STANDARD TECHNIQUE D'ARCHITECTURE ET PRECONISATIONS POUR UN NOUVEL ENVIRONNEMENT AIX/ORACLE LINUX/MYSQL/PGSQL WINDOWS/SQLSERVER STOCKAGE DES DONNEES

PARTIE 1

STANDARD TECHNIQUE D'ARCHITECTURE AIX/ORACLE

Cette partie du document décrit la norme des spécificités techniques définie pour intégrer une nouvelle application nécessitant une tierce base de données Oracle hébergée sur un serveur Unix AIX.
L'éditeur doit s'assurer de la compatibilité de son logiciel ou de sa solution avec :
- les versions & configurations AIX et ORACLE définies dans ce document,
- les autres outils (EON, Rubrik, …)
- les autres préconisations (sécurité, documentation, …)

A) Architecture OS Unix

1 - Type et version

Le serveur héberge un système d'exploitation Unix IBM AIX en version 7.2 TL5.
Toutes les partitions Unix seront installées dans des environnements virtualisés (VIO serveur).

2 - FileSystems

Les données sont stockées sur un système de fichiers JFS2 (ou JFS évolué).
Les Filesystems seront créés par le CHU pour être adaptés à l'architecture de stockage du CHU selon la norme décrite en annexe.
L'éditeur devra donner les points de montage nécessaires (taille, nom, contraintes).

3 - Environnement

Deux environnements sont mis à disposition : un serveur de production dédié et un serveur de test soit dédié soit mutualisé.

4 - Utilisateurs Unix

Les composants Oracle nécessitent un utilisateur Unix par version de noyau Oracle : ora<version> (propriétaires des binaires Oracle) et oracle (propriétaire des binaires de l'agent de supervision OEM Cloud Control).
L'éditeur devra fournir la liste des utilisateurs applicatifs ainsi que leurs caractéristiques.

5 - Charge applicative

L'éditeur devra également fournir une estimation du nombre de processus clients dédiés (et simultanés si possible) activés sur la plateforme de production. Dans l'hypothèse où cette information ne serait pas disponible, le nombre d'utilisateurs finaux constituerait une information pertinente.

6 - Exploitation

L'exploitation d'un serveur AIX implique un redémarrage automatique une fois par mois minimum. L'éditeur devra fournir les commandes, scripts ou méthode d'arrêt/démarrage des éléments applicatifs (qui seront utilisés dans les scripts arret_exploit et lance_exploit sous /u/exploit).

7 - Ressources système

L'éditeur devra fournir la description des ressources systèmes nécessaires pour son application (CPU, RAM, stockage) dans le contexte de l'utilisation de l'application au CHU de Toulouse.

B) Architecture SGBD Oracle

1 - Version

Le serveur Unix AIX héberge un système de gestion de base de données en version 12.2.0.1 ou 19c.

2 - Environnements

Deux environnements sont mis à disposition : un serveur de production dédié et un serveur de test soit dédié soit mutualisé.

3 - Nommage de l'instance

Le nom de l'instance Oracle doit être en majuscules et composé de 8 caractères maximum.

4 - Arborescence des binaires

Les binaires RDBMS Oracle en version 12.2.0.1 ou 12.2.0.3 (19c) seront installés dans l'arborescence /oracle/product/<version>.

5 - Arborescence de la base de données

Les fichiers de base de données seront hébergés sous /oracle/oradata/<SID>. L'extension de ces fichiers suit la norme : fichiers de données .dbf, fichiers de contrôle .ctl, fichiers de journalisation .rdo et fichiers d'archive .arc.

Les fichiers liés à l'exploitation de l'instance seront hébergés sous /oracle/admin/<SID> : fichiers d'audit (.aud) sous adump, script de création de l'instance sous create et fichier caractère de paramètres d'initialisation sous pfile (init<SID>.ora).

Après création de l'instance, un fichier binaire de paramètres d'initialisation (spfile<SID>.ora) sera généré sous /oracle/<version>/dbs. Toute mise à jour d'un paramètre d'initialisation devra s'effectuer via la commande ALTER SYSTEM … SCOPE=SPFILE.

6 - Mode ARCHIVELOG

Le mode ARCHIVELOG est systématiquement activé après la création de l'instance. Les fichiers d'archive seront hébergés sous /sv<SID>/archives.

L'éditeur devra fournir une estimation du volume d'archivelogs généré quotidiennement.

