

	DOCUMENT INFORMATIF	Diffusion par : <Ne pas modifier>	<Ne pas modifier>
	Annexe technique : intégration serveurs et stockages Processus : Direction des services Numériques	Page 1 / 8	V. <Ne pas modifier>

1. OBJECTIF DU DOCUMENT

Ce document décrit les standards retenus et appliqués ainsi que l'infrastructure dans laquelle seront intégrées les solutions métiers acquises par le CHU de Nantes.

Cette annexe doit permettre aux candidats de répondre aux différentes consultations émises par le CHU de Nantes en proposant une solution technique adaptée et optimisée à l'environnement cible.

Les candidats devront se conformer aux infrastructures et standards techniques mis en place.

Le respect de cette annexe technique ne présuppose pas de l'implémentation qui devra être validée par les équipes des services numériques.

Le CHU de Nantes est certifié ISO27001 et Hébergeur de Données de Santé. Dans le cadre des intégrations, le respect de ce cadre sera exigé selon les processus en vigueur.

2. DOCUMENTS DE REFERENCE

Sans objet

3. ENVIRONNEMENTS DES MACHINES VIRTUELLES

Le CHU de Nantes assure l'intégration des services applicatifs principalement sur des environnements virtualisés ou physiques sous conditions. (CF chapitre 12 pour les serveurs physiques)

La plateforme applicative doit être agnostique de l'hyperviseur l'hébergeant.

Les attributs de performance et de capacité (vCPU, RAM, partitions, latence réseau, ...) ne doivent pas être directement dérivés d'une infrastructure physique et seront challengés par les équipes d'intégration techniques du CHU de Nantes.

Il est important de préciser qu'aujourd'hui le coût de la plateforme (CPU/RAM/STO/licences OS, middleware,...) est réintégré dans l'évaluation financière de la solution.

La résilience de la plateforme est portée par les mécanismes de plateforme virtuelle.

Toute option portant un système de tolérance de panne propre (cluster, serveur en standby...) ne sera pas retenue.

4. REGLES DE NOMMAGES DES MACHINES VIRTUELLES

Le nommage des Machines Virtuelles est à l'appréciation de l'équipe d'intégration technique en fonction des règles d'implémentation en vigueur.

5. INTEGRATION DES SERVEURS DANS LE SI

L'intégration du serveur dans le domaine Active Directory de l'établissement nécessite de respecter les règles de sécurité et de conformité imposées.

Dans le cas contraire, le serveur sera isolé du reste du SI, par des règles de pare-feu, sans possibilité de communiquer directement avec les autres composants du SI (pas d'accès direct au stockage massif par exemple). Une matrice de flux complète et précise sera exigée.

La responsabilité de la maintenance de cet actif est totalement assurée par l'éditeur ou intégrateur dans le cadre du contrat.

La mise en œuvre technique des environnements de production est réalisé à partir d'une validation technique et fonctionnelle de la plateforme de tests.

REDACTEUR(S)	VERIFICATEUR(S)	APPROBATEUR(S)	Date d'application
<Ne pas modifier>	<Ne pas modifier>	<Ne pas modifier>	<Ne pas modifier>

6. GESTION DES LICENCES ET RESSOURCES SERVEURS

Le CHU de Nantes achète des licences auprès des éditeurs de système d'exploitation et base de données, en plus des licences applicatives nécessaires au bon fonctionnement de la solution.

Le coût des licences Microsoft est en outre, déterminé en fonction du nombre de CPU affectés à une machine virtuelle, avec une facturation annuelle. Il est donc demandé d'encourager les systèmes de type Open Source au maximum.

Par conséquent, il est demandé d'affecter les ressources adaptées et de ne pas sur-dimensionner les serveurs. Dans le cas contraire, le CHU de Nantes appliquera une réduction des ressources dans la limite du bon fonctionnement des environnements et sur la base des métriques fournies pour les outils internes.

