


| | | | |
|---|---|--------------------------------|-------------|
|  | DOCUMENT INFORMATIF | Diffusion par : PILNH - DSN | 0085-DI-217 |
| | Annexe technique - exploitation de la solution | Page 1 / 4 | V. 01 |

Processus : INF-CHU-Gestion des Services Numériques

1. OBJECTIF DU DOCUMENT

Ce document décrit les principes et obligations liés à l'exploitation des solutions mises en œuvre au 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.

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. DOCUMENTATION ET CONTRAT DE MAINTENANCE

Le fournisseur s'engage à fournir toute la documentation nécessaire et réaliser le transfert de compétences vers le service exploitation de la DSNT, en lien avec le chef de projet (schéma technique, schéma logique, etc.)

Les contrats de support seront précisés et vérifiés régulièrement.

Les plages de maintenance de l'application seront définies et les procédures associées fournies par le fournisseur.

Le périmètre d'intervention de l'équipe d'Exploitation sera formalisé et explicité.

4. SUPERVISION

4.1 Principe

Le CHU de Nantes assure la supervision des systèmes dont il a la responsabilité du maintien en condition opérationnelle.

Les équipements proposés doivent supporter les protocoles de supervision standard :

- snmp v3
- wmi
- api

Un outil supplémentaire peut-être déployé pour améliorer les indicateurs, de type NSCLient.

4.2 Intégration

Par défaut, le système est supervisé avec des indicateurs standard :

- Disque
- Processeur
- Mémoire
- Réseau (interface)

| 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 |

Des compléments peuvent être demandés du type :

- Base de données (Oracle, sql, ...)
- Services Windows
- Processus linux
- Serveurs web
- Age de fichiers,
- archive logs
- ...

Un catalogue des possibilités est disponible auprès de la DSNT.

L'éditeur s'engage à fournir un schéma infrastructure physique et/ou logique afin de l'intégrer aux tableaux de bords de la supervision.

L'éditeur s'engage à affiner avec l'aide du CHU de Nantes les seuils d'alertes, disponibilité et performances relatifs aux composants déployés.

4.3 Cas particulier et exclusions

Dans le cas où l'éditeur est entièrement responsable de la gestion des bases de données ou système, une supervision minimale est mise en œuvre mais ne pourra dans ce cas être précise et servir à des fins de diagnostics lors des incidents.

5. SAUVEGARDES

Par défaut, toutes les données produites dans le cadre de l'activité doivent être sauvegardées conformément à la Politique Technique de Sécurité relative aux Sauvegardes.

Différents types de sauvegardes sont mis en œuvre :

- Vm
- Agent
- Nas

Le CHU de Nantes s'appuie sur la solution Veeam Backup pour la sauvegarde de ses données.

5.1 Type agent

La solution Veeam met à disposition un agent Oracle et SQL Server qui permet d'assurer la sauvegarde et l'intégrité des bases de données. Cette solution est à privilégier.

Un agent de type Fichiers existe également pour sauvegarder des volumes sans traiter l'ensemble du système.

5.2 Type export/dump

Les bases de données non couvertes par un agent Veeam pour la sauvegarde doivent être traitées différemment (postgresql, mysql, mariadb, ...)

Un export en mode fichier de la base est à réaliser sur un partage NFS ou CIFS spécifique, en dehors du système.

Aucun backup en local ne sera accepté. Celui-ci est obligatoirement déporté le cas échéant.

5.3 Type NAS

Il s'agit d'un agent qui permet de faire de la sauvegarde en mode fichier sur un système physique ou virtuel.

6. SECURITE

6.1 Mise à jour OS

En standard, pour accéder au réseau "trusted" et sécurisé, les mises à jour système sont à prérequis pour l'intégration de la solution sur le réseau du CHU de Nantes. Elles sont pilotées soit par un système de type Microsoft WSUS ou bien par des serveurs miroirs linux.

Dans le cas où la solution ne supporte pas ces mises à jour, le système sera isolé dans un réseau dédié dit "untrusted" avec des fonctionnalités et des accès au système d'information limités.