7 - Jeu de caractères

Les jeux de caractères nationaux de base de données préconisés sont AL32UTF8 (unicode) et WE8MSWIN1252 (non unicode). L'éditeur devra préciser quel jeu de caractères est nécessaire pour son application.

8 - Rôles et privilèges

L'utilisation du rôle (ensemble de privilèges affectés à un utilisateur Oracle) prédéfini DBA (gestion des utilisateurs et tables associées) doit être limitée car cela peut constituer une faille de sécurité.

9 - Taille de la base de données

L'éditeur devra fournir la taille de la base de données nécessaires et un pourcentage annuel d'accroissement du volume des données (données structurées et non structurées).

C) Sauvegarde OS

1 - Outil et version

La sauvegarde du système est gérée par l'outil Rubrik.

2 - Stratégie

La stratégie de sauvegarde est de générer une sauvegarde toutes les nuits. Si la stratégie ne correspond pas au besoin de l'application, l'éditeur devra l'indiquer et préciser ses préconisations.

3 - Consignes particulières

L'éditeur devra donner une procédure de restauration des données applicatives et des consignes de reprise de l'application après une restauration des données complète ou partielle.
Il devra aussi fournir la liste des FileSystems ou répertoires à exclure de la sauvegarde Rubrik.

D) Sauvegarde SGBD Oracle

1 - Outil et version

La sauvegarde de la base de données Oracle est gérée par l'outil Rubrik via RMAN Oracle (proposé en natif avec le SGBD).

2 - Arborescence

Les fichiers de sauvegarde sont générés sous des points de montage NFS Rubrik.

3 - Méthodes

Deux méthodes de sauvegarde sont proposées :
- Base ouverte (online), méthode par défaut limitant la perte de données en cas de restauration
- Base fermée (offline), méthode marginale liée à une contrainte applicative

4 - Ordonnancement

Save/purge archivelog toutes les 2H par toutes les SLA Oracle Rubrik.
Via SLA Rubrik :
- SLA Oracle Prod déclenche une save incrémentale 20h – 07h
- SLA Oracle Test déclenche une save incrémentale 19h-07h

La nécessité de synchroniser la sauvegarde de la base de données et la sauvegarde de données applicatives externes devra être spécifiée et décrite par l'éditeur.

E) Supervision OS

1 - Outil et version

La supervision des serveurs Unix est gérée par l'outil EyesOfNetwork en version 5.0.

2 - Arborescence

Les binaires sont installés sous /opt.

3 - Alertes

Les alertes de type "système" sont définies par l'équipe INFRA CHU sur tous les serveurs : surveillance des taux de remplissage des FileSystems, des ressources systèmes, des process Oracle, …

L'éditeur devra indiquer quels sont les process de l'application à surveiller et, le cas échéant, quelles actions doivent y être associées.

F) Supervision SGBD

1 - Outil et version

La supervision des bases de données Oracle est gérée par l'outil OEM Cloud Control en version 13.4.0.0.

Les binaires associées à l'agent de surveillance sont installés sous /oracle/product/ag13c.

2 - Métriques spécifiques

La liste des métriques spécifiques liées à la base de données à surveiller peut-être fournie par l'éditeur : ils seront intégrés à la supervision dans la mesure du possible.

G) Autres composants logiciels

L'éditeur pourra installer son serveur Apache/Tomcat. Si cette installation est réalisée par le CHU, voici ce qui sera installé :

1 - Apache

2 - Apache Tomcat

Le serveur d'applications installé par défaut est en version 6.0.35 sous /opt/tomcat.

3 - Autres composants logiciels

L'éditeur devra fournir la liste des composants ou logiciels nécessaires (c++, SAMBA, …).

H) Architecture globale et exploitation de l'application

1 - Architecture

L'éditeur devra fournir un document d'architecture et un document décrivant l'interaction et/ou dépendance entre les différents composants de l'architecture globale. Il inclura le(s) serveur(s) de base de données, le(s) serveur(s) frontal(aux), le(s) serveur(s) applicatif(s), les postes clients (lourd ou léger), le(s) flux de données, ...

2 - Contraintes d'exploitation

L'éditeur devra fournir les contraintes de disponibilité de service pour chaque environnement. Notamment les créneaux horaires d'interruption où des interventions de type "maintenance" pourraient être réalisées.

3 - Consignes de reprise

L'éditeur devra donner des consignes de reprise de l'application après un arrêt anormal.

4 - Cycle de vie des données

L'éditeur peut proposer toute solution d'archivage ou d'épuration des données anciennes ou obsolètes, pour les données structurées en base de données ou pour les données non structurées.
Il devra fournir les scripts de purge permettant de supprimer les données obsolètes.