7. GESTION DES SYSTEMES D'EXPLOITATION

La production du CHU de Nantes prend en charge les systèmes d'exploitation suivants :

- Windows server, version maintenue officiellement au minimum sur les 3 prochaines années, à date de mise en production.
- Linux Ubuntu Server sous maintenance 3 ans minimum à date de mise en production.
- Oracle Linux sous maintenance 3 ans minimum à la date de mise en production : imposé pour l'hébergement d'instances Oracle.
- Red Hat Linux sous maintenance 3 ans minimum à la date de mise en production

Ces systèmes sont déployés via les modèles maintenus par le CHU de Nantes.

En cas de choix alternatif, merci de demander une instruction spécifique.

Si le l'OS imposé par l'éditeur ne peut être pris nativement en charge par la DSN, la responsabilité de la gestion de l'OS, des failles de sécurité, mises à jour incombe entièrement à l'éditeur qui s'engage à corriger cela à minima une fois par an et immédiatement sur alertes CVE critiques diffusées par les instances (CERT, ...).

Les patches de sécurité sont déployés automatiquement par des solutions de management adaptées (MS MECM, Intune, Ansible), condition impérative pour intégrer le serveur dans le domaine Active Directory de l'établissement.

D'une manière générale, il est recommandé d'utiliser les versions les plus récentes des applications, middleware, OS, outils divers afin d'éviter des opérations de migration à court terme. Ce sera une donnée importante à qualifier avec la DSN et lors de l'homologation SSL.

8. GESTION DES MIDDLEWARE ET BASES DE DONNEES

Dans le cadre d'un renforcement de la sécurité et du traitement des failles, les bonnes pratiques d'exploitation seront appliquées, avec notamment l'application des patches correctifs pour les composants déployés.

Sur le même principe que les OS, l'éditeur s'engage à maintenir la version à jour de ces composants, avec un minimum de 3 ans avant la fin de support de celui-ci.

L'installation sur les serveurs d'applications non nécessaire au bon fonctionnement de l'application est interdite et ce afin de limiter les risques et maintenance tiers des écosystèmes serveurs (exemple : pas de notepad++, de chrome, de 7-zip, ...)

8.1 Gestion des bases de données

8.1.1 Version de SGBD

Le CHU de Nantes supporte par défaut des bases de données suivantes :

- 1 [MariaDB](#), en version supportée et maintenue (sécurité en particulier) par le fournisseur de l'application.
- 2 [PostgreSQL](#), en version supportée et maintenue (sécurité en particulier) par le fournisseur de l'application.
- 3 [MySQL](#), en version supportée et maintenue (sécurité en particulier) par l'éditeur Oracle au moment de la mise en production.

- 4 Oracle, en version supportée et maintenue (sécurité en particulier) par l'éditeur Oracle au moment de la mise en production.
- 5 SQL Server, en version supportée et maintenue (sécurité en particulier) par l'éditeur Microsoft au moment de la mise en production.

Le CHU de Nantes souhaite limiter au maximum le déploiement de nouvelles instances de Microsoft SQL Server, pour des raisons de coûts de licences imposées. Les conditions seront à évaluer au cas par cas.

Tout autre type de base de données proposées doit faire l'objet d'un échange afin de définir les limites de responsabilités de maintenance et d'exploitabilité de ce qui serait imposé et hors du périmètre de compétences du CHU de Nantes.

8.1.2 *Best practices à respecter pour l'installation d'instances de bases de données*

- Le fournisseur s'engage à fournir le nom de l'instance et l'encodage nécessaire. Aucun accès administrateur complet du serveur de base de données ne sera autorisé. Les droits administrateurs sont réduits aux instances de bases seules, via un compte de service spécifique qui sera fourni.
- Le CHU de Nantes met à disposition un serveur avec une organisation de système de fichier à respecter, afin de séparer, logs, fichiers de bases, tempdb, traces, audits, sources, ...
- **La sauvegarde des bases de données sera réalisée par script vers un stockage de type S3.** Les procédures spécifiques seront à fournir et à valider conjointement. La conservation de « dumps » en local sur les serveurs n'est pas autorisé.
- la DSNT dispose de toute une documentation technique pour l'installation de divers base de données (Oracle, SQL serveur, [MariaDB](#) ...). Lors de l'implémentation, il faudra sous la validation du responsable technique, les respecter (répertoires de stockages des données, des scripts et requêtes divers).
- Même si votre base de données n'est pas connue par la DSNT mais que vous en assurez la maintenance et l'exploitation, comme les système d'exploitation, nous exigeons des bases de données dans une version supportée et maintenue par l'éditeur concerné.
- L'application ne doit pas fonctionner avec un compte système de la base, comme SYS ou SA. Les mots de passes de ces comptes peuvent être modifiés à tout moment.

8.1.3 *Responsabilités de la maintenance des bases de données*

Le CHU de Nantes est responsable de fournir l'environnement et les ressources nécessaires au bon fonctionnement et est propriétaires des données de la base.

Le fournisseur est responsable des performances de sa base de données, par l'optimisation des index, requêtes, schémas, ...

8.2 Les middleware pris en charge par défaut :

8.2.1 *Serveurs Web*

- Apache Web Server, en version supportée et maintenue (sécurité en particulier) par le fournisseur de l'application.
- [NginX](#), en version supportée et maintenue (sécurité en particulier) par le fournisseur de l'application.
- Internet Information Server (IIS), en version supportée et maintenue par Microsoft.

Un système de rotation de logs sera impérativement mis en place.

8.2.2 *Clients SGBD*

Tout client déployé doit être maintenu par l'éditeur. L'utilisation de client obsolète type Oracle 11 ou 12 par exemple est interdit.

De plus, l'installation de logiciels d'interrogations SQL est limité à SQL Developer et Microsoft Management Studio. Les versions panda, SQLite, ... sont interdites et seront supprimées dans le cadre du suivi de conformité des serveurs.

8.2.3 Autres composants middleware

Tout composant non cité dans ce document doit faire l'objet d'un échange avec le CHU de Nantes et doit être remonté au plus tôt dans la phase d'analyse, en amont de l'intégration.

9. GESTION DES INTERFACES

Dans le cadre de l'interopérabilité des applications, des interfaces peuvent être mise en place et devront s'appuyer sur les recommandations spécifiques de l'équipe INTER-OP du CHU de Nantes.

Ces interfaces seront à référencer dans la matrice de flux et fonctionneront sur des protocoles standards type FTP(s) ou socket.

Les fichiers seront à déposer dans des répertoires spécifiques dédiés et feront l'objet d'une purge régulière qui sera à définir avec les équipes d'intégration.

10. GESTION DES ENVIRONNEMENTS DE TYPE CONTENUS

Le CHU de Nantes ne dispose pas de plateforme d'hébergement de conteneurs de type Kubernetes.

Cependant, des ressources de type « Docker » peuvent être prise en charge, sous réserve de respecter les pré-requis d'intégration spécifiques du CHU de Nantes dont :

- Les conteneurs Docker ne doivent pas fonctionner avec des privilèges de type « root ». Séparation des droits utilisateurs : administrateur système, administrateur docker, utilisateur remap
- Les conteneurs sont connectés sur un réseau interne spécifique autre que celui par défaut défini à l'installation du moteur : plage ip imposée 172.30.0.0/16
- Externalisation des logs
- Pas de base de données conteneurisée.
- Les images « custom éditeur », sont considérées comme non conformes et sous l'entière responsabilité l'éditeur et doivent être identifiées et documentées en amont du projet.
- Conservation de 2 versions d'images au maximum en local sur le serveur.
- Pas de « secret » en clair dans les fichiers de configuration.
- Système de fichier défini avec « /app » et « /app-logs »

La sécurité de ce type d'environnement conteneurisé est à gérer « by design ».

Le CHU de Nantes ne propose pas à ce jour de répertoire d'images de type Gitlab.

L'intégration de ce type d'environnement sera soumis à la validation des référents techniques conformément aux spécifications internes du CHU de Nantes.

11. GESTION DES CERTIFICATS

Le CHU de Nantes dispose d'une infrastructure PKI interne en capacité de délivrer des certificats adaptés pour la sécurisation des services web par exemple.

Le fournisseur précisera en amont de l'intégration tous les certificats nécessaires au bon fonctionnement de son application, qu'ils soient internes, auto-signés ou à créer par le CHU.

La documentation fournie précisera l'impact de l'expiration de chaque certificat sur la solution par niveau de criticité, ainsi que les modalités de renouvellement si spécifiques.

L'éditeur devra proposer une solution de gestion des certificats à déployer dans des équipements (caméras, biomed, ...) et expliciter l'impact sur l'exploitation (ajout, suppression, remplacement) : certificat propre éditeur, certificat auto-signé, ...

12. GESTION DU STOCKAGE DES MACHINES VIRTUELLES

Le CHU de Nantes utilise massivement les architectures virtualisées, pour la plupart des infrastructures applicatives. Cela implique que le stockage est également et en général traité "en mode bloc" pour tout ce qui concerne l'exécution des machines virtuelles ou containers.

Le fournisseur est tenu de fournir le niveau de service générique suivant pour chaque type de donnée générée :

- SYSTEM : volumes systèmes des environnements applicatifs (Typiquement root Linux et C: Windows)
- BDD : volumes de type base de données, logfiles, archivlogs, traces etc. ... / orienté performance, mode block
- DATA : volumes de type non structurés, stockage massif / priorité au volume consommé, pas d'engagement de performance, mode file ou objet
- ARC : volume de type non structurés ou structuré mais stocké à des fins d'archivage patrimonial ou légal / priorité au volume, par exemple archives PACS, WORM etc., mode file ou objet
- AUTRE : volume spécifique, à discuter et instruire avec la DSNT

13. HEBERGEMENT DE VOLUMES DE STOCKAGE MASSIF STRUCTURES ET NON STRUCTURES

En dehors des use-cases traditionnels couverts par les précédents chapitres, certaines applications réclamant du stockage massif (Limite dynamique mais supérieure quoi qu'il en soit au To) doivent faire l'objet d'un traitement particulier et notamment être instruit par le service architecture pour évaluer l'opportunité d'un hébergement sur des supports adaptés à ce type de donnée.

Il faut en particulier être vigilant quant aux données catégorisées comme DATA ou ARC.

Le fournisseur devra proposer des alternatives au stockage classique direct sur des volumes virtuels intégrés, typiquement CIFS, NFS et même privilégier le protocole S3.

L'accès direct à un volume de stockage massif depuis un serveur non maîtrisé par le CHU de Nantes et donc isolé en mode « Untrusted » est interdit. Il est imposé de passer par un équipement « rebond », sécurisé et conforme aux règles de sécurité du CHU de Nantes.

14. GESTION DE LA MATRICE DE FLUX

Chaque environnement applicatif doit faire l'objet de la formalisation d'une matrice de flux et de schémas technique associés, fournis **AVANT** le déploiement du moindre composant.

Cette matrice de flux doit être COMPLETE (qu'elle prenne en compte TOUS les flux applicatifs et techniques nécessaire à son fonctionnement) et notamment décrire précisément les **sources**, **destinations**, sens de connexion ainsi que les **protocoles/port IP utilisés**.

Cette matrice de flux sera intégrée dans les livrables de la solution.

15. HEBERGEMENT DE SERVEURS PHYSIQUES

Par défaut, toute application qui nécessite la mise en place de ressources physiques en salle Datacenter, doit faire l'objet d'une demande formelle à instruire avec les équipes d'architecture technique.

Les questions de continuité de services, réplication, maintenances des équipements après garantie seront notamment à valider en amont du déploiement.

