

	DOCUMENT INFORMATIF	Diffusion par : PILNH - DSN	0085-DI-218
	Annexe technique - architecture serveurs et stockage	Page 1 / 3	V. 01

Processus : INF-CHU-Gestion des Services Numériques

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.

2. DOCUMENTS DE REFERENCE

Sans objet

3. ENVIRONNEMENTS DES MACHINES VIRTUELLES

Le CHU de Nantes travaille majoritairement avec des environnements applicatifs virtualisés. Cela signifie que, **PAR DEFAUT**, une application est assujettie à un certain nombre de règles en matière d'installation, de fonctionnement et d'environnement d'exécution. Chaque élément applicatif doit absolument respecter un certain nombre de bonnes pratiques avant d'être éligible à une mise en production.

TEST, PROD

Sauf cas particulier, à chaque environnement de production doit correspondre un environnement de TEST et qualification équivalent en terme de couverture fonctionnelle. Pour cela, la plupart des systèmes techniques sur lequel s'appuient les environnements de production existent aussi sous la forme d'environnement de TEST. C'est le cas en particulier pour :

- NSX-T et ses fonctions de micro-segmentation
- Les machines virtuelles
- La volumétrie primaire

4. REGLES DE NOMMAGES DES MACHINES VIRTUELLES

Quelle que soit la VM provisionnée elle doit respecter les règles de nommages suivantes :

- Nom jusqu'à 16 caractère
- Aucun caractère accentué, ni majuscule : seules les caractères minuscules sont autorisés
- Le Tired, l'Under score et le point
- Nommage général : <établissement ght>-<nom de l'appli> <partie applicative> <environnement> <numéro d'ordre>

Exemple : pacsbddprd1, easyvista-bdd-prd1, easly-sqltst1, chgd-citrix-sql01

5. PUISSANCES DES MACHINES VIRTUELLES

Chaque machine virtuelle faisant l'objet d'une livraison **NE DOIT PAS ETRE** directement dérivé d'une infrastructure physique historique. Le niveau de performance souhaité (vCPU, mémoire, latence réseau et stockage, notamment) **doit faire l'objet** d'une discussion préalable avec les équipe de la DSNT ainsi qu'une stratégie **ADAPTEE** au cas du CHU de Nantes, associé à des justificatifs précis (abaques, compte-rendu de simulateurs de charge).

En effet, la stratégie utilisée au CHU de Nantes est la suivante : avec l'aide du fournisseur, nous adoptons les besoins de performance **minimum** a priori. Ensuite seulement, après la mise en production et en fonction des besoins réels constatés, avec graphiques et reports l'appui, nous faisons évoluer le dimensionnement des environnements.

REDACTEUR(S)	VERIFICATEUR(S)	APPROBATEUR(S)	Date d'application
Eric MALEVIALLE (Responsable - PILNH \Services Numériques\Infrastructures)	Pierrick MARTIN (Coordonnateur qualité - PILNH \Services Numériques)	<Ne pas modifier>	30/05/2023

6. GESTION DES SYSTEMES D'EXPLOITATION

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

- Windows server, version maintenu officiellement au minimum sur les 3 prochaine 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 : recommandé pour l'hébergement d'instances Oracle.

En cas de spécificité, merci de demander une instruction à l'équipe Architecture.

Dans ce cas, 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.

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 DSNT et lors de l'homologation SSI.

7. 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.

Le CHU de Nantes supporte l'ensemble des bases de données suivants :

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

7.1 Best practices à respecter pour l'installation d'instances de bases de données :

- Si votre application fait un usage spécifique de DUMPs de base de donnée (exports complets et cohérents) et que la base de données en question est prise en charge nativement par notre outil de Sauvegarde institutionnel, l'utilisation de ces dumps n'est pas autorisée par défaut et doit être exclue des volumes disques demandés. Parlez de ce sujet spécifique à la DSNT lors de l'intégration de votre workload. Nous pouvons mettre en place un "espace de manœuvre" non sauvegardé mais sécurisé pour stocker temporairement vos exports de base
- 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, dans la mesure du possible et avec l'aide 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.

7.2 Les middleware pris en charge par défaut :

- 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.

8. GESTION DU STOCKAGE DES MACHINES VIRTUELLES

Le CHU de Nantes utilise massivement l'hyper-convergence (HCI) pour la plupart des infrastructures applicatives. Cela implique que le stockage est également et en général traité "en 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, archive logs, 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

9. 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 à quelques 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 dans la mesure du possible des alternatives au stockage classique direct sur des volumes virtuels intégrés, typiquement CIFS, NFS voir même S3 si possible.

10. GESTION DE LA MATRICE DE FLUX

Chaque environnement applicatif doit faire l'objet de la formalisation d'une matrice de flux et de schémas techniques associés. Le formalisme n'est pas imposé pour le moment, nonobstant, il faut que cette matrice de flux soit COMPLETE (qu'elle prenne en compte TOUS les flux applicatifs et techniques nécessaires à son fonctionnement) et notamment décrire précisément les sources, destinations, sens de connexion ainsi que les protocoles/port IP utilisés. Cette matrice est un prérequis à toute mise en production validée. De même, en général, les schémas doivent être intégrés tôt ou tard aux fiches Wiki décrivant le fonctionnement de l'application. Le fournisseur doit être capable de fournir ces documentations et constituer qu'il maîtrise son application tant au niveau sécurité qu'au niveau réseau.

11. HEBERGEMENT DE SERVEURS PHYSIQUES

Par défaut, toute application qui nécessite la mise en place de ressources physiques, doit faire l'objet d'une demande formelle à instruire par et avec l'équipe exploitation. Le fait que ces ressources soient physiques **NE DEDOUANE EN AUCUN CAS** le fournisseur de la fourniture d'une matrice de flux adaptée, au même titre qu'une machine virtuelle plus traditionnelle.

12. 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 alternative 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.