6.2 Mise à jour des composants

Le fournisseur s'engage à informer le CHU de Nantes des mises à jour disponibles pour les composants déployés (serveur web, base de données, framework, ...). Celles -ci peuvent être déployées suivant accord soit par le CHU soit par le fournisseur.

Les failles de sécurité de ces composants doivent être prises en compte et faire l'objet d'un plan d'actions spécifiques pour leurs remédiations.

Aucun composant obsolète ne sera accepté.

6.3 Antivirus

Le CHU s'appuie sur les solutions Trend Micro afin d'assurer la sécurité des composants déployés.

Les solutions retenues doivent être compatibles avec cet outil. Les exceptions potentielles seront à définir et limitées au minimum.

Dans le cas où la solution ne supporte pas la contrainte d'un antivirus, elle sera déployée en réseau "untrusted" et donc avec des limitations.

6.4 Matériels virtuels

Dans le cas de serveurs virtualisés, la mise à jour régulières des vmtools est du matériel virtuel est impératif. L'application doit être en capacité de fonctionner avec les versions supportées par l'éditeur VMware.

6.5 Audits

Le CHU de Nantes est amené à pratiquer des audits internes et/ou externes dans le cadre de ses certifications : sécurité, habilitations, obsolescence.

Le fournisseur s'engage à prendre en compte les conclusions de ces audits au travers d'un plan d'actions spécifique.

7. INTEGRATIONS ET PRE-REQUIS

7.1 Système et composants middleware

Le CHU de Nantes applique ses procédures pour la gestion des OS et des arborescences. Le fournisseur s'engage à respecter les prérequis fournis.

L'installation de l'application sera effectuée dans des répertoires dédiés et identifiés dans la documentation.

Les logs seront stockés sur un volume dédié autre que le disque système.

Le déploiement de base de données respectera l'organisation établie (Logs, bases, application, temp, ...)

7.2 Comptes et délégations de droits

La solution proposée doit impérativement pouvoir fonctionner sans avoir à ouvrir une session de type autologon Windows.

Des habilitations dédiées peuvent être étudiées, mais le principe du moindre privilège doit s'appliquer de facto.

La création de compte de type "admin local" est à proscrire.

Le lancement ou la configuration du compte de connexion fournisseur à l'intérieur de l'application est totalement exclu car les mots de passe de ce compte sont amenés à être modifiés à tout moment.

7.3 Compte de service

Des comptes de service sont à définir afin d'isoler et identifier plus facilement les services rendus et les sécuriser le cas échéant.

L'utilisation du compte de connexion fournisseur dans la configuration de l'application ou des services est totalement exclu.

7.4 Virtualisation

Dans le cadre de serveur virtuel, la configuration des ressources en terme de CPU et RAM est le fruit d'un accord entre fournisseur et CHU de Nantes.

Le CHU de Nantes se réserve le droit d'ajuster les ressources des serveurs virtuels en fonction des indicateurs de performances remontés par VMware, au travers de rapports sur les serveurs surdimensionnés ou bien sous-dimensionnés.

Le serveur virtuel est par défaut déployé avec une carte réseau de type VMXNET3 optimisée pour le fonctionnement avec les VMware Tools.

7.5 Accès Internet

Par défaut, un serveur ne dispose pas d'accès à Internet. Si cela est nécessaire, une validation du RSSI est nécessaire et tracée pour justifier du besoin.

7.6 Flux et interopérabilité

Le CHU de Nantes sécurise les flux via de la micro-segmentation à l'intérieur même de son réseau. Le fournisseur s'engage à préciser la matrice de flux spécifique à son application.

- Source
- Destination
- Port
- Protocole
- Description/rôle

Consulter les annexes techniques réseau pour plus d'informations.

Le fournisseur s'engage à fournir une cartographie applicative et technique de l'ensemble des flux traités par son application :

- Répertoires d'échange
- Type : socket mllp, ftp, ...
- Source
- Destination

Tous ces flux sont identifiés auprès du service interopérabilité du CHU de Nantes.