16. COMPOSANTS PHYSIQUES SPECIFIQUES A L'APPLICATION (DONGLES NOTAMMENT)

Par défaut, les dongles et autres éléments physiques qui réclament une connexion physique à l'un des composants logiciels de l'application sont **PROHIBES**.

En cas de difficulté, le fournisseur devra proposer une solution alternatives LOGICIELLE (service de licences de type flex par exemple). Si ces composants sont indispensables, ils devront, avant toute mise en œuvre être discutés et instruits par le service architecture au préalable.

17. PRINCIPES DE SUPERVISION

Le CHU de Nantes dispose d'une supervision de ses équipements utilisant les protocoles standards connus : SNMP, WMI, API, scripts.

Le fournisseur doit être en capacité de fournir les éléments à superviser, de les hiérarchiser **ET** de définir les composants **bloquants** ou **dégradants** de son infrastructure afin de construire une météo applicative à destination des utilisateurs ou responsables fonctionnels.

Chaque intégration de sonde de supervision s'accompagne obligatoirement d'une action à réaliser pour résoudre l'alerte remontée. En l'absence de solution, la sonde ne sera pas intégrée.

18. PRINCIPES DE SAUVEGARDE

La solution sera protégée via la mise en place de la politique de sauvegarde de l'établissement.

Les principales caractéristiques sont :

- Sauvegarde quotidienne.
- Backup quotidien des bases de données avec gestion des journaux de transaction.

Le CHU de Nantes assure cette mission de sauvegarde selon ses pré-requis, sur la base de ses scripts et procédures. Aucune sauvegarde sur les disques locaux ne sera acceptée.

19. PRINCIPES D'INTEGRATION DE LA SECURITE.

La sécurité fait l'objet d'une attention forte par les équipes du CHU de Nantes. Le principe de moindre privilèges est à appliquer.

19.1 Accès sécurisé par double facteur sur les services CHU NANTES

Le CHU NANTES doit respecter la réglementation et les évolutions associées sur la sécurisation des accès. L'accès à des services fournis par le CHU NANTES depuis Internet impose une authentification de forte multi-facteurs obligatoire : accès télétravail, accès à des outils via application smartphone, accès via portail web.

Le non respect des principes de sécurité exigés par le CHU de Nantes imposera un refus de déploiement ou une intégration en mode isolé « Untrusted » des composants concernés, avec une redéfinition des responsabilités entre chaque partie.

19.2 Accès sécurisé par double facteur sur les applications SAAS

L'utilisation de service applicatif en mode SAAS nécessite également la mise en place d'une authentification double facteur, à minima pour les accès de type administrateur.

Un référentiel des habilitations est à maintenir et sera contrôlé régulièrement, en lien avec le RSSI.

19.3 Agents déployés

Les systèmes par défaut sont implémentés avec à minima les composants suivants :

- EDR crowdstrike, aucune exclusion tolérée
- Client MECM (Microsoft)

Si les pré-requis sont respectés, les OS Microsoft sont intégrés dans un active directory et les stratégies de groupes (GPO) génériques de l'établissement lui seront appliquées.

19.4 Politique de gestion des comptes à privilèges

Les applications fonctionnant avec un compte administrateur local, ou avec une session de type « autologon » sont interdites.

Dans le cadre d'un composant intégré au SI du CHU de Nantes :

- Les comptes administrateur local des serveurs Windows sont gérés à travers Microsoft LAPS, avec une rotation des mots de passe imposée.
- Les autres administrateurs locaux ont une politique d'accès (PSO) spécifiques, avec un changement de mot de passe imposé annuellement et à minima.

- Sur les systèmes linux, le compte root ne pourra être utilisé pour l'installation. Des clés SSH spécifiques seront intégrées, avec un niveau de privilège à définir.

L'ajout d'administrateurs locaux et à limiter au maximum, principe du moindre privilège. L'application doit pouvoir fonctionner sans nécessiter de privilèges administrateur. Dans le cas contraire, des délégations seront à définir.

