés pour fournir ses remarques.

EP-16 Une réunion de lancement est organisée sous 30 jours après notification de l'accord-cadre.

Cette réunion de lancement se tient en présentiel dans les locaux du Shom à Brest.

Lors de cette réunion de lancement, le titulaire détaille à minima les points suivants :

- Présentation des membres de l'équipe ;
- Validation de l'organisation générale de la prestation et des procédures d'échanges entre les intervenants ;
- Présentation des moyens et des différentes tâches à effectuer pour réaliser le poste 1 de montée en compétences.

EP-17 Le titulaire rédige un compte rendu synthétique de cette réunion de lancement et le transmet au Shom par mail pour approbation dans un délai de 3 jours ouvrés. Le Shom dispose alors de 5 jours ouvrés pour fournir ses remarques.

5.3 Exigences relatives à la gestion de la documentation

EP-18 Le titulaire propose un espace documentaire projet partagé et accessible aux référents désignés du Shom. Ce dernier peut être un espace collaboratif d'Odyssée ouvert à l'extérieur.

EP-19 Les documents sont rédigés en français. Les circuits de visa pour prise en compte des commentaires du Shom avant validation officielle sont réalisés par voie électronique.

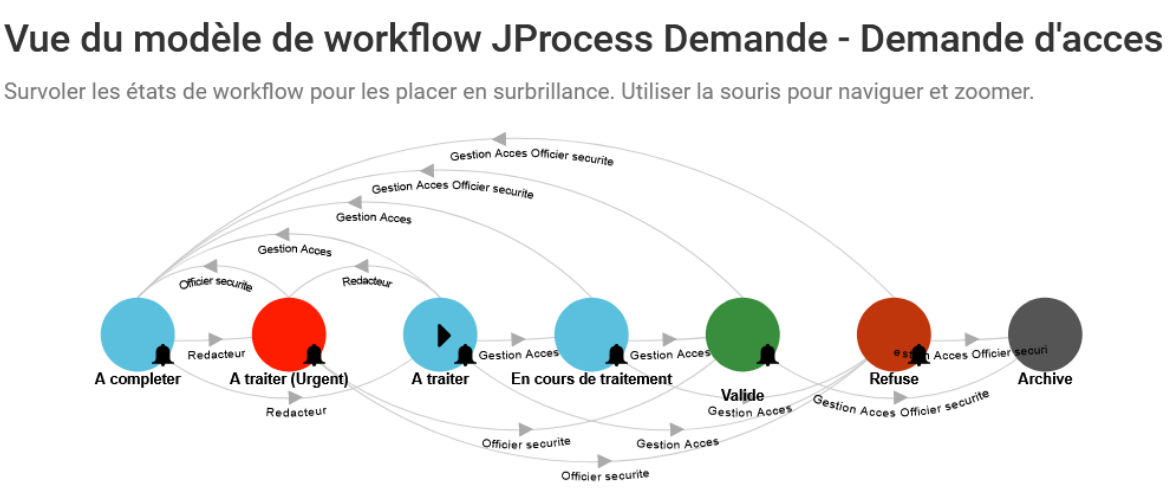
EP-20 Le titulaire définit et exécute un processus de contrôle préalable en interne sur la forme et le fond avant toute livraison au Shom.

6. Poste 1 : Montée en compétences

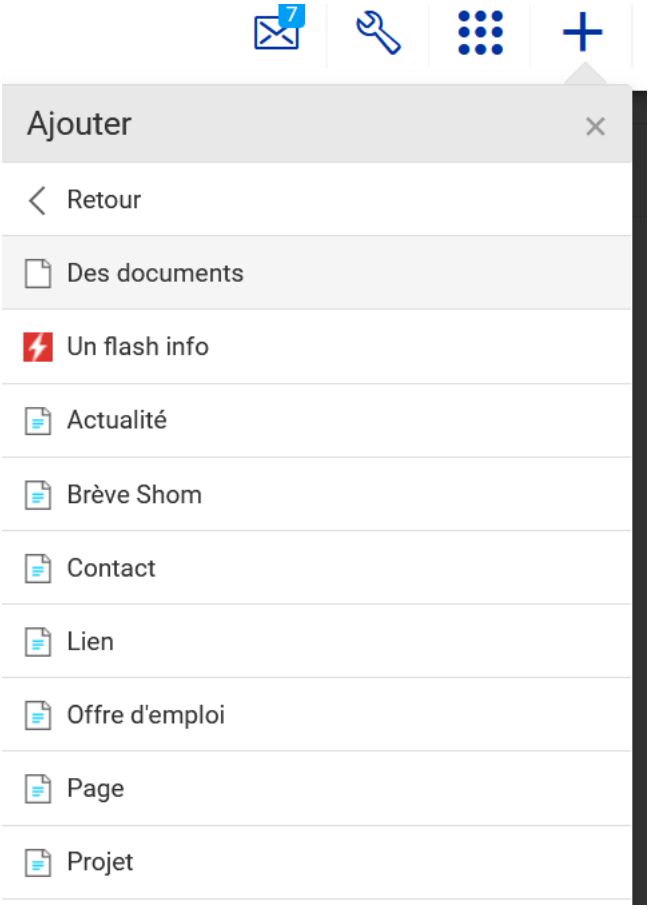
EP-21 Le titulaire planifie et met en œuvre une période de montée en compétences.

EP-22 Le périmètre technique est décrit au paragraphe 3. D'un point de vue fonctionnel, outre le paramétrage des 2 plateformes JALIOS (Liberty et Teamwork) non spécifiques, se rajoutent :

- un process spécifique pour le workflow de demande d'accès au site qualifié de difficulté moyenne dont voici le diagramme d'état :

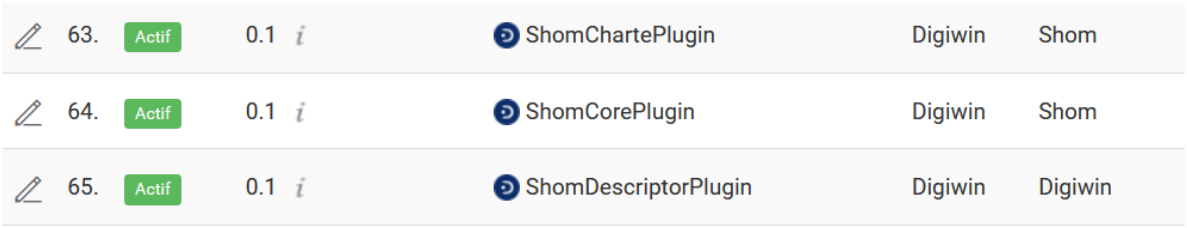


- Des types de contributions spécifiques avec leur mise en œuvre dans le CMS de la plateforme liberty :



- Et la mise en œuvre de la charte graphique du Shom.

Ces spécificités sont paramétrées et intégrées sous la forme de trois modules spécifiques :



Ces éléments sont documentés et le code est maintenu par le titulaire du précédent accord-cadre. Ces documentations, codes et accès total aux environnements Jalios du Shom seront fournis au titulaire du présent accord-cadre comme livrables d'entrée du poste.

6.1 UO du poste :

- P1-DEP1

6.2 Livrables attendus du poste 1

- Plan de montée de compétences ;
- Tableau de suivi de la montée en compétences du titulaire ;
- Documentation existante annotée et amendée de la description des éventuelles lacunes.

EP-23 A la fin de cette période, le titulaire est réputé être en pleine capacité d'assurer les MCO, MCS et TMA sur Odyssée. En cas de défaillances ultérieures, le titulaire prendra à sa charge les conséquences de celles-ci.

7. Poste 2 : MCO – MCS et assistance de la solution de digital workplace Odyssée.

Ce poste couvre la maintenance (corrective et évolutive) ainsi que l'assistance sur les modules de Jalios Workplace déployés initialement et à la suite de demande d'évolutions.

EP-24 Le titulaire assure la maintenance de ce qui a été livré, paramétré et conçu. Il assure aussi la maintenance et/ou la mise à niveau vers chaque nouvelle version du *digital workplace* ainsi que l'assistance au personnel Shom qui administre la plateforme.

7.1 Maintenance corrective, évolutive et MCS

EP-25 Le titulaire a la charge de la maintenance du *digital workplace* (incluant tous les modules associés déployés) ainsi que de la documentation produite. La maintenance s'applique à tous les éléments livrés et concerne toutes les possibilités d'intégration, de paramétrage et de configuration de ces éléments.

EP-26 Le titulaire assure la maintenance corrective et évolutive de l'ensemble du système intégré au SI Shom pendant la période de MCO.

EP-27 En cas d'alerte de sécurité, le titulaire applique les préconisations éditeur sur le digital workplace du Shom en relation avec le RSSI du Shom et l'OSSI du Shom.

Chaque livraison fait l'objet d'opérations de vérification d'aptitude (VA) et de vérification de service régulier (VSR).

EP-28 Chaque composant livré et accepté par le Shom fait l'objet d'une garantie.

EP-29 Les mises à jour correctives, évolutives ou de sécurité livrées au Shom sont historisées et archivées.

7.1.1 Maintenance corrective

La maintenance corrective recouvre la correction des anomalies et dysfonctionnements logiciels du *digital workplace*.

EP-30 Le titulaire met à disposition du Shom une plateforme de saisie en ligne des anomalies. Cette plateforme permet de suivre le traitement des anomalies jusqu'à leur résolution.

Cette plateforme de saisie en ligne est accessible en mode web par les administrateurs techniques et fonctionnels. Elle permet de récupérer (d'exporter) en fin de contrat l'ensemble des tickets pour être conservés par le Shom.

EP-31 Lors de la prise en compte de l'anomalie, le titulaire identifie si celle-ci est de son domaine de responsabilité ou imputable au produit. Dans les deux cas, le titulaire reste l'unique interlocuteur du Shom dans le traitement de l'anomalie.

EP-32 L'anomalie est qualifiée (gravité, impact) en accord avec le Shom.

EP-33 Le titulaire résout les anomalies et dysfonctionnement dans les délais consignés dans le tableau ci-dessous en fonction de la qualification des anomalies :

Qualification de l'anomalie	Délai de prise en charge (GTI)	Délais de résolution (GTR)
Bloquante	0.5 jours ouvrés	2 jours ouvrés
Majeure	2 jours ouvrés	10 jours ouvrés
Mineure	5 jours ouvrés	3 mois calendaires

Bloquante : anomalie ou dysfonctionnement entrainant un arrêt d'une fonction empêchant toute poursuite de l'utilisation du logiciel, même de façon dégradée avec un impact fort (population touchée ou activité soutenue).

Majeure : anomalie ou dysfonctionnement entrainant un arrêt d'une fonction empêchant toute utilisation nominale du logiciel. Un contournement est possible avec un impact relatif (population touchée ou activité soutenue).

Mineure : anomalie ou dysfonctionnement pouvant ne pas entrainer d'arrêt de fonction et ne présentant pas de conséquences lors de l'utilisation du logiciel.

Le délai de pris en charge démarre à partir de la déclaration de l'anomalie.

Les délais de résolution des anomalies démarrent à partir de la qualification de celles-ci par le Shom sur la plateforme de saisie des anomalies. La plateforme notifie les anomalies au personnel du titulaire en charge de leur prise en compte dès la fin de leur saisie par le Shom.

Les temps de demande d'accès et d'accès effectif à l'infrastructure seront décomptés des délais annoncés.

Une anomalie sera considérée comme close après que le Shom ait reçu et vérifié la correction au problème exprimé.

EP-34 Les corrections des anomalies bloquantes et majeures sont livrées, sauf accord explicite, au fil de l'eau. Les corrections des anomalies mineures sont livrées par lots à date précise ou en même temps que l'envoi de corrections d'anomalies bloquantes ou majeures.

EP-35 La maintenance corrective couvre également le maintien de l'intégrité des données et le cas échéant, leur remise à niveau en cas de dégradation dans le cadre de l'utilisation normale du *digital workplace*.

7.1.2 Maintenance évolutive, MCS

La maintenance évolutive et le maintien en condition de sécurité recouvre le maintien à jour du *digital workplace* et de la documentation associée par rapport aux évolutions et corrections proposées par l'éditeur.

EP-36 Les mises à jour logicielles des licences et modules du *digital workplace* sont récupérées auprès de l'éditeur Jalios par le titulaire. Ce dernier effectue l'installation, l'intégration et la recette usine des nouvelles versions dans son environnement. Il vérifie en particulier la non régression technique et fonctionnelle des nouvelles versions par rapport aux paramétrages et aux travaux d'intégration effectués auparavant et mis en production au Shom. Il prend à sa charge tous travaux de réintégration ou de re-paramétrage nécessaires suite aux mises à jour logicielles.

EP-37 Afin que les montées de versions mineures ou majeures aient lieu sans besoin de reprendre en partie les travaux d'intégration et de paramétrage déjà effectués, le titulaire s'attache à intégrer et paramétrer les fonctionnalités du *digital workplace* en respectant au mieux les préconisations et règles de paramétrage de l'éditeur.

EP-38 Le titulaire livre au Shom des mises à jour s'installant de manière automatique et ne nécessitant pas ou peu d'actions manuelles complémentaires de la part des administrateurs techniques.

EP-39 Le titulaire informe le Shom des évolutions de la solution Jalios Workplace et soumet à l'approbation du Shom un planning de montée en version.

7.2 Assistance / Support technique

Afin d'améliorer la maîtrise de l'emploi du système, le Shom peut faire appel au titulaire sur des prestations ponctuelles d'assistance permettant d'approfondir l'expertise des correspondants techniques et fonctionnels du Shom sur des points particuliers (paramétrage de l'application, intégration dans le SI…).

EP-40 Le titulaire met à disposition une cellule de support technique joignable par mail, téléphone et tickets ainsi qu'une base de données de résolution des erreurs connues.

EP-41 Ce support technique est assuré en langue française.

EP-42 Les demandes du Shom doivent être prises en compte par le titulaire dans un délai de 5 jours ouvrés. Une réponse doit être apportée dans un délai maximum de 10 jours ouvrés.

A titre de volumétrie, 195 tickets auprès du support client ont été créés entre le 20 mars 2023 et le 23 janvier 2026.

7.3 UO du poste

- P2-DEP1

7.4 Livrables attendus du poste 2

Dans le cadre de la maintenance, pour chaque livraison reçue, qu'elle soit corrective ou évolutive, le titulaire fournit :

- Le paquet d'installation ;
- La mise à jour de la documentation suivante si celle-ci est impactée :

- Guide d'installation ;
- Guide d'administration technique et d'exploitation ;
- Guide d'administration fonctionnelle ;
- Guide utilisateur.

Dans le cadre de l'assistance, les réponses apportées (retour par mail, dans le ticket, au téléphone…) par le titulaire constituent les livrables.

8. Poste 3 : Prestation d'accompagnement sur les modules de travail collaboratif

Dans le cadre de l'amélioration de l'adoption du digital workplace par le personnel du Shom, il pourra être demandé au titulaire de :

- Livrer un nouveau module ;
- Modifier l'ergonomie du digitale workplace ;
- Modifier ou créer un workflow ;
- Assurer des prestations d'accompagnement ciblées.

De manière générale, des prestations spécifiques de formulation, de conception, de paramétrage, de communication ou d'information, pouvant être réalisées à distance ou sur site, pourront être commandées.

EP-43 Les actions de formation sur site ou à distance incluent systématiquement la fourniture d'un support de formation.

UO du poste :

- P3-DEP1.

Livrables attendus du poste 3 :

Selon la nature des prestations d'accompagnement commandées des livrables principalement documentaires (spécification, support de formation, guide utilisateur, rapport de paramétrage…) seront demandés.

9. Poste 4 : Prestations complémentaires

La solution Jalios Workplace comporte de nombreux modules auxquels de nouveaux modules sont régulièrement ajoutés. En cours d'exécution de l'accord cadre, il pourrait être nécessaire de déployer d'autres modules.

Ce poste permet ainsi, à travers un bordereau des prix, de commander des prestations complémentaires de déploiement, d'accompagnement, de maintenance et d'assistance.

Ce poste peut également permettre de réaliser des prestations de formation et de réversibilité.

9.1 Prestations complémentaires de déploiement

Des prestations complémentaires de déploiement (installation, intégration et paramétrage) peuvent être commandées afin de mettre en service d'autres modules de la solution Jalios Workplace/Teamwork non identifiés à ce stade.

Ces prestations complémentaires peuvent également porter sur la réalisation de connecteurs vers une application tierce (GED ou ITSM par exemple).

Ces prestations complémentaires peuvent également porter sur le paramétrage de workflows, spécifiés par le Shom, dans le module JProcess pour compléter/amender les workflows existants (demande d'accès au site, évaluation des formations).

UO du poste :

- P4-DEP1

Livrables attendus :

Les livrables attendus seront précisés dans le bon de commande correspondant.

9.2 Prestations complémentaires de maintenance et d'assistance

Si des modules complémentaires de la solution Jalios Workplace/Teamwork sont déployés ou si des connecteurs supplémentaires sont réalisés (cf. 9.1), des prestations complémentaires de maintenance (corrective et évolutive) et d'assistance peuvent être commandées afin d'en assurer le bon fonctionnement dans la durée du présent accord-cadre.

UOs du poste :

- P4-DEP2
- P4-DEP3

Livrables attendus :

Les livrables prévus au poste 2 seront étendus aux éventuels modules complémentaires déployés ou connecteurs supplémentaires réalisés dans le cadre de prestations complémentaires.

9.3 Prestations complémentaires d'upgrade de version

Il se peut que l'éditeur publie une nouvelle version dont les fonctionnalités sont pertinentes pour le Shom tout en maintenant le MCS de la version déployée au Shom. Ainsi, le Shom peut décider de déployer cette version.

UO du poste :

- P4-DEP4

Livrables attendus :

- Les environnements de recette puis de production (après VA et VSR) à jour de la nouvelle version.
- Le corpus documentaire à jour.

9.4 Prestations complémentaires de formation

Des prestations complémentaires de formation (administration, utilisation standard, utilisation d'Odyssée) peuvent être commandées afin de faire monter en compétence un nouveau gestionnaire de configuration, un nouvel agent dans l'équipe d'administration, un groupe de nouveaux arrivants...

Un bon de commande sera émis avec le périmètre (nombre de personnes, modalités sur site ou à distance, type de formation : usage, administration etc.) de la prestation et les livrables attendus.

UOs du poste :

- P4-DEP5
- P4-DEP6

Livrables attendus :

Les livrables attendus seront précisés dans le bon de commande correspondant. Nonobstant, chaque prestation complémentaire de formation donnera lieu à une séance de formation et la fourniture d'un support de formation.

9.5 Prestations de réversibilité

Les prestations complémentaires de réversibilité portent sur le transfert vers un autre prestataire de la maintenance et de l'assistance de la solution déployée (en cas de renouvellement d'accord cadre de MCO/MCS).

Cette prestation de transfert vers un prestataire serait commandée au plus tard dans le mois qui précède la fin du contrat.

Pour permettre au titulaire et au nouveau prestataire d'organiser au mieux l'affectation de leurs équipes, la réversibilité sera planifiée sur une durée maximum de deux mois.

Les opérations de transfert se dérouleront en trois phases :

- Première phase : le titulaire transmettra au repreneur l'ensemble des livrables qui sont remis lors de l'exécution de chaque prestation et l'intégralité de la documentation. Il veillera à transmettre un dossier exhaustif et à jour. Le cas échéant, il complétera la documentation existante, pour y intégrer les évolutions récentes. Au cours de cette période, le titulaire continuera à assurer la maintenance et l'assistance de la solution déployée. Le repreneur commencera la prise de connaissance ;
- Deuxième phase : Le repreneur approfondira la prise de connaissance. Le titulaire pourra être amené à effectuer des entretiens de transmission technique. Le titulaire poursuivra la maintenance et l'assistance de la solution déployée ;
- Troisième phase : le repreneur prendra en charge la maintenance et l'assistance de la solution déployée avec l'assistance du titulaire, qui se tiendra disponible pour répondre aux demandes de compléments d'information.

EP-44 La documentation sera fournie sous forme numérique et sera libre de tout droit de reproduction, adaptation et utilisation pour l'usage exclusivement interne du Shom.

EP-45 Lors des changements de version de la solution Jalios Workplace et de ses modules additionnels, la documentation produit associée si elle a été impactée par le changement de version, sera mise à jour. Les évolutions par rapport à la version précédente de la documentation concernée seront mises en évidence dans une note de livraison (release note).

UO du poste :

- P4-DEP7

Livrables attendus :

Les livrables attendus sont :

- Plan de transfert de compétences ;
- Tableau de suivi de la montée en compétences du nouveau titulaire ;
- Ensemble des livrables remis lors de l'exécution de chaque prestation et l'intégralité de la documentation ;
- Restitution des données issues de l'outil de ticketing.

10. Protection des données à caractère personnel

EP-46 Le titulaire conseille et accompagne le Shom pour garantir que le *digital workplace* déployé respecte le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données dit RGPD).

EP-47 Le paramétrage de la solution Jalios Workplace/Teamwork déployée sur le SI du Shom respecte le RGPD.

EP-48 Les actions de communication auprès des agents concourent également au respect du RGPD.

EP-49 Le guide d'administration technique et d'exploitation du système intégré dans le SI Shom, ainsi que la Charte d'utilisation du *digital workplace* précisent les dispositions prises pour se conformer au RGPD.

11. Numérique responsable

EP-50 Le titulaire fournira au Shom un plan de gestion et d'optimisation des ressources liées aux systèmes mis en œuvre dans le cadre de cet accord-cadre. A cet effet, il est demandé dans le mémoire technique de consigner les initiatives que le titulaire mettra en œuvre dans l'exécution de l'accord cadre.

12. ANNEXES

12.1 ANNEXE I : MODULES DÉPLOYÉS SUR ODYSSÉE

Modules faisant partie du socle du digital workplace

- Module Zimbra CS
- Module CAS (connexion SSO)
- Module Export PDF
- Module Visites Guidées et JGuide
- Module JProcess

Modules spécifiques développés par le précédent titulaire pour le Shom

- ShomCorePlugin
- ShomChartePlugin
- ShomDescriptorPlugin (désactivé)
- Module d'import Mediawiki
- Module d'import de la Photothèque

Module de rédaction collaborative

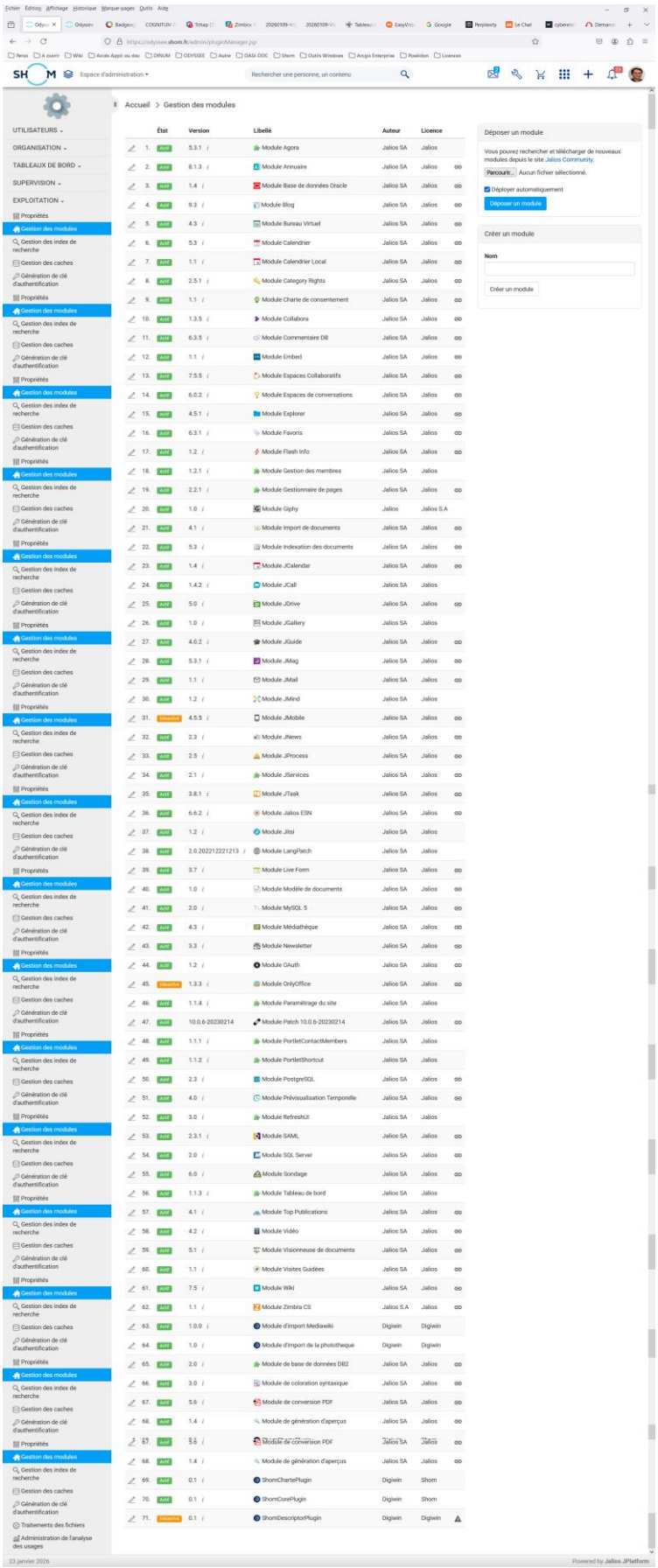
- Module d'édition collaborative Collabora

Module actuellement désactivé mais faisant partie de la solution acquise par le Shom mobile

- Module JMobile (acquis par le Shom mais non mis en œuvre)
- Module OnlyOffice (remplacé par le module Collabora)

Autres modules du digital workplace

Les autres modules du Digital Workplace sont ceux non mentionnés ci-dessus et indiqués dans la liste fournie en image écran ci-dessous.


Accueil > Gestion des modules
Déposer un module
Créer un module

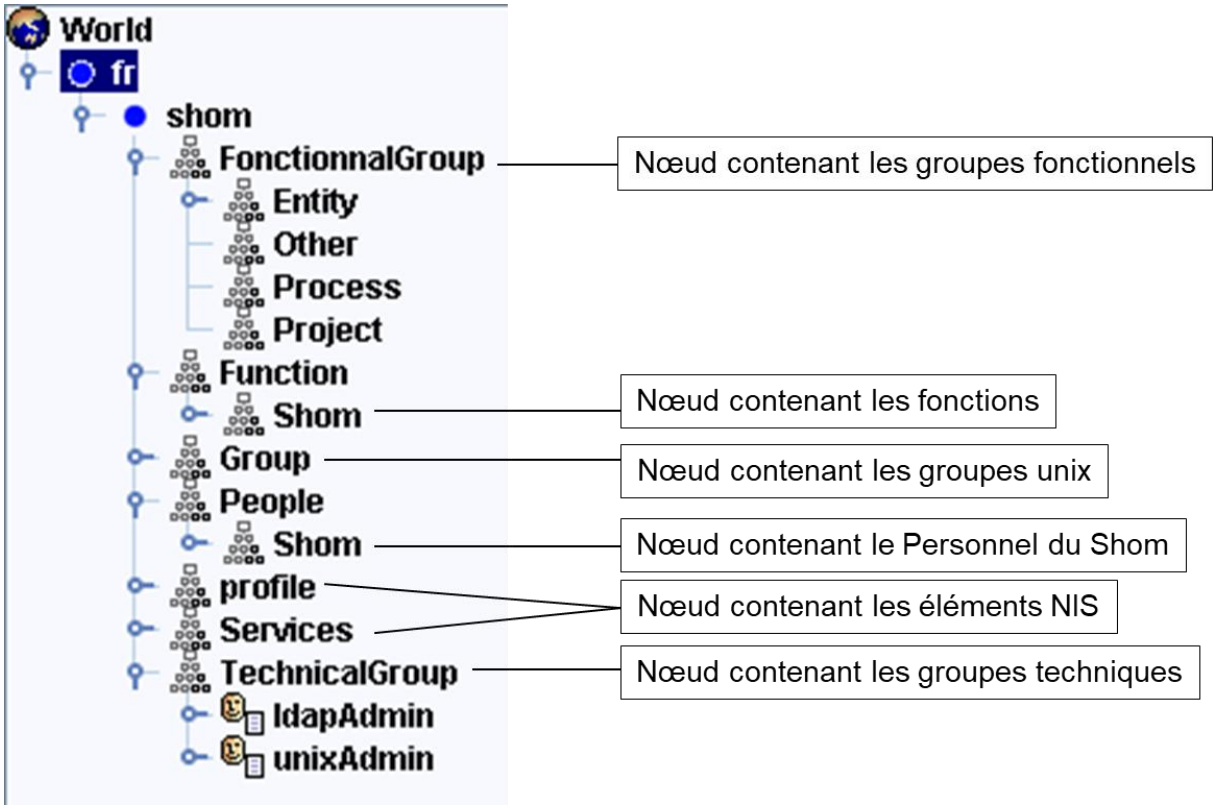
12.2 ANNEXE II : STRUCTURE DE L'ANNUAIRE SHOM

Les informations contenues dans l'annuaire LDAP du Shom sont stockées dans une structure de fichiers arborescente. L'organisation des informations de l'annuaire est détaillée ci-après.

L'historique des changements des informations de l'annuaire est stocké dans une base de données dont les tables relatives aux personnes et fonctions sont indiquées au III-5.

III-1. Arborescence générale de l'annuaire

Dans l'arborescence des objets de l'annuaire LDAP, les fonctions sont situées dans le nœud « Shom » sous le nœud « Function ».

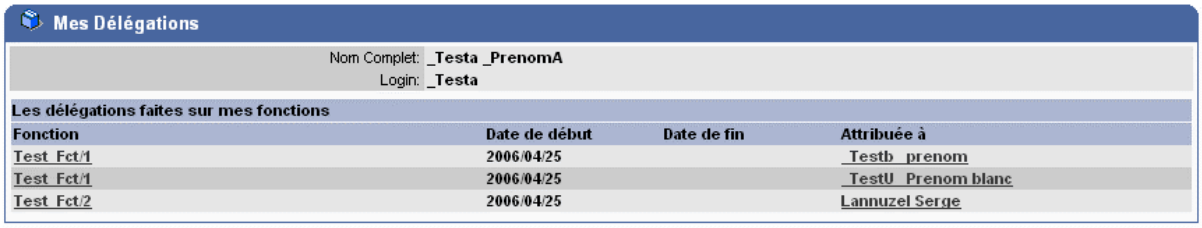


III-2. Branche « fonction » de l'annuaire

III-2.1. *Délégation de fonctions*

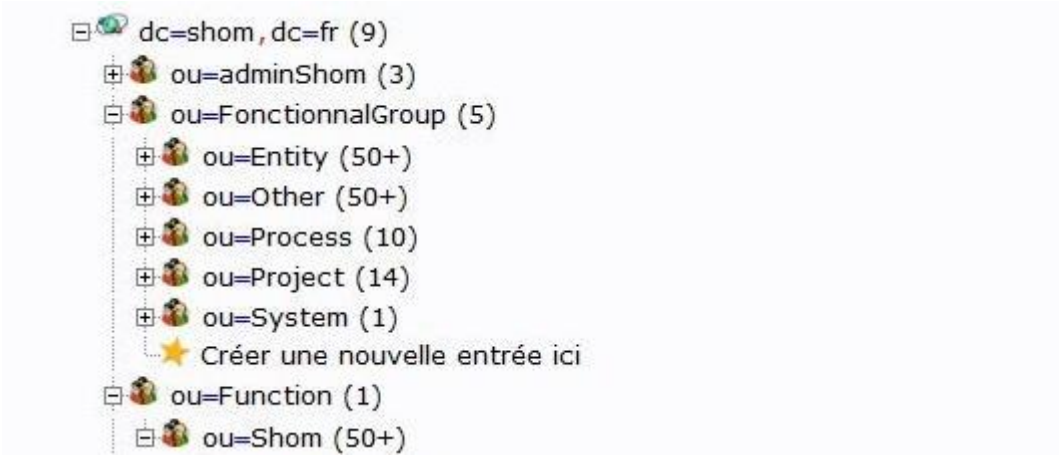
L'annuaire d'entreprise du Shom permet de rattacher des fonctions à une ou plusieurs personnes. Il autorise ensuite l'utilisateur à déléguer (temporairement ou sans date de fin) sa ou ses fonctions à une ou plusieurs personnes de son choix, notamment pendant ses congés.

Ci-dessous une fenêtre de l'interface utilisateur de l'annuaire présentant pour un utilisateur fictif les délégations qu'il a attribuées à d'autres personnes avec des dates de début et de fin (pas de date de fin dans l'exemple présenté).



III-2.2. *Visualisation de la branche « fonction » de l'annuaire*

Exemple de fonctions déclarées dans l'annuaire sous ou=Function, ou=Shom. Les noms sont anonymisés.



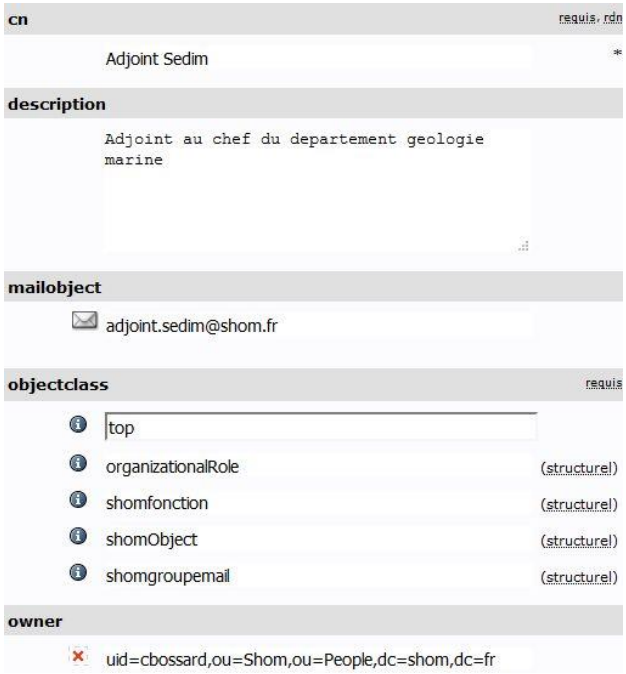
cn=dsi-pi-d
cn=dsi-pi-d_Prenom1 Nom1_20200323_20200327
cn=dsi-pi-d_Prenom2 Nom2_20200309_20200320
cn=dsi-pi-d_Prenom3 Nom3__

III-2.3. *Syntaxe d'une fonction attribuée à une personne*

Pour chaque personne à qui est attribuée la fonction « dsi-pi-d », l'annuaire crée un « cn » suffixé par « _Prénom Nom__ ». Lorsqu'une personne délègue temporairement (date de fin connue) ou non (pas de date de fin) une de ses fonctions à une autre personne, un « cn » suffixé par « _Prénom Nom__ » de la personne puis suffixé par « _DateDebut_DateFin » est généré : voir le schéma de la branche « fonctions » ci-dessus.

III-2.4. *Attributs d'une fonction*

Ci-après le détail, pour l'exemple de la fonction « Adjoint Sedim », des attributs d'une fonction :



III-2.5. *Gestion automatique des délégations*

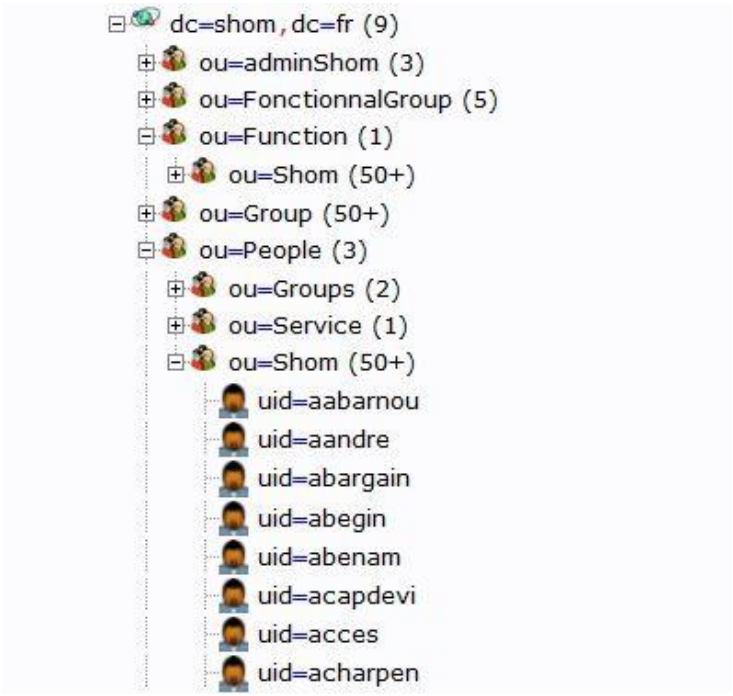
Les délégations de fonctions sont gérées automatiquement par le système. Une tache de fond de type « cron » compare la date du jour avec les dates de début et de fin des cn de type « fonction_Prénom Nom_DateDebut_DateFin » et les conserve ou supprime dans l'annuaire.

III-3. Branche « personne » de l'annuaire

Exemple de personnes déclarées dans l'annuaire sous ou=People, ou=Shom.

III-3.1. *Visualisation de la branche » personne » de l'annuaire*

Les personnes sont listées par leur « uid » qui correspond au login de l'utilisateur.



III-3.2. ***Attributs d'une personne***

Ci-dessous la liste des attributs utilisée pour une personne lorsqu'on sélectionne un UID :

Attachto
Bloque
Carlicense
Cn
Courriel
Employeettype
Gecos
Gidnumber
Givenname
Homedirectory
Homephone
Jpegphoto
l
Loginshell
Objectclass
Ordreentite
Ou
Role
Roomnumber
Sn
Telephone
Title
Type
Uidnumber
User Name

III-4. Récupération des données de l'annuaire en ligne de commande

III-4.1. ***Récupération des fonctions et délégations de fonctions***

Pour une personne donnée définie par son « UID », la requête LDAP permettant de récupérer ses fonctions et fonctions déléguées est la suivante (exemple pour l'UID « nom1 ») :

ldapsearch -LLL -x -h ldap -b "ou=function,dc=shom,dc=fr" "(personne=uid=nom1,ou=shom,ou=people,dc=shom,dc=fr)" fonction |grep ^fonction

Qui ramène comme résultat :

⇨ Les fonctions représentées par « cn= » rattachées à l'UID « nom1 »

fonction: cn=reseau,ou=Shom,ou=Function,dc=shom,dc=fr

fonction: cn=inf-pi-bas-d,ou=Shom,ou=Function,dc=shom,dc=fr

fonction: cn=dsi-pi-bas-d,ou=Shom,ou=Function,dc=shom,dc=fr

fonction: cn=dsi-pi-d,ou=Shom,ou=Function,dc=shom,dc=fr

III-4.2. ***Récupération des personnes pour une fonction donnée***

Pour une fonction donnée, la requête LDAP permettant de récupérer les « UID » des personnes rattachées à cette fonction ainsi que les « UID » des personnes à qui on a délégué cette fonction est la suivante (exemple pour la fonction « dsi-pi-d ») :

ldapsearch -xLLL -hldap -b"ou=function,dc=shom,dc=fr" "cn=dsi-pi-d" personne*

Qui ramène comme résultat :

⇨ La personne Prenom1 Nom1 qui a la fonction « dsi-pi-d »

dn: cn=dsi-pi-d, ou=Shom,ou=Function,dc=shom,dc=fr

dn: cn=dsi-pi-d_Prenom1 Nom1__, ou=Shom,ou=Function,dc=shom,dc=fr

personne: uid=nom1,ou=Shom,ou=People,dc=shom,dc=fr

⇨ La personne Prenom2 Nom2 qui a la fonction « dsi-pi-d » par délégation pour la période du 9 mars 2020 au 20 mars 2020

dn: cn=dsi-pi-d_Prenom2 Nom2_20200309_20200320, ou=Shom,ou=Function,dc=shom,dc=fr

personne: uid=nom2,ou=Shom,ou=People,dc=shom,dc=fr

⇨ La personne Prenom3 Nom3 qui a la fonction « dsi-pi-d » par délégation pour la période du 23 mars 2020 au 27 mars 2020

dn: cn=dsi-pi-d_Prenom3 Nom3_20200323_20200327, ou=Shom,ou=Function,dc=shom,dc=fr

personne: uid=nom3,ou=Shom,ou=People,dc=shom,dc=fr

III-5. Tables de la base de données historiques de l'annuaire LDAP

Ci-dessous les tables de l'annuaire LDAP du Shom concernées par les fonctions.

III-5.1. *Table « personne »*

```
CREATE TABLE `personne` (
  `id` int(10) unsigned NOT NULL auto_increment,
  `dateCreation` date default NULL,
  `idCreation` varchar(45) default NULL,
  `dateSuppression` date default NULL,
  `idSuppression` varchar(45) default NULL,
  `cn` varchar(45) default NULL,
  `uid` varchar(45) default NULL,
  `dn` varchar(128) default NULL,
  PRIMARY KEY (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=31115 ;
```

III-5.2. *Table « fonction »*

```
CREATE TABLE `fonction` (
  `id` int(10) unsigned NOT NULL auto_increment,
  `dateCreation` date default NULL,
  `idCreation` varchar(45) default NULL,
  `dateSuppression` date default NULL,
```

```
  `idSuppression` varchar(45) default NULL,
  `cn` varchar(45) default NULL,
  `description` varchar(128) default NULL,
  `dn` varchar(128) default NULL,
  PRIMARY KEY  (`id`)
```

III-5.3. ***Table « function personne »***

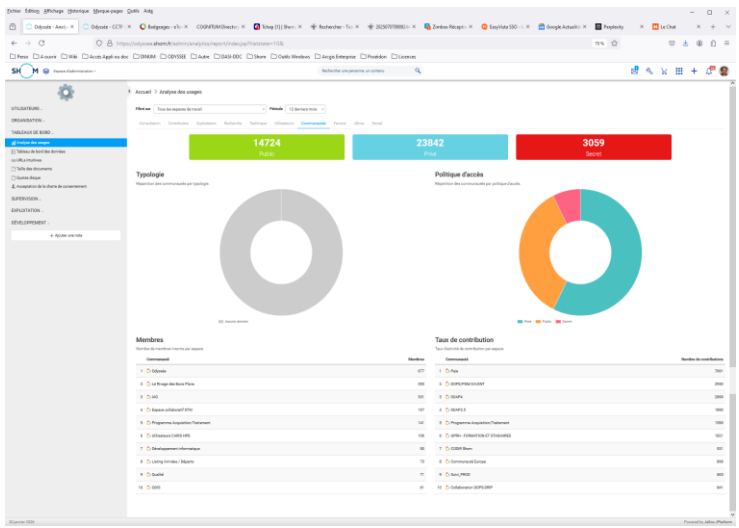
```
CREATE TABLE `fonction_personne` (
  `id` int(10) unsigned NOT NULL auto_increment,
  `dateCreation` date default NULL,
  `idCreation` varchar(45) default NULL,
  `dateSuppression` date default NULL,
  `idSuppression` varchar(45) default NULL,
  `id_fonction` int(10) unsigned default NULL,
  `id_personne` int(10) unsigned default NULL,
  `date_debut` date default NULL,
  `date_fin` date default NULL,
  `id_deleguant` int(10) unsigned default NULL,
  `delegation` int(10) unsigned default NULL COMMENT '1 = c''est une dÃ©lÃ©gation\r\n0 = c''est une attribution',
  PRIMARY KEY  (`id`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=10886 ;
```

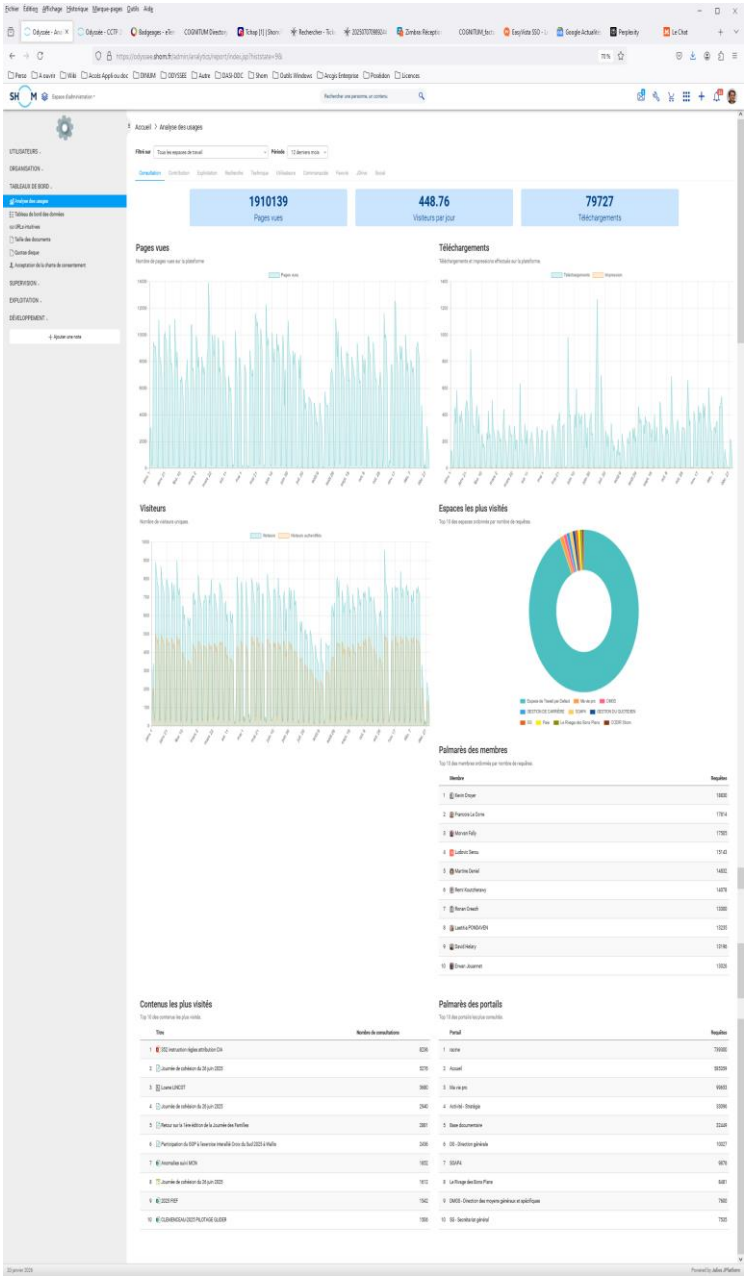
12.3 ANNEXE III : RÈGLES DE FILTRAGE IMPLÉMENTÉE DANS ODYSSÉE

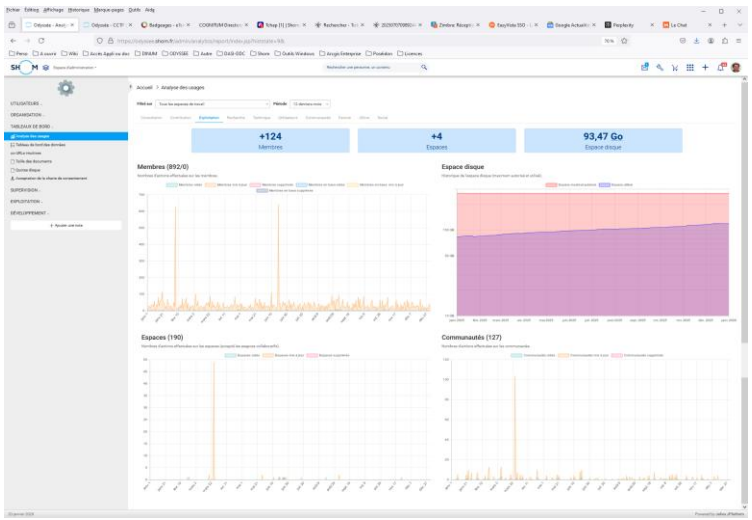
Un certain nombre de comptes de personnes n'appartenant pas au Shom sont rassemblés dans des entités dites fictives. Mis à part quelques exceptions, les comptes ayant pour attribut une entité fictive sont bloqués par le filtre de recherche LDAP. Le filtre de recherche LDAP mis en place dans ODYSSEE sélectionne les comptes à importer selon les règles suivantes :

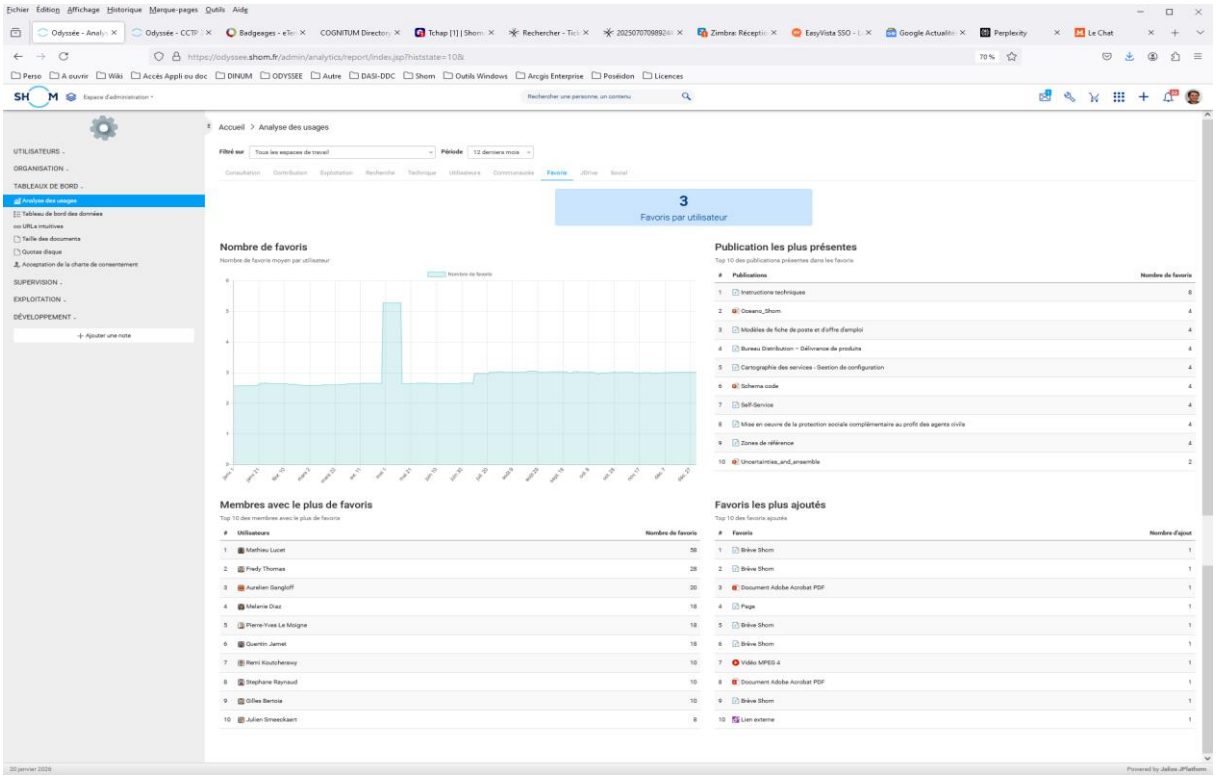
```
(|
(&
   (uid={0})                  Les comptes ayant un « uid »
   (objectClass=person)       Les comptes d'ObjectClass « person »
   (type=reel)                Les comptes de type « reel »
   (|                         Les comptes ayant un shell bash, ksh ou tcsh
      (loginshell=/bin/bash)
      (loginshell=/bin/externes.bash)
      (loginshell=/bin/ksh)
      (loginshell=/bin/tcsh)
   )
   (bloque=N)                       Les comptes non bloqués
   (ou=*)                     Les comptes dont l'entité est renseignée
   (!(ou=CISMF))              Les comptes dont l'entité n'est pas « CISMF »
   (!(ou=ComptesApplicatifs))       Les comptes dont l'entités n'est pas
                              «ComptesApplicatifs»
   (!(ou=DESACTIVES))         Les comptes dont l'entité n'est pas «DESACTIVES»
   (!(ou=HorsEntites))        Les comptes dont l'entité n'est pas «HorsEntites»
   (!(ou=OCI))                Les comptes dont l'entité n'est pas «OCI »
   (!(ou=restaurant))         Les comptes dont l'entité n'est pas «restaurant»
   (!(ou=Social))             Les comptes dont l'entité n'est pas «Social»
)
   (|
      (uid=fdebiais)          Le compte du prestataire responsable du MCO Odyssée
      (!(ou=Sous-Traitants)) Les comptes dont l'entité est «Sous-Traitants»
   )
)
```

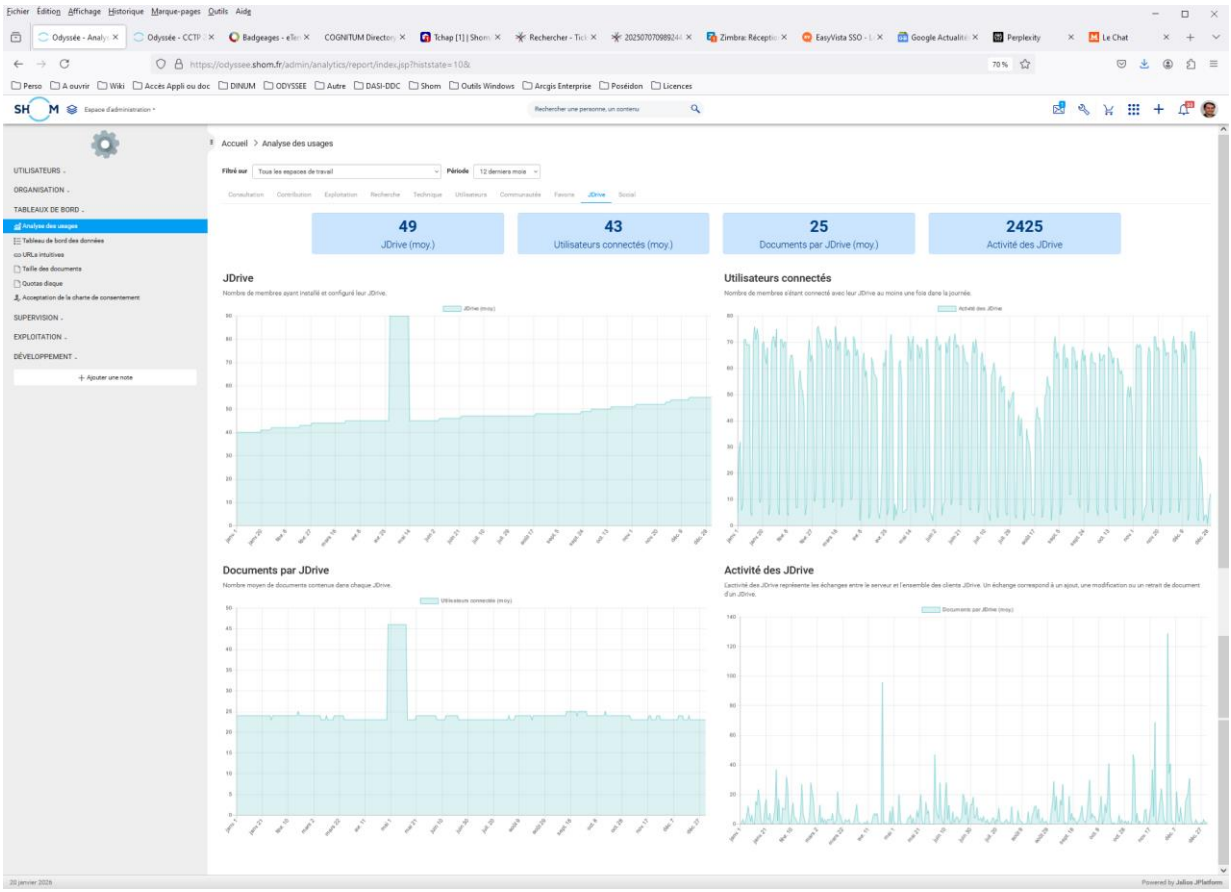
12.4 ANNEXE IV : RECAPITULATIF DES USAGES D'ODYSSEE SUR 1 AN A LA DATE DU 20 JANVIER 2026

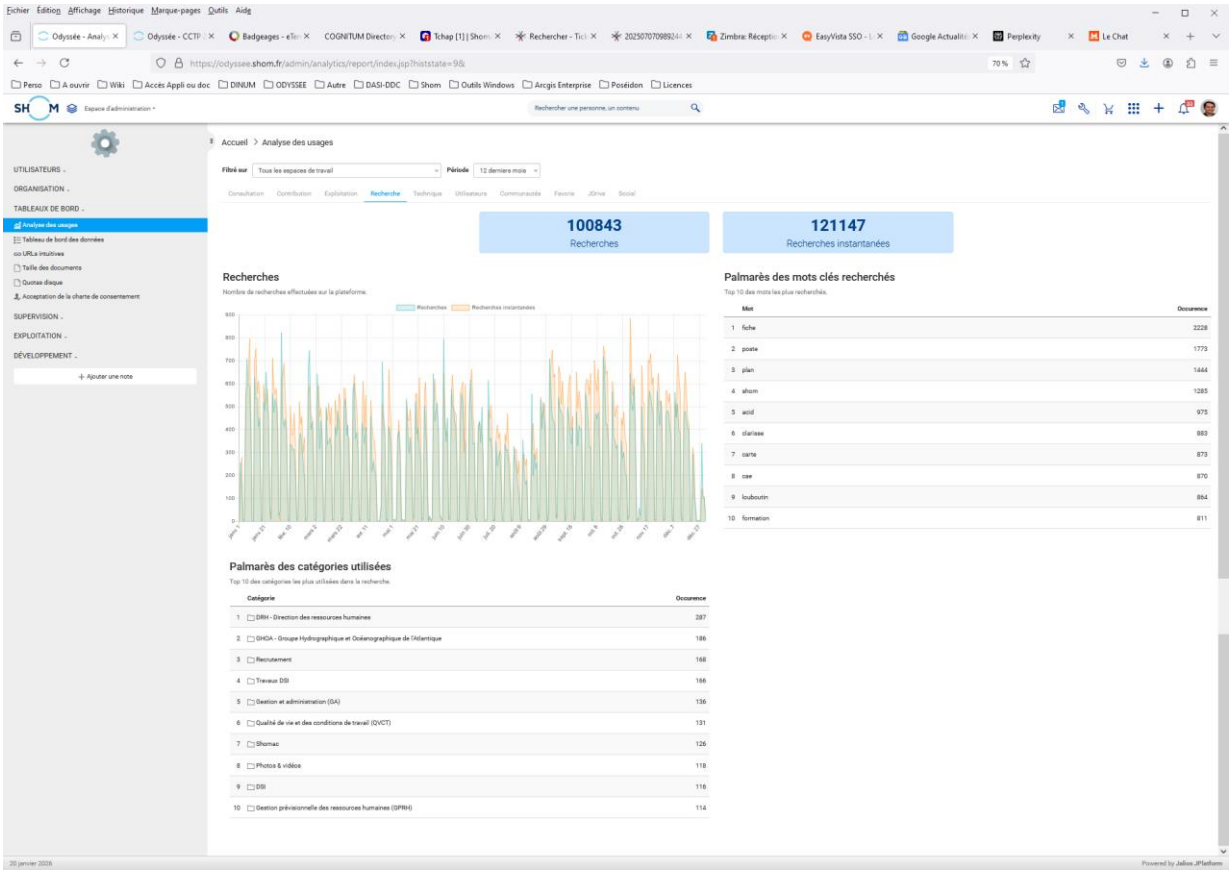


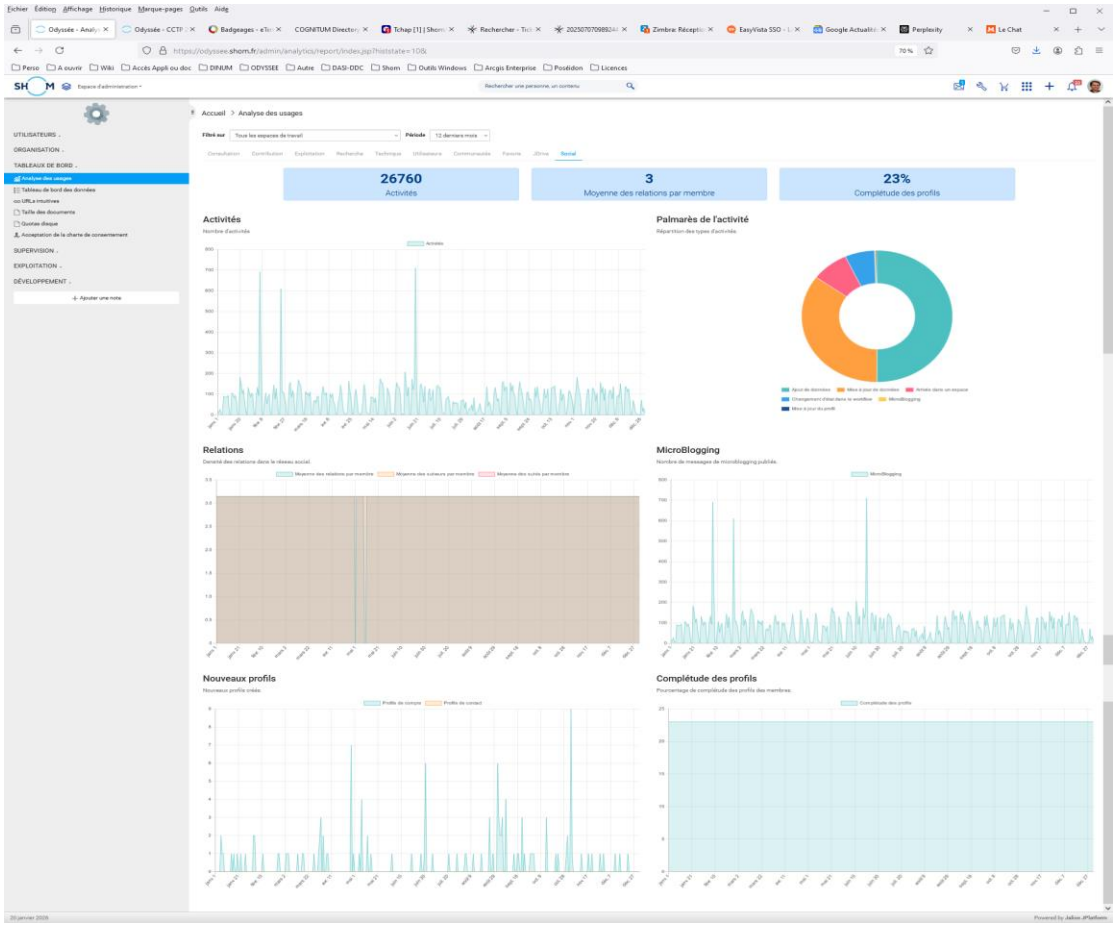


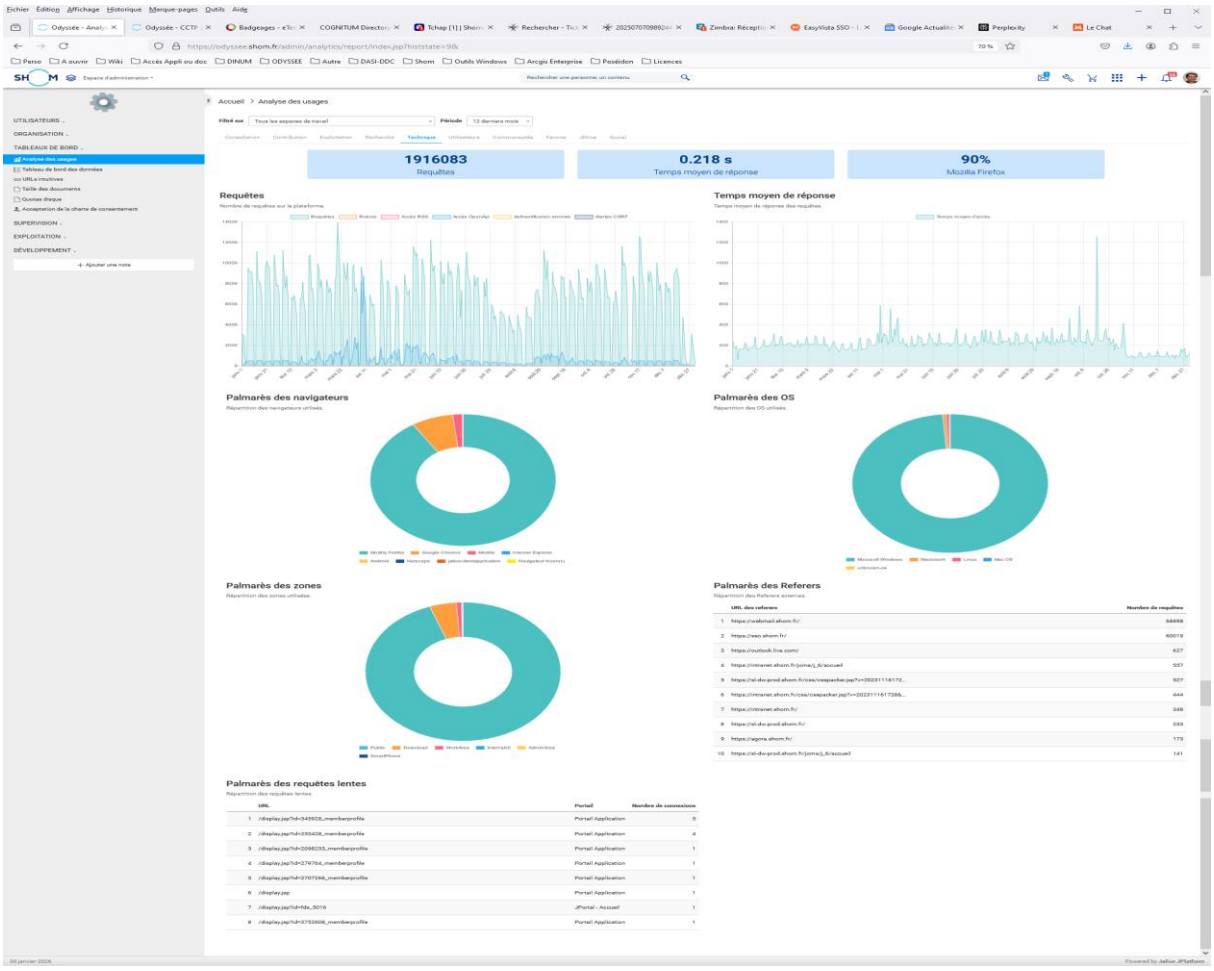


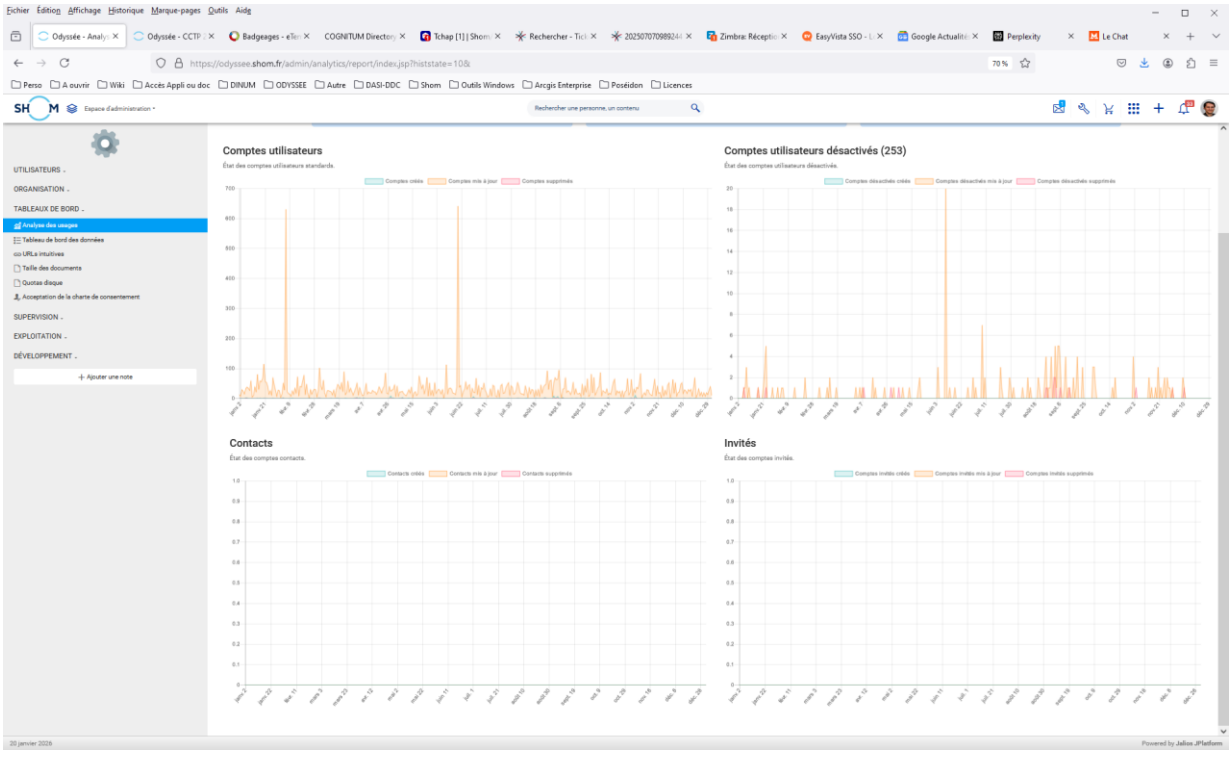

Accueil > Analyse des usages
3
Favoris par utilisateur
Nombre de favoris
Publication les plus présentes
Membres avec le plus de favoris
Favoris les plus ajoutés

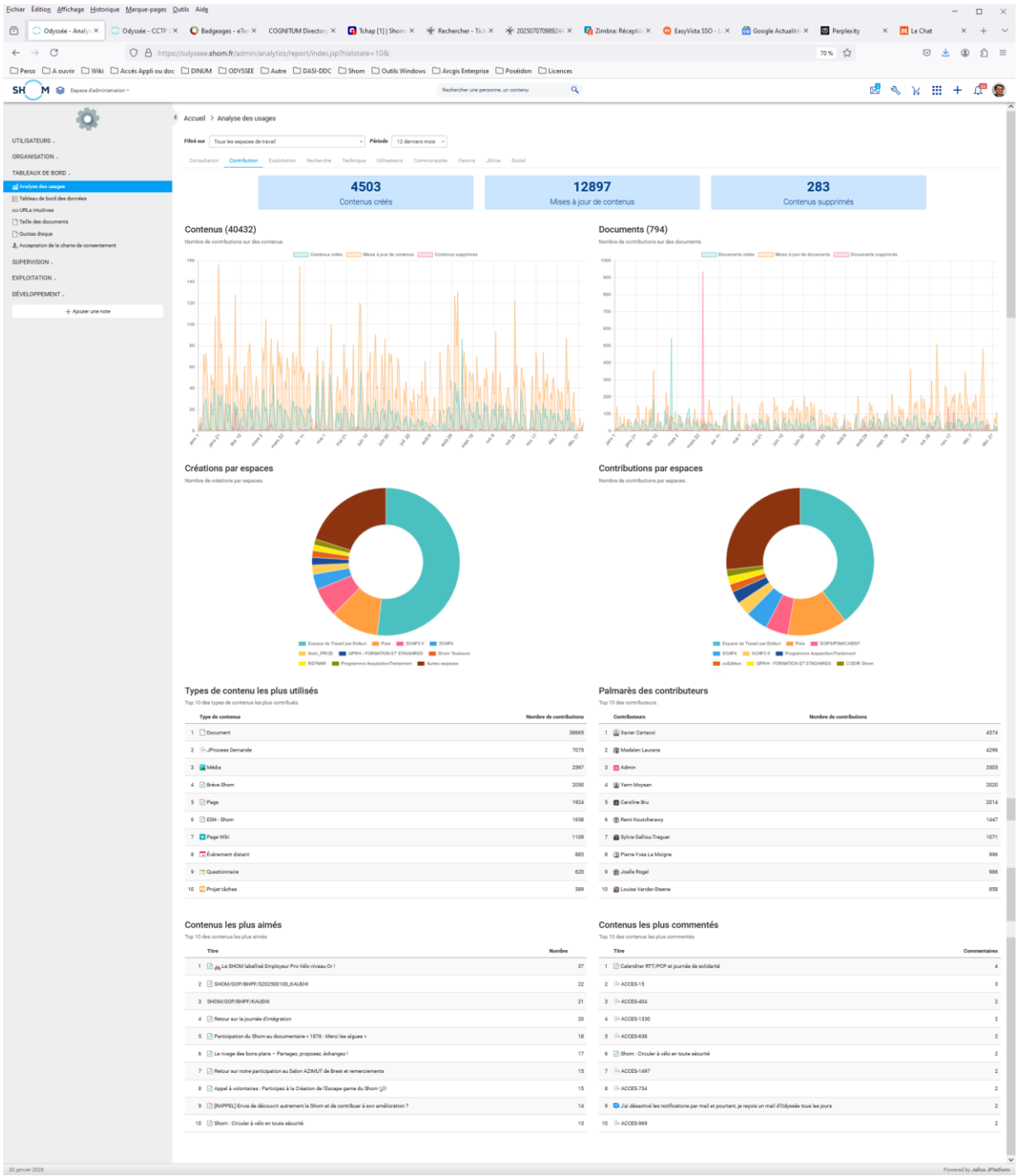

Accueil > Analyse des usages
49
JDrive (moy.)
43
Utilisateurs connectés (moy.)
25
Documents par JDrive (moy.)
2425
Activité des JDrive
JDrive
Utilisateurs connectés
Documents par JDrive
Activité des JDrive


Accueil > Analyse des usages
100843
Recherches
121147
Recherches instantanées
Recherches
Palmarès des mots clés recherchés
Palmarès des catégories utilisées

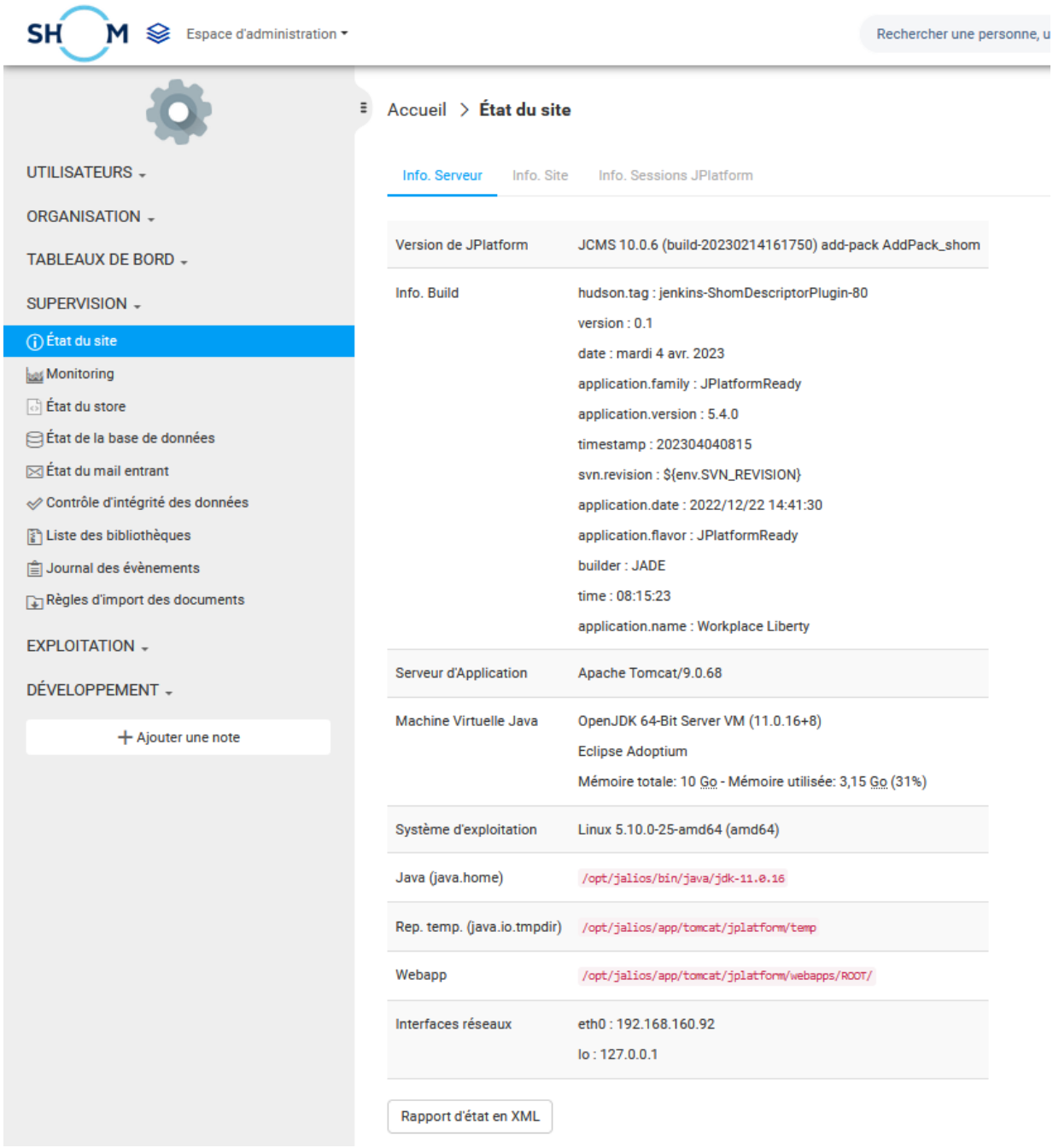

Accueil > Analyse des usages
26760
Activités
3
Moyenne des relations par membre
23%
Complétude des profils
Activités
Palmarès de l'activité
Relations
MicroBlogging
Nouveaux profils
Complétude des profils

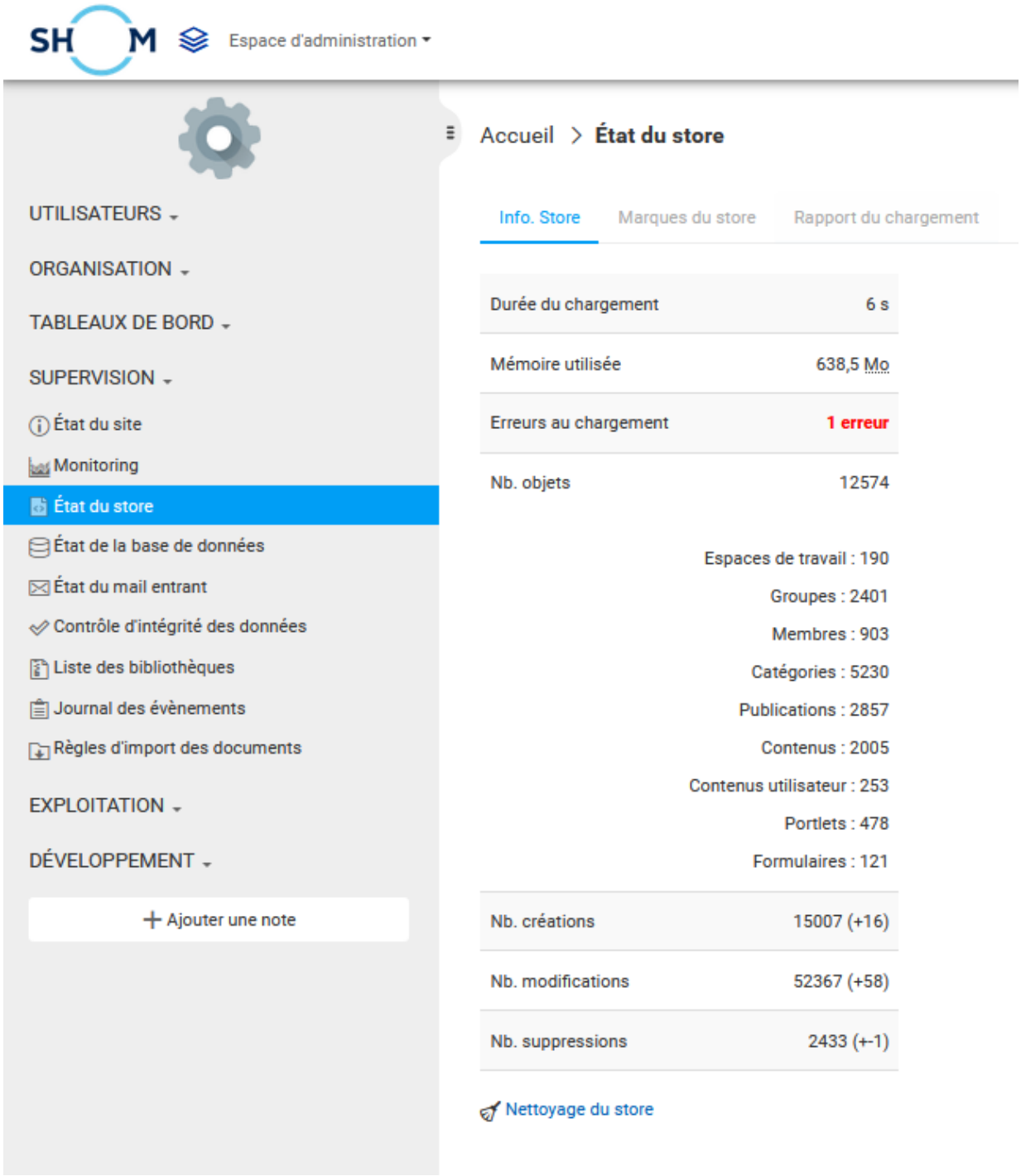

Accueil > Analyse des usages
1916083
Requêtes
0.218 s
Temps moyen de réponse
90%
Mozilla Firefox
Requêtes
Temps moyen de réponse
Palmarès des navigateurs
Palmarès des OS
Palmarès des zones
Palmarès des Referers
Palmarès des requêtes lentes

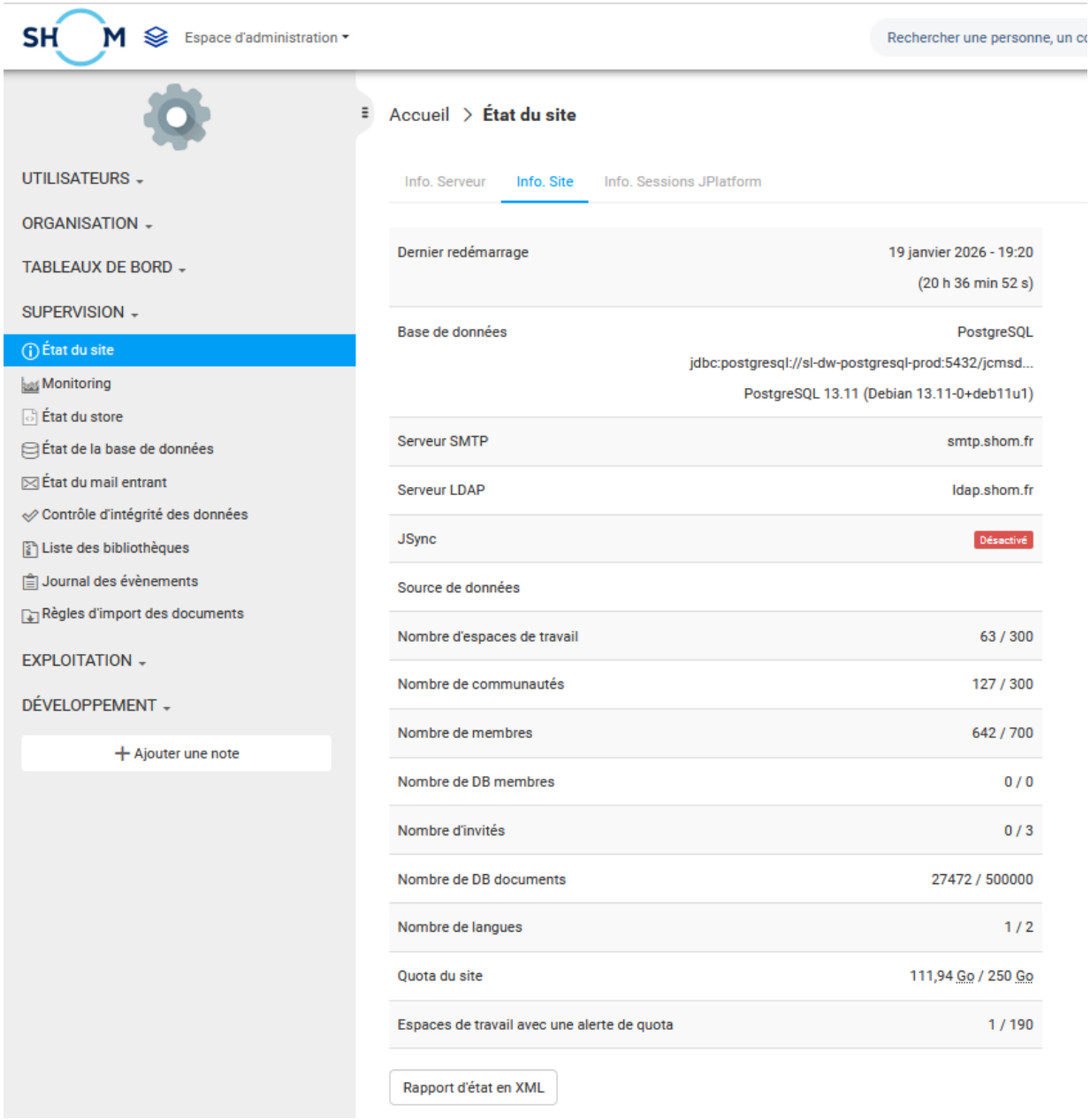

Comptes utilisateurs
Comptes utilisateurs désactivés (253)
Contacts
Invités


Accueil > Analyse des usages
4503
Contenus créés
12897
Mises à jour de contenus
283
Contenus supprimés
Contenus (40432)
Documents (794)
Créations par espaces
Contributions par espaces
Types de contenu les plus utilisés
Palmarès des contributeurs
Contenus les plus aimés
Contenus les plus commentés

12.5 ANNEXE V : INFORMATION ET VOLUMETRIE ACTUELLE SUR ODYSSEE




Espace d'administration
UTILISATEURS
ORGANISATION
TABLEAUX DE BORD
SUPERVISION
État du site
Monitoring
État du store
État de la base de données
État du mail entrant
Contrôle d'intégrité des données
Liste des bibliothèques
Journal des évènements
Règles d'import des documents
EXPLOITATION
DÉVELOPPEMENT
Ajouter une note
Accueil > État du store
Info. Store
Marques du store
Rapport du chargement
Durée du chargement 6 s
Mémoire utilisée 638,5 Mo
Erreurs au chargement 1 erreur
Nb. objets 12574
Espaces de travail : 190
Groupes : 2401
Membres : 903
Catégories : 5230
Publications : 2857
Contenus : 2005
Contenus utilisateur : 253
Portlets : 478
Formulaires : 121
Nb. créations 15007 (+16)
Nb. modifications 52367 (+58)
Nb. suppressions 2433 (+-1)
Nettoyage du store


Espace d'administration
Rechercher une personne, un co
UTILISATEURS
ORGANISATION
TABLEAUX DE BORD
SUPERVISION
État du site
Monitoring
État du store
État de la base de données
État du mail entrant
Contrôle d'intégrité des données
Liste des bibliothèques
Journal des évènements
Règles d'import des documents
EXPLOITATION
DÉVELOPPEMENT
Ajouter une note
Accueil > État du site
Info. Serveur
Info. Site
Info. Sessions JPlatform
Dernier redémarrage
19 janvier 2026 - 19:20
(20 h 36 min 52 s)
Base de données
PostgreSQL
jdbc:postgresql://sl-dw-postgresql-prod:5432/jcmsd...
PostgreSQL 13.11 (Debian 13.11-0+deb11u1)
Serveur SMTP
smtp.shom.fr
Serveur LDAP
ldap.shom.fr
JSync
Désactivé
Source de données
Nombre d'espaces de travail
63 / 300
Nombre de communautés
127 / 300
Nombre de membres
642 / 700
Nombre de DB membres
0 / 0
Nombre d'invités
0 / 3
Nombre de DB documents
27472 / 500000
Nombre de langues
1 / 2
Quota du site
111,94 Go / 250 Go
Espaces de travail avec une alerte de quota
1 / 190
Rapport d'état en XML

12.6 ANNEXE VI : CADRE DE COHÉRENCE TECHNIQUE DU S.I SHOM

Non protégé

SHOM

Procédure spécifique

Cadre de Cohérence Technique (CCT) du Shom

http://agora.shom.fr/docQual/2025/PS/PS2025-017

Etat : Approuvé

Version : Version 25-03
Dernière modification le 2025/08/21 13:35

Editeur
leo.milhade@shom.fr
Responsable du pôle interopérabilité et architectu
le 2025/08/21 13:36

Vérificateur
jeanne.lher@shom.fr
Correspondant qualité de M1 Management
le 2025/10/17 14:08

Approbateur
xavier.thuault@shom.fr
Responsable de la Division du Système d'Informatio
le 2025/10/17 16:46

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

SHOM L'océan en référence

Direction des opérations, de la production et des services
Division des Système d'information

Annexe au CCTP - Cadre de Cohérence Technique du Système d'Information du Shom

Version 25-03

Shom – 13, rue du Chatellier – CS 92803 – 29228 Brest CEDEX 2
BCRM – **Shom** – CC08 – 29240 Brest CEDEX 9
www.shom.fr

Table des matières

1 Documents applicables....3
2 terminologie. 3
3 3
4 Suivi des versions....4
5 Etats des préconisations....5
6 Périmètre et cadre d'emploi....6
7 Matériel 6
7.1 Postes clients 6
7.1.1 Configuration physique 6
7.1.2 Configuration virtuelle....7
7.2 Machines Serveurs....7
7.2.1 Caractéristiques des serveurs physiques....7
7.2.2 Configuration des serveurs virtuels....7
7.3 CalculateurS....7
7.3.1 DATARMOR....7
7.3.2 BELENOS 8
8 Logiciels 8
8.1 Systèmes d'exploitation....8
8.1.1 Microsoft Windows 8
8.1.2 Linux....8
8.1.3 Le calculateur DATARMOR 8
8.2 Bases de données 8
8.2.1 SGBD 8
8.2.2 Exigences de sécurité....9
8.2.3 Exigences de qualité 10
8.3 Le développement logiciel....11
8.3.1 Les langages....11
8.3.2 Conteneurisation 11
8.3.3 Ateliers de génie logiciel....11
8.3.4 Méthodologies....11
8.3.5 Tests unitaires....12
8.4 Navigateurs....12
8.5 Outils collaboratifs....12
8.6 Les systèmes d'information géographique....12
8.7 Intégration des logiciels....13
8.8 Mises en production....14
8.8.1 Linux....14

8.8.2 Windows....14
8.8.3 Docker....14
8.8.4 Industrialisation....15
8.8.5 Réseau du Shom 15
8.9 Proxy....15
9 stockage....15
10 Sauvegardes....15
11 archivage....16

4 SUIVI DES VERSIONS.

Version	Date	Commentaire
20-01	11/02/20	Suppression du calculateur Aquarium ; actualisation des versions logicielles
20-02	12/03/20	SSI : Spécification relative aux droits d'accès sur les données.
20-03	03/04/20	Ajout d'une précision sur l'utilisation du registre Docker.
20-04	23/04/20	Ajout des paragraphes : - 5.3.3 - Méthodologies - 5.9 - Mises en production
20-05	03/09/20	Intégration des états des préconisations. Ajout de l'introduction, de NGINX, de contraintes de sécurité Docker.
20-06	15/10/20	Correction de la version ArcGis obsolète.
21-01	27/05/21	Mise en forme ; ajout de FME Desktop et Server ; mise à jour des versions SGBD.
21-02	07/10/21	Modification de la version de l'annuaire Ldap ; précisions sur Gitlab Enterprise Edition.
21-03	11/10/21	Ajout de l'orchestrateur Kubernetes dont l'intégration est planifiée jusqu'au 01/01/2023, date à laquelle Swarm deviendra obsolète sur le SI.
21-04	09/11/21	Prise en compte remarques SG/Achat et mise en forme.
22-01	10/03/22	Mises à jours de versions logicielles (MySql, PHP, PERL, Windows serveur, Java) et matérielles (serveurs).
22-02	17/03/22	Ajout d'exigences relatives aux bases de données.
22-03	23/05/22	Ajout des informations de paramétrage du proxy
23-01	17/01/23	Modification des versions d'Oracle, Gitlab ; ajout de SambaAD, VEEAM, stockage S3, calculateur BELENOS, Jupyter. Remplacement du paragraphe d'introduction par une définition du périmètre et du cadre d'emploi. Modification des modalités Docker
24-01	08/07/24	Modification des versions des SGBD Postgresql et MariaDB Ajout du paragraphe 8.3.2 Conteneurisation Suppression de SVN et Pentaho Remplacement de Xen Libre par VMWare Ajout d'Ansible
25-01	26/02/25	Ajout de précisions concernant l'intégration : - Intégration continue et gitlab ; - Documents exigibles lors de la livraison de code source.
25-02	09/04/25	Précisions apportées concernant les versions des bases de données et langages de programmation.
25-03	15/05/25	Nouvelle version du CCT Minarm édition 2025 Mise à jour des versions de FME desktop et serveur, Global Mapper et Arcgis Pro.

5 ETATS DES PRECONISATIONS

Etat	Signification
INT	En cours d'intégration : technologie dont la mise en production est prévue.
REC	Recommandée (état par défaut des technologies présentes dans le CCT).
NR	Non recommandée : technologie présente sur le SI, dont le Shom souhaite réduire l'empreinte.
OBS	Obsolète : technologie en cours de remplacement.

6 PERIMETRE ET CADRE D'EMPLOI

Le cadre de cohérence technique [CCT] est un référentiel des choix techniques du SHOM dans le domaine des SIC. Il concerne l'infrastructure technique SIC du SHOM.

Ce référentiel doit être pris en compte par les projets de SIC et référencé au CCTP des marchés publics dont la finalité est la mise en place d'un système informatique hébergé sur le SI SHOM (directement ou à terme).

Il a pour but de faciliter l'intégration sur le SI du SHOM des solutions livrées par les titulaires des marchés publics et d'en faciliter le MCO et MCS.

Tout écart au CCT doit être argumenté et faire apparaître des gains significatifs pour le SHOM sur au moins un des aspects suivants :

- Financier,
- délais de réalisation,
- risques critiques pour le projet,
- innovation,
- performance,
- perspective à long terme,
- administration ou exploitation,
- pérennité,
- maintien en condition opérationnelle ou de sécurité.

Les écarts proposés doivent de préférence s'inscrire dans le CCT MINARM.

7 MATERIEL

La description du matériel qui suit décrit l'état du SI à la date d'émission du CCT ; il s'agit de la configuration minimale standard.

7.1 POSTES CLIENTS

7.1.1 Configuration physique

Les machines dédiées à la bureautique qui sont mises en œuvre comme postes client standards ont les caractéristiques suivantes :

- Micro-processeur : Intel core i3 ou i5 ;
- Mémoire centrale : 8 Go ;
- Disque dur : 320 Go ou SSD 256 Go ;
- Carte graphique : standard avec possibilité bi-écran.

Les machines dédiées à des traitements plus lourds et mises en œuvre comme postes client standards ont les caractéristiques suivantes :

- Micro-processeur : Intel core i7 ;
- Mémoire centrale : 16 Go ;
- Disque dur : hybride 1 To ;
- Carte graphique : NVIDIA quadro K620 2 Go.

7.1.2 Configuration virtuelle

Machine virtuelle Linux ou Windows installée sous "Virtualbox" sur une machine physique cliente Windows. Caractéristiques minimales de la VM :

- Nombre de cœur(s) : 1 ;
- Mémoire vive : 1 Go ;
- Stockage : 32 Go ;
- Add-ons Virtualbox installés.

7.2 MACHINES SERVEURS

7.2.1 Caractéristiques des serveurs physiques

Le Shom possède un parc de serveurs HP Proliant DL360(p) et DL380 Gen8, Gen9 et Gen10 dont les caractéristiques génériques sont les suivantes :

- 2 processeurs Intel Xeon bits de 2.3 à 3.1 GHz et de 10 à 18 cœurs chacun suivant les générations ;
- Mémoire vive de 256 à 1024 Go ;
- Double alimentation ;
- Système RAID 1 avec un disque spare ;
- Carte fibre 10 Gbit/s et carte cuivre 1 Gbit/s ;
- Rackable ;
- Administrable à distance.

Ces serveurs physiques sont installés en configuration hyperviseur VMWare afin d'héberger des machines virtuelles.

7.2.2 Configuration des serveurs virtuels

Le parc serveurs du Shom se compose essentiellement de machines virtuelles s'appuyant sur lelogiciel VMWARE.

Les disques de ces serveurs sont supportés par un système de stockage virtuel utilisant la technologie DATACORE.

7.3 CALCULATEURS

Le Shom a accès à deux ordinateurs puissants et dédiés aux traitements lourds : le calculateur DATARMOR et le calculateur BELENOS.

7.3.1 DATARMOR

Les capacités de calcul :

- Cluster HPC : 11088 coeurs - 426 Tflops ;
- 128 Go de RAM et 28 cœurs par nœud ;
- Cluster SMP : 240 cœurs, 5 To RAM ;
- Cluster WEB : 10 serveurs dédiés ;
- 4 GPUs.

Les capacités de stockage :

- Espace très haute performance dédié au HPC : 0,5 Po en Lustre (SCRATCH) ;
- Données de référence : 1,5 Po en Lustre (DATAREF) ;

- Données de travail : 5 Po en GPFS (DATAWORK) ;
- Home directories : 40 To en NFS (DATAHOME) ;
- Services applicatifs web ou autres : 100 To.

7.3.2 BELENOS

Ce calculateur situé à Météo-France à Toulouse présente la configuration suivante :

- 2256 nœuds de calculs comprenant chacun 128 coeurs et 256 Go de mémoire
- 48 nœuds de calculs comprenant chacun 128 coeurs et 512 Go de mémoire, dont 12 seront essentiellement destinés à des pré et/ou post-traitements. Ces derniers disposent d'interfaces réseau directement connectées au coeur de réseau MF.
- 3 nœuds comprenant chacun 128 coeurs et 512 Go de mémoire ainsi que 4 cartes GPU NvidiaV100.

8 LOGICIELS

Les dispositions relatives aux logiciels en usage au sein du Shom et encadrées par le service informatique respectent les directives éditées par la circulaire du Premier Ministre N° 5608/SG du 19 septembre 2012 relative aux ''orientations pour l'usage des logiciels libres dans l'administration''.

La description des logiciels qui suit décrit l'état du SI à la date d'émission du CCT. Il n'est pas exhaustif et décrit les logiciels susceptibles d'être mis en œuvre dans le cadre du projet. Cependant, le prestataire peut recourir à des solutions innovantes s'appuyant sur de nouveaux logiciels.

Le Shom attache un grand intérêt à la prise en compte de l'évolution des systèmes dans la prestation.

8.1 SYSTEMES D'EXPLOITATION

8.1.1 Microsoft Windows

Microsoft Windows 10 64 bits et Windows server 2022 64 bits ou ultérieur.

8.1.2 Linux

Linux Debian (dernière version majeure stable ou précédente).

8.1.3 Le calculateur DATARMOR

- OS : SLES12 SP1 ;
- Scheduler : PBS PRO 14.2.4 ;
- Compilateurs ;
- Intel 17.0.2.174 ;
- Intel 16.0.4.258 ;
- Intel 15.0.5.223 ;
- Bibliothèques : Netcdf, MKL, etc.

8.2 BASES DE DONNEES

8.2.1 SGBD

Deux types de Systèmes de Gestion de Bases de Données (SGBD) sont préconisés :

- PostgreSQL – la version préconisée est la dernière version majeure disponible (se référer à https://www.postgresql.org/support/versioning/) ;

- Dernière version Long-term stable release disponible préconisée (se référer à https://mariadb.com/kb/en/mariadb-server-release-dates/).

Le Shom souhaite privilégier les solutions libres. Les bases propriétaires ne sont plus intégrées dans les choix architecturaux, cependant le SGBD Oracle reste toléré en version 19 Standard (https://support.oracle.com/knowledge/Oracle%20Database%20Products/742060_1.html) [NR].

8.2.1.1 OS

Oracle est hébergé par des serveurs Oracle Linux Virtual Machine basée sur des versions de Red Hat Enterprise Linux Server.

PostgreSql et Mysql/Mariadb sont hébergés essentiellement par des serveurs Linux Debian.

8.2.1.2 Nommage

- Le nom de la base doit tout d'abord être descriptif et parlant pour l'application ou le projet, il ne doit surtout pas être le mot "shom".
- Le nom de base peut reprendre tout ou partie du nom du logiciel associé, mais ne doit pas contenir d'indication de version de ce logiciel.
- Il ne doit pas contenir le caractère '-' (utiliser si nécessaire le caractère souligné '_').

a. Spécificités pour Oracle

- Il convient d'utiliser un nom différent pour la base de recette, intégrant le mot test ou re7 (pour recette).

En effet, le tnsnames.ora (dispositif que le Shom utilise pour définir les noms de connexion aux bases auprès de leurs clients) n'est pas pris en compte par certains logiciels, un nom de base identique sur différents serveurs peut alors être source d'erreurs.

- Le nom d'une base est limité (par Oracle) à 8 caractères.

b. Spécificités pour PostgreSQL/MySQL

- Il faut utiliser le même nom en recette et en production, afin de pouvoir réutiliser simplement les scripts. Il n'y a pas de risque d'erreur d'accès au mauvais serveur, car des droits d'accès spécifiques à chaque client sont mis en place dans la configuration des bases.
- Le nom d'une base est limité à 13 caractères (exigence DBA).

8.2.2 Exigences de sécurité

8.2.2.1 Profil 'Propriétaire' de la base

Le profil « propriétaire » de la base doit toujours être un utilisateur spécifiquement créé, auquel les droits nécessaires seront accordés, et non pas l'administrateur général des bases. Sinon, il serait impossible d'assurer la séparation entre les différentes bases d'un même serveur. En effet, les serveurs de bases de données étant mutualisés, l'administrateur général a accès à toutes les bases qu'il sert. Aucun logiciel associé à une base ne pourra donc disposer des droits étendus de ce compte.

8.2.2.2 Comptes applicatifs

Certaines bases de données intégrées au sein de progiciels nécessitent des comptes applicatifs pour fonctionner. Ces comptes, réservés à l'usage exclusif de l'application, ne doivent pas posséder de droits d'administrateurs « dba ».

8.2.2.3 Mots de passe

Il est impératif que dans les différentes sources de programmes, aucun mot de passe ne figure.

Les appels aux modules de l'application ne doivent pas non plus faire apparaître de mots de passe dans le listage des processus de la machine.

8.2.2.4 Sauvegardes

Les sauvegardes de bases doivent pouvoir être faites « base ouverte » (à chaud), et en autonomie (uniquement au niveau du SGBD). Dans le cas contraire il est impératif de le spécifier : Ainsi, si des sauvegardes doivent être effectuées en synchronisation avec celles de l'applicatif, ou nécessitent un état particulier de celui-ci ou de la base, les procédures à utiliser doivent être documentées et fournies aux administrateurs de bases.

8.2.2.5 Schéma public

Les serveurs du Shom étant mutualisés, les schémas publics doivent être évités (comme par exemple le schéma public standard de Postgres) pour stocker des données dont l'accès devra être limité, car ce sont par défaut des schémas accessibles à tous les utilisateurs du serveur.

8.2.3 Exigences de qualité

8.2.3.1 Erreurs dans les logs

Les erreurs récurrentes produites par le logiciel dans les logs de sa base de données associée seront considérées comme des anomalies et un indice de mauvaise qualité du logiciel. Un logiciel ne pourra donc être autorisé à passer en production tant qu'il sera ainsi responsable d'erreurs dans les fichiers de log du serveur de bases de données.

8.2.3.2 Encodage et paramétrage

L'encodage et les paramètres de langues à utiliser pour toute nouvelle base de données doivent impérativement être précisés :

- Soit dans les scripts de création de base livrés ;
- Soit dans la documentation d'installation fournie.

8.2.3.3 Utilisation des rôles

L'utilisation systématique des rôles est fortement recommandée : Elle permet d'uniformiser les droits attribués aux utilisateurs et de les redéfinir dynamiquement : il suffit de changer les privilèges du rôle pour que tous les utilisateurs possédant ce rôle voient leurs privilèges changer.

8.2.3.4 Performances

Toute préconisation nécessaire au bon fonctionnement ou à l'optimisation de la base de données doit être précisée dans les scripts livrés ou la documentation fournie.

Sur Oracle, les données et les index qui s'y rapportent seront placés dans des tablespaces différents, de façon à augmenter les performances.

8.2.3.5 Informations de connexion

Toutes les informations utilisées pour contacter la base doivent être placées à un seul endroit de l'application (fichier de configuration par exemple). Cela facilite les éditions, mais aussi la gestion des différents environnements de test, ainsi que le déplacement de la base sur un autre serveur. Ces paramètres concernent, entre-autres, les informations suivantes :

- La chaîne de connexion : Nom du serveur, port, nom de la base,
- Les identifiants utilisateur
- La gestion de la sécurité (SSL, certificats, etc.)

Il est impératif que dans les différentes sources de programmes, le chemin complet, le nom de machine, et le nom d'utilisateur ne figurent pas.

Dans le cadre de la maintenance, la base doit être déplaçable sur un autre serveur en modifiant simplement la cible de l'alias de serveur utilisé dans sa chaîne de connexion, et en relançant l'application ou le progiciel associé.

Toute contrainte autre pour mener à bien le déplacement de la base est à spécifier.

8.3 LE DEVELOPPEMENT LOGICIEL

8.3.1 Les langages

Sous Linux, les langages de développement sont disponibles ou mis en place à la demande : PYTHON, JAVA, PHP, C, C++, PERL et FORTRAN.

Dans le cas du langage PYTHON, la version la plus récente possible est préconisée. Au minimum, cette version doit toujours être supportée à la fin du projet(https://devguide.python.org/versions/).

Tous les projets développés en Python devront contenir un fichier requirements.txt au format PIP ou un fichier environnement.yml (au format conda), contenant la liste des paquets utilisés et leurs versions.

Le Shom préconise l'usage de la version la plus récente du langage afin d'éviter un écart de version préjudiciable au MCO des logiciels.

Dans le cas du langage JAVA, et sous les deux OS, une version stable jusqu'à la fin du projet doit être privilégiée.

Les versions Oracle de JAVA sont à proscrire au profit de :

- Sur les postes de travail : utilisation du composant binaire AdoptOpenJDK ou Témurin **[INT]** ;
- Sur les serveurs : version binaire non Oracle basée sur OpenJDK apportée par l'OS.

De manière générale, un point d'attention est porté sur la préférence du Shom pour les logiciels libres.

8.3.2 Conteneurisation

Lorsque cela est nécessaire les développements peuvent être livrés sous forme conteneurisée via Docker . Les images Docker livrées doivent avoir été analysées par un outil type Clair ayant une base de vulnérabilités à jour et être exempt de vulnérabilité.

Sauf nécessité démontrée les bases de données n'ont pas vocation à être conteneurisées.

8.3.3 Ateliers de génie logiciel

Au sein du Shom, peu de développements sont réalisés avec des outils collaboratifs. Toutefois, le logiciel de développement intégré ECLIPSE est utilisé pour les développements en JAVA, C, C++, Python 3, PHP 8.x (https://www.php.net/downloads.php) et en PERL 5.

Les IDE PyCharm, Spyder et Jupyter Notebook sont également mis en œuvre dans le cadre des développements en langage PYTHON.

8.3.4 Méthodologies

Les méthodes de type Agile sont préconisées lorsque les développements s'y prêtent.

Dans le cadre d'un projet mené en mode agile, lorsque c'est possible, les versions intermédiaires sont intégrées au sein d'une chaine DEVOPS mise en œuvre par gitlab-ci. Dans ces cas-là un accompagnement à la mise en place de la chaine peut être nécessaire et la livraison des version intermédiaires doit se faire via git.

Si le déploiement ne peut pas être automatisé, le SI du Shom n'a pas vocation à intégrer l'ensemble des versions intermédiaires et l'opérateur doit prévoir la mise à disposition des versions « intermédiaires » issues de chaque itération sur une plate-forme externe au Shom et accessible à distance. L'ensemble des versions doit être livré au Shom, et seules celles destinées à être mises en production seront intégrées sur le SI.

8.3.5 Tests unitaires

Les tests unitaires devront passer à 100 % sur les versions destinées à être mises en production.

8.4 NAVIGATEURS

Dans le cadre de développements orientés web (clients légers), les navigateurs à privilégier sont:

- FireFox Extended Support Release (esr) ;
- Internet explorer / Edge sur le système Windows ;
- Google Chrome.

8.5 OUTILS COLLABORATIFS

Les outils collaboratifs mis en œuvre au sein du SI sont les suivants (liste non exhaustive) :

- Annuaire LDAP, OpenLdap-ltb (OpenLDAP du projet LDAP Toll Box) v2.4.59 ;
- Annuaire SambaAD v4.14.14 ;
- Système d'authentification de type SSO Web avec loadbalancer : lemonldap-ng v2.0.7 (CAS, LDAP, OpenID Connect, REST, SAML 2.0 / Shibboleth, WebID);
- Serveurs de courrier électronique : postfix (smtp) pour les serveurs, zimbra (imap, smtp, webmail) pour le site principal et postfix/roundcube (imap, smtp, webmail) pour les sites distants ;
- Serveur ftp (vsftp) pour le transfert des gros fichiers depuis et vers l'extérieur ;
- Serveur « Nextcloud » pour le partage de fichiers en interne et externe ;
- Serveurs web : Apache2 associé au CMS Drupal, Tomcat v9; NGINX (Zimbra, BigBlueButton) , NodeJS ;
- Les serveurs Apache2 sont systématiquement associés à un serveur reverse proxy ou encore à un serveur SSO en interne ;
- Serveur d'intégration continue Jenkins Version 2.x ;
- ETL (Extract, Transform, Load) : FME Desktop 2024.1et Server 2024.2 ;
- Informatique décisionnelle (ou business intelligence) : Business Object Business Intelligence 4.1.
- Progiciel de gestion intégré : SAGE X3 V7 ;
- Docker CE version 27.x intégrant l'orchestrateur/cluster Swarm ;

  L'orchestrateur Swarm est en cours de remplacement.

Des solutions de remplacement par Kubernetes sont en cours de déploiement : K3S dans un premier temps.

- Registre Docker privé utilisant Harbor 1.10 ;
- Gitlab Community Edition (privé) version 15.3.3.
- Groupe Gitlab sue la plateforme gitlab.com (70 licences utilisateurs).

8.6 LES SYSTEMES D'INFORMATION GEOGRAPHIQUE

Le Shom utilise les clients SIG suivants :

- QGIS 3.x ;

- Global Mapper v25 (licence site) ;
- ArcGis 10.7 et ArcGis Pro 3.2 (avec MCO ESRI) ;
- GeoServer .v2.x.

8.6.1.1 Edition

Les logiciels couramment utilisés dans la cadre de l'édition et de la conception de documents :

- Microsoft Office 2019 (Word - Excel - PowerPoint) ;
- draw.io ;
- LibreOffice 6.x sous Windows 10 ou Debian.

8.7 INTEGRATION DES LOGICIELS

La procédure d'intégration d'un logiciel dans le SI du Shom est la phase préliminaire à la période de recette métier. Cette procédure doit être documentée en respectant les attendus cités dans le cahier des charges.

Le logiciel sera fourni sous la forme d'un paquet regroupant tous les éléments permettant de générer le logiciel. En fonction des systèmes d'exploitation mis en œuvre et en fonction des attendus du chef de projet métier, le logiciel pourra être livré sous la forme de fichiers source (cas le plus courant) ou sous la forme de fichiers exécutables pour des cas qui doivent rester exceptionnels.

Lorsque cela est possible, le code est livré par itérations successives accompagné d'une procédure permettant la mise en place d'une intégration continue sur le serveur gitlab interne du shom. Cette procédure doit être sous la forme d'une documentation, d'un ensemble de tests et si possible d'un script d'intégration yaml compatible avec gitlab-ci.

En effet, le Shom doit détenir les droits adéquats sur les logiciels afin que la DSI puisse posséder tous les éléments nécessaires à des générations ultérieures du logiciel notamment en cas d'évolution des systèmes d'exploitation.

Hormis le respect du cahier des charges, la documentation d'installation devra impérativement énumérer les prérequis et détailler la procédure d'installation.

Dans le cas d'une livraison de code source, les schémas suivants sont attendus :
- Schéma applicatif ;
- schéma d'architecture ;
- schéma du modèle conceptuel.

L'intégration du logiciel dans le SI du Shom est effectuée par les administrateurs de la DSI du Shom avec l'assistance du titulaire. Lorsque cela est possible les administrateurs de la DSI en collaboration avec l'industriel intégreront le logiciel via une chaine DEVOPS.

Afin d'éviter les désagréments liés à une procédure d'intégration immature, le chef de projet invitera l'industriel à se rapprocher au plus tôt de la DSI afin de préparer et de planifier la phase d'installation avec un préavis suffisant par rapport à la date de livraison.

Pour mémoire, les bonnes pratiques recommandent de respecter l'indépendance entre les données et les traitements. Ce principe permet de faciliter les évolutions futures des applications. Toute modification ou refonte des données n'impacte pas ou très peu le domaine des traitements, et réciproquement.

Sauf exception dûment motivée, les applications devront fonctionner en mode « utilisateur », sans privilège particulier. Il s'agit d'appliquer le principe de moindre privilège recommandé par l'ANSSI.

En l'occurrence et sous Linux, elles ne devront pas fonctionner en utilisant le compte « root ».

8.8 MISES EN PRODUCTION

Après l'intégration, lorsque la recette est jugée conforme aux attendus, la version du logiciel a vocation à être mise en production sur le SI du Shom.

La planification des mises en production est effectuée par le service responsable (Production Informatique).

8.8.1 Linux

Sous Linux, il convient de respecter le formalisme suivant :

- S'assurer que le chemin d'installation soit paramétrable ;
- Configurer les utilitaires d'installation pour qu'ils permettent également la désinstallation du logiciel (exemple : $ make –desinstall).
- La DSI privilégie la fourniture d'un paquet d'installation avec dépendances en fonction de la distribution (.deb pour Debian, .rpm pour Redhat, etc…)

8.8.2 Windows

Sous Windows, l'installation et la désinstallation du logiciel devront être réalisables en mode silencieux et en ligne de commande.

- La DSI privilégie la fourniture d'un paquet .msi.

8.8.3 Docker

Image contenant du code propriété du Shom ou Open-Source :

- La livraison d'image n'est pas acceptée par le Shom.
- Le code est livré versionné et accompagné du docker-file permettant la génération des images docker.
- Le Shom génèrera en interne les images docker, et analysera la qualité du code via le logiciel SonarQube.

Image contenant du code propriétaire et/ou commercial :

- Les livraisons des binaires et/ou images propriétaires sont acceptées ; tout module complémentaire propriété du Shom sera livré selon les conditions ci-dessus.

Le Shom dispose d'un registre Docker privé basé sur Harbor :

- Excepté les images de base, seules les images de ce registre privé sont déployées sur l'architecture : le déploiement d'un container provenant d'internet ou de tout autre registre n'est pas autorisé ;
- Les images livrées doivent être versionnées ;
- L'exécution des containers en mode unprivileged est préférée au mode privileged pour des raisons de sécurité ;
- L'exécution des containers devra se faire sans proxy ;
- Les images fournies seront déposées dans le registre privé du Shom et ne devront présenter aucune vulnérabilité critique et un nombre limité de vulnérabilités non critiques (sous validation du RSSI) ;
- L'exécution des containers ne devra pas se faire en utilisant le compte root ;
- Le Shom impose de faire de la réassignation ou du remappage d'uid et de gid lors des exécutions de container(s) ; le host networking est ainsi interdit.
- L'ensemble des volumes utilisés ou créés doivent être dénommés.

8.8.4 Industrialisation

La SHOM expérimente des outils d'industrialisation afin de faciliter les déploiements et la gestion de configuration. L'usage d'Ansible est privilégié. La DSI garde la maîtrise de son organisation Ansible et à ce titre les industriels peuvent proposer un playbook lequel sera éventuellement modifié par l'industriel en collaboration avec la DSI.

8.8.5 Réseau du Shom

Le réseau du Shom se décompose en 3 unités logiques :

- Une unité de distribution

Cette unité permet la connexion des postes clients sur des ports POE+ à 1Gbps maximum.

Les postes clients sont connectés sur des commutateurs regroupés en unité logique "Stack" disposant de 2 liens à 10Gbps vers les cœurs de réseau.

- Une unité dénommée cœur de réseau

Cette unité est composée de 2 commutateurs 56 ports dont 32 ports sous licence 10 Gbps en redondance (actif/actif).

Ces deux équipements sont localisés dans 2 salles différentes.

- Une unité dénommée Fabric Ethernet

Cette unité permet la connexion des serveurs sur des ports 10Gbps (cuivre) et 10Gbps (Sfp+).

Les commutateurs de cette Fabric sont interconnectés par des liens fibre optique 40Gbps.

En fonction du besoin en débit, les serveurs peuvent être connectés sur plusieurs ports.

8.9 PROXY

Les accès vers l'extérieur du SI Shom doivent passer par un proxy (proxy.shom.fr:3128).

9 STOCKAGE

L'accès au stockage se fait en IP iscsi en mode bloc.

Conformément aux bonnes pratiques en matière de sécurité informatique, les droits d'accès aux fichiers et répertoires stockés doivent être définis de la manière la plus restrictive.

En l'occurrence, les droits en écriture pour les groupes indéfinis (Other) sont bannis.

Un service de stockage S3 est en cours d'intégration **[INT]**.

10 SAUVEGARDES

Les machines virtuelles du Shom sont sauvegardées par la solution et VEEAM, et les NAS par la solution libre BORGBACKUP, ainsi que Netbackup sur les bâtiments hydrographiques.

Les systèmes de fichiers sont sauvegardés une fois par jour.

Les bases de données sont sauvegardées une fois par jour. Les bases Oracle sont sauvegardées à chaud via l'utilitaire RMAN. Les bases de données PostgreSQL ou MySQL/MariaDB réalisent des exports à chaud, qui sont ensuite sauvegardés en tant que fichiers sur les systèmes de fichiers.

Certaines sauvegardes des bases de données sont effectuées à froid lorsque les applications qui les utilisent l'exigent.

11 ARCHIVAGE

Les archivages intermédiaires et historiques des données s'appuient sur la solution ArcSys version 5.1.1.1.