

ANNEXE CCTP - CONTRAINTES DSI

DOCUMENT

<i>Version</i>	3.0	
<i>Auteur</i>	Pascal DUNAUD	
<i>Date de diffusion</i>	04/2024	document de travail

DESCRIPTION

<i>Objet</i>	Fournir les éléments concernant la partie informatique pour la rédaction des CCTP
--------------	---

PRESENTATION :

Les chapitres suivants donnent par thématique les éléments devant être inclus aux cahiers des charges techniques des différentes consultations du CHU dès lors qu'une composante informatique fait partie des offres. Le choix des chapitres est à adapter selon leur utilité par rapport à l'offre.

GENERALITES :

Pour les composantes informatiques de son offre, le candidat devra se conformer strictement aux attentes spécifiées dans les sous-chapitres suivants. En cas de non-conformité, il devra clairement identifier cette non-conformité et expliciter son choix.

De manière générale, le candidat décrira précisément les composants informatiques de son offre, ses spécifications, les modes d'installation, de support et d'évolution des versions.

Notamment les différents produits devront répondre aux exigences de sécurité suivantes :

- versions supportées par les éditeurs uniquement et maintient dans le temps de ces versions à jour
- antivirus sur les systèmes d'exploitation
- détail de tous les flux réseau utilisés et durcissement des systèmes par désactivation des services inutiles

SERVEURS

GENERAL

- La virtualisation est à privilégier, sauf nécessité technique
- Les machines virtuelles seront hébergées sur les infrastructures du CHU qui utilisent exclusivement l'hyperviseur NUTANIX AHV

Eléments CCTP DSI

- Si l'offre nécessite un serveur physique, le CHU pour des raisons d'homogénéité de son parc fera de préférence l'acquisition sur ses marchés propres
- Si l'offre comprend obligatoirement la fourniture d'un serveur physique, pour pouvoir être hébergé dans le datacenter du CHU, il devra :
 - o être en format rack 19 pouces
 - o posséder des alimentations redondantes
 - o proposer des cartes réseaux redondantes, mode teaming (également supportée par l'OS et l'ensemble de la solution logicielle), interfaces 10Gb cuivre
 - o Proposer une interface d'administration type Idrac, ILO ou IPMI
- Le CHU possède ses propres marchés pour les licences Microsoft, elles ne doivent donc pas être fournies dans l'offre
- Les spécifications détaillées des serveurs doivent à minima comprendre :
 - o indications CPU
 - o mémoire RAM
 - o Disques et partitions
 - o performances disques attendues
 - o OS (préciser version française ou anglaise)
- Le CHU supporte et peut installer les OS suivants : Windows 2019, Windows 2022, Redhat 8 et 9, AlmaLinux 8 et 9, UBUNTU 20 ou 22
- Les serveurs devront de préférence être joints au domaine Active Directory du CHU pour permettre l'authentification nominative des administrateurs. Les serveurs Windows héritent alors de l'antivirus Microsoft et des mises à jour automatiques. Pour les serveurs Windows hors domaine, l'éditeur devra proposer une solution antivirus.
- Les serveurs Linux et Windows rentrent dans une politique de mise à jour système automatique. A défaut, le fournisseur s'engage à réaliser régulièrement ces mises à jours.

STOCKAGE NAS

- Pour des besoins de stockage, un partage NAS peut être mis à disposition par le CHU sous réserve de disponibilité
- Ce partage peut être disponible en NFS ou CIFS. Dans ce dernier cas, les droits sont affectés sur la base d'un compte Active Directory.
- Un mode WORM peut permettre l'archivage. Les modalités précises de mise en œuvre seront à valider.

BASES DE DONNEES

Les bases de l'établissement sont hébergées sur une plateforme virtualisée « Nutanix Database Service – DbaaS ». Cette plateforme est maintenue par l'équipe DBA du CHU.

L'établissement supporte les SGBD suivants :

- Oracle Database
- Microsoft SQL Server
- MySQL Community Server
- PostgreSQL

Les bases de données « Oracle Database », « Postgresql » et « MySQL Community Server » sont hébergées sur des serveurs « Oracle Linux », maintenu par l'équipe DBA du CHU.

Les bases de données « Microsoft SQL Server » sont hébergées sur des serveurs « Windows Server », maintenu par l'équipe DBA du CHU.

Des mises à jour systèmes sont appliquées régulièrement avec redémarrage de l'OS et des bases de données.

Les versions des moteurs de bases de données devront être officiellement supportées par l'éditeur et évoluer dans le cadre de la maintenance pour le rester.

L'accès aux serveurs (SSH/MSTSC) qui hébergent les bases de données est exclusivement réservé à l'équipe DBA du CHU.

Les privilèges « élevés » (DBA/SYSADMIN/ALL PRIVILEGES/etc.) sont exclusivement réservés pour l'équipe DBA du CHU. Pendant la phase de « MCO », le compte/schéma de l'application devra avoir des privilèges non intrusifs. Lors d'une mise à jour, il est possible de temporairement d'élever les privilèges d'un compte/schéma.

Pour chaque base de données une base de type « standby » (Oracle Dataguard, Mysql Replication, SQL Server AlwaysOn, Postgresql Replication) sera déployée par l'équipe DBA du CHU sur le site de PRA.

Les sauvegardes sont réalisées par des scripts maintenus par l'équipe DBA du CHU mais également par la fonctionnalité TimeMachine « Nutanix Database Service ».

Les bases de données des environnements de « test » (formation, preprod, test, etc), sont déployées au travers de la fonctionnalité « Clone – TimeMachine » de « Nutanix Database Service ».

La supervision des bases de données est réalisée au travers de la solution de supervision du CHU.

Si le candidat propose un autre type de base de données, il devra assurer le support, la sécurité et l'exploitation : évolutions, maintenance, sauvegarde, restauration, surveillance.

TELEMAINTENANCE

- Le fournisseur devra utiliser le portail SSL mis à disposition par le CHU
- Seulement sur dérogation accordée par le CHU suite à étude technique, une autre solution justifiée pourra être utilisée
- Les comptes utilisateurs sont nominatifs. Il est nécessaire de fournir un numéro de téléphone portable ou à défaut une adresse mail individuelle pour obtenir le code OTP
- Sur exception justifiée, un compte générique et une adresse mail générique peuvent être utilisés (uniquement pour des plateformes de support)
- Les sessions de télémaintenance sont enregistrées

RESEAU

- Le réseau filaire 100/1000 Mb/s
- Réseau WIFI :
 - o Couverture des zones de circulation
 - o Privilégier bande des 5Ghz
- Sécurisation 802.11x
 - o Sur la base d'un compte utilisateur AD
 - o Ou d'un compte machine dans l'AD
 - o Ou à défaut par adresse MAC
- Les adresses IP et VLAN sont fixées par le CHU
- Les équipements ne seront connectés que s'ils respectent les règles élémentaires de sécurité : mises à jour, version supportée, antivirus
- La disponibilité en prise réseau doit être étudiée en amont
- Les autorisations d'accès extérieur devront être validées avant d'être envisagées

FOURNITURE DE POSTES CLIENTS

- Les postes clients sont préférentiellement fournis par le CHU
- A défaut, les postes devront respecter les règles élémentaires de sécurité : mises à jour, version supportée, antivirus
- Ils devront être inclus au domaine CHU pour gestion centralisée
- Les versions système et les logiciels utilisés devront être validés

APPLICATIONS CLIENTS LOURDS

- Les logiciels doivent être référencés par la direction informatique
- Les installations sont à fournir sous forme de .MSI pour être distribuables

APPLICATIONS WEB

- Les navigateurs validés sont EDGE,Firefox et Chrome
- Pour des raisons de sécurité, Internet Explorer n'est plus supporté
- L'application doit respecter les standards et n'utiliser que le protocole https

SAUVEGARDE

- Sauvegarde : un descriptif détaillé des données à sauvegarder est attendu (emplacement et périodicité) pour minimiser le risque de perte de données avec éventuellement les scripts qui permettront ces sauvegardes s'il y a lieu.
L'intégration à l'outil de sauvegarde du CHU, VEEAM, est préconisée, à défaut le prestataire engage sa responsabilité sur la mise en place et le suivi des sauvegardes.