5 - Données temporaires

Les données temporaires (dumps, exports, extractions, chargements ponctuels, …) devront être déposées dans des FileSystems dédiés. L'éditeur devra fournir la liste et le volume de ces données.

I) Sécurité

L'éditeur devra donner la liste des protocoles et services utilisés (ssh, sftp, sendmail, https …). Tout autre protocole ou service non-spécifié sera désactivé.
Les règles de sécurité basiques sont imposées :
- Pas de connexion directe au serveur AIX avec l'utilisateur Unix root (utilisation de sudo) ;
- Pas de user=password et un minimum de 12 caractères pour le mot de passe ;
- Utilisation du protocole ssh pour la connexion et le transfert de données entre les serveurs ;
- L'utilisation des protocoles non sécurisés (telnet, ftp, rsh, …) est formellement interdite ;
- Modification du mot de passe par défaut de l'utilisateur Oracle DBSNMP ;
- Ne pas attribuer systématiquement le rôle DBA aux utilisateurs Oracle de l'application.

J) Plateforme client

Le poste client héberge un système d'exploitation Windows10 ou Windows11.

K) Annexe

OS UNIX	
Type	AIX
Version	7.2 TL5
FS	jfs2
Utilisateur SGDB Unix	ora12201 /ora12203
Utilisateur Supervision Oracle Unix	oracle
Utilisateurs applicatifs Unix	Fournir la liste des utilisateurs applicatifs et leurs caractéristiques
Type d'environnement	Production (serveur dédié) Test (serveur dédié ou mutualisé)
Norme de nommage du serveur	srvxxx (xxx=sigle application ; plateforme de production)

	srvxxxtst (xxx=sigle application ; plateforme de test dédiée) srvenvtstn (plateforme de test mutualisée)
Exploitation	Reboot mensuel ou hebdomadaire Fournir les éléments d'arrêt/démarrage applicatif (scripts d'automatisation arret_exploit et lance_exploit sous /u/exploit)
Charge applicative	Fournir une estimation du nombre de processus clients
SGBD ORACLE	
Version RDBMS	12.2.0.1 / 12.2.0.3 (19c)
Type d'environnement	Production (serveur dédié) Test (serveur dédié ou mutualisé)
Norme de nommage de l'instance	SID en majuscules, 8 caractères maximum
Arborescence binaires	/oracle/product/<version>
Arborescence applicative	/oracle/oradata/<SID> /oracle/oraindx/<SID> /oracle/ oradata/<SID>/redo01 /oracle/ oradata/<SID>/redo02 /oracle/ oradata/<SID>/ctrl01 /oracle/ oradata/<SID>/ctrl02
Arborescence d'exploitation	/oracle/admin/<SID>/adump /oracle/admin/<SID>/create /oracle/admin/<SID>/pfile /oracle/diag
Arborescence fichiers d'archive	/sv<SID>/archives
Norme de nommage des fichiers	Fichiers de données .dbf Fichiers de contrôle .ctl Fichiers de redo .rdo Fichiers d'archive .arc
Gestion fichier d'initialisation binaire	/oracle/dbs/<version>/spfile<SID>.ora
Tolérance perte de données	ARCHIVELOG
Volumétrie	
Volumétrie à moyen terme (3 ans)	
Jeu de caractères	AL32UTF8, WE8MSWIN1252
Privilèges et rôles des utilisateurs Oracle	Limiter l'octroi du rôle DBA
Archivage	Fournir les scripts et/ou méthodes pour archiver les données applicatives
SAUVEGARDE OS	
Outil	Rubrik
Version	9.2
SAUVEGARDE SGBD ORACLE	
Outil	Rubrik via RMAN
Arborescence sauvegarde	/sv<SID>/base
Méthode de sauvegarde	Base ouverte Tâche journalière planifiée via SLA Rubrik
Synchronisation applicative	Fournir les scripts et/ou méthodes de synchronisation de sauvegarde Oracle et éléments applicatifs
SUPERVISION OS	
Outil	EyesOfNetwork

Version	5.0
SUPERVISION SGBD ORACLE	
Outil	Oracle Enterprise Manager Cloud Control
Version	13.4.0.0
Arborescence binaires	/oracle/product/ag13c
COMPOSANTS	
Java SDK/JDK	6.0.0.375
Apache	2.2
Apache Tomcat	6.0.35
PLATEFORME CLIENT	
Type	Windows
Version	10/11
Client Oracle	12c ou 19c