Les mots de passes seront conformes à la PSSI du CHU de Nantes (ex : 25 caractères, complexité forte).

19.5 Politique des comptes de services

Les comptes de services sont limités à leur rôle uniquement et seront du type Microsoft gMSA principalement sur les serveurs Windows.

Pour les serveurs linux, un utilisateur spécifique non « root » devra être ajouté.

Les mots de passes seront conformes à la PSSI du CHU de Nantes (ex : 25 caractères, complexité forte)

19.6 Politique de mise à jour des patchs de sécurité

L'application des mises à jour de sécurité des systèmes serveurs et middleware est automatisée.

Tous les serveurs sont redémarrés par défaut au moins une fois par semaine. La séquence d'arrêt/relance, avec relance automatique de l'application sera spécifiée dans les livrables d'exploitation fourni par l'éditeur.

19.7 Logs et traçabilité

La solution doit pouvoir être connectée à une infrastructure SIEM afin d'assurer la traçabilité des événements sur la base de la politique définie par le CHU de Nantes.

19.8 Accès distants aux serveurs

Le CHU de Nantes a mis en œuvre une politique d'accès aux serveurs conforme aux recommandations actuelles, sur la base de « Tiering », avec des comptes à privilèges dédiés et nominatifs.

L'accès direct des utilisateurs MOA en mode « connexion à distance » est interdit.

Consulter l'annexe relative à la gestion des accès fournisseurs pour plus de détails.

19.9 Gestion des profils locaux

Le CHU de Nantes assure la conformité des serveurs et intègre dans ses politiques la suppression automatique des profils locaux lors des redémarrages des serveurs. Aussi, il est demandé de ne rien stocker dans ces profils mais d'utiliser un répertoire spécifique sur un volume de type « datas ».

19.10 Gestion des serveurs en DMZ

Les serveurs en DMZ, accessibles depuis le réseau Internet sont sources de risques et doivent être limités en nombre. Il est demandé de ne pas exposer de serveurs Microsoft Windows dans cette zone.

Une intégration spécifique est à réaliser et doit être prise en compte dans la solution :

- 3 cartes réseaux pour la rupture de flux (IN, OUT, OOB)
- Pas de domaine Active Directory, comptes locaux, soumis aux règles de sécurité du CHUN.
- Déploiement d'un agent EDR CrowdStrike
- Tests de conformité aux outils de cyber-sécurité validés avant ouverture du service (I-Trust, ...)

Les serveurs et composants déployés doivent obligatoirement être maintenus à jour. Le système d'exploitation sera automatiquement mis à jour directement auprès des serveurs éditeurs.

Les mises à jour applicatives doivent inclure obligatoirement une révision complète des composants installés, à minima une fois par an.

Les accès à distance sur ces serveurs seront réalisés à partir d'une station de rebond spécifique. Ces accès seront activés/désactivés à la demande, motivés et tracés.

19.11 Gestion des partages Windows

Il est demandé de respecter les bonnes pratiques de sécurité en cas d'utilisation de partage de dossiers, en sécurisant les accès via les ACL et le partage lui-même. L'utilisation de groupe AD est recommandé afin de faciliter l'exploitation.

L'accès à des répertoires via les partages administratifs du système (ex : C\$, ou D\$) sont interdits.

L'exécution d'application depuis des partages réseau est interdite.

19.12 Gestion des scripts

Les scripts déployés sur les serveurs sont à référencer et devront à minima :

- Etre versionnés, documentés, déposés dans le Gitlab du CHUN.
- Ne disposer d'aucun mot de passe en clair
- Etre conforme aux règles de l'art en terme de développement
- Pourraient être intégrés dans un Gitlab

20. LIVRABLES

Le fournisseur devra proposer un livrable technique reprenant :

- Procédure d'installation
- Schéma d'architecture technique ET fonctionnel
- Matrice de flux
- Procédure d'arrêt/relance