

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

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

Version 25-01

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

1 DOCUMENTS APPLICABLES.

Documents	
[REF 1]	Politique de Sécurité des Systèmes d'Information de l'Etat (PSSIE) du 17 juillet 2014
[REF 2]	Directive N°40/DEF/DGSIC portant sur le développement des applications informatiques et des logiciels robustes du ministère de la défense
[REF 3]	Recommandations pour la mise en œuvre de langages de développement (GU2013-042 du Référentiel Documentaire du Shom)
[REF 4]	Documentation exigible dans un développement informatique (FO2008-016 du Référentiel Documentaire du Shom)
[REF 5]	Cadre de cohérence technique des systèmes d'information et de communication du ministère des armées (CCT MINARM de la DGNUM)
[REF 6]	Circulaire du Premier Ministre N° 5608/SG du 19 septembre 2012 relative aux orientations pour l'usage des logiciels libres dans l'administration

2 TERMINOLOGIE.

Terme / Sigle	Signification
DBA	Data Base Administrator (Administrateur de Bases de Données)
DSI	Division du Système d'Information
MCO	Maintien en Condition Opérationnelle
MCS	Maintien en Condition de Sécurité
Shom	Service hydrographique et océanographique de la marine
SI	Système d'Information

3

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.

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 le logiciel 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 cœurs - 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 cœurs et 256 Go de mémoire
- 48 nœuds de calculs comprenant chacun 128 cœurs 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 cœur de réseau MF.
- 3 nœuds comprenant chacun 128 cœurs 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 édictées 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 (une par an) ;

- MySQL [NR] (version 5.6 encore présente sur le SI, mais maintenant remplacée par MariaDB – Dernière version Long-term stable release disponible préconisée).

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 [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, seule une version 3.x est à utiliser.

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, la version Java 11 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 7.x 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 chaîne DEVOPS mise en œuvre par gitlab-ci. Dans ces cas-là un accompagnement à la mise en place de la chaîne peut être nécessaire et la livraison des versions 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 : lemondap-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 et Server 2020.2 ;
- Informatique décisionnelle (ou business intelligence) : Business Object Business Intelligence 4.1.
- Progiciel de gestion intégré : SAGE X3 V7 ;
- Docker CE version 19.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.
- Groupe Gitlab sur 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 v23 (licence site) ;
- ArcGis 10.7 et ArcGis Pro 2.7 (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 chaîne 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 générera 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.