PARTIE 2

STANDARD TECHNIQUE D'ARCHITECTURE LINUX

Cette partie du document décrit la norme des spécificités techniques définie pour intégrer une nouvelle application

A) Architecture OS Linux

1 - Type et version

Le serveur héberge un système d'exploitation Linux des distributions suivantes : RedHat 8/9, Debian 11/12 ou Ubuntu 20/22.
Toutes les VM Linux seront installées dans des environnements virtualisés VSphere 7 ou 8. Le CHU ne fait pas de réservations de ressources sur les environnements virtuels. Les VMs doivent être compatibles, snapshot, vmotion et storage vmotion.
Seuls les OS de type Linux hébergeront les SGBD de type Mysql, MariaDB ou PGSQL.

2 - FileSystems

Les données sont stockées sur un système de fichiers xfs (par defaut) ou ext4.
Les Filesystems seront créés par le CHU pour être adaptés à l'architecture de stockage du CHU selon la norme décrite en annexe.
L'éditeur devra donner les points de montage nécessaires (taille, nom, contraintes).

3 - Environnement

Deux environnements sont mis à disposition : une VM de production et une VM de test.

4 - Utilisateurs Linux

L'éditeur devra fournir la liste des utilisateurs applicatifs ainsi que leurs caractéristiques. Le compte root reste à discrétion du CHU. Utilisation possible de sudo si nécessaire.

5 - Charge applicative

L'éditeur devra également fournir une estimation du nombre de processus clients dédiés (et simultanés si possible) activés sur la plateforme de production. Dans l'hypothèse où cette information ne serait pas disponible, le nombre d'utilisateurs finaux constituerait une information pertinente.

6 - Exploitation

L'exploitation d'une VM Linux implique un redémarrage automatique une fois par mois minimum. L'éditeur devra fournir les commandes, scripts ou méthode d'arrêt/démarrage des éléments applicatifs.

7 - Ressources système

L'éditeur devra fournir la description des ressources systèmes nécessaires pour son application (CPU, RAM, stockage) dans le contexte de l'utilisation de l'application au CHU de Toulouse. Il devra également fournir la liste des packages à installer sur la VM Linux, nécessaires au fonctionnement de l'application (ex : Apache, Mysql, PGSql …)

B) Sauvegarde OS

1 - Outil et version

La sauvegarde du système est gérée par l'outil Rubrik en version 9.2. La VM est sauvegardée globalement et la restauration peut être complète ou granulaire.

2 - Stratégie

La stratégie de sauvegarde est une sauvegarde incrémentale journalière avec une rétention de 6 mois.
Si ces stratégies ne correspondent pas au besoin de l'application, l'éditeur devra l'indiquer et préciser ses préconisations.

3 - Consignes particulières

L'éditeur devra donner une procédure de restauration des données applicatives et des consignes de reprise de l'application après une restauration des données complète ou partielle.
Il devra aussi fournir la liste des FileSystems ou répertoires à exclure de la sauvegarde Rubrik.

C) Supervision OS

1 - Outil et version

La supervision des serveurs Linux est gérée par l'outil EyesOfNetwork en version 5.0.

2 - Alertes

Les alertes de type "système" sont définies par l'équipe INFRA CHU sur tous les serveurs : surveillance des taux de remplissage des FileSystems, des ressources systèmes …
L'éditeur devra indiquer quels sont les process de l'application à surveiller et, le cas échéant, quelles actions doivent y être associées.

D) Autres composants logiciels

L'éditeur devra fournir la liste des composants ou logiciels nécessaires (apache, mysql, pgsql, perl, SAMBA, …).
Ces composants devront être en cours de support LTS.

E) Architecture globale et exploitation de l'application

1 - Architecture

L'éditeur devra fournir un document d'architecture et un document décrivant l'interaction et/ou dépendance entre les différents composants de l'architecture globale. Il inclura le(s) serveur(s) de base de données, le(s) serveur(s) frontal(aux), le(s) serveur(s) applicatif(s), les postes clients (lourd ou léger), le(s) flux de données, ...

2 - Contraintes d'exploitation

L'éditeur devra fournir les contraintes de disponibilité de service pour chaque environnement. Notamment les créneaux horaires d'interruption où des interventions de type "maintenance" pourraient être réalisées.

3 - Consignes de reprise

L'éditeur devra donner des consignes de reprise de l'application après un arrêt anormal.

4 - Cycle de vie des données

L'éditeur peut proposer toute solution d'archivage ou d'épuration des données anciennes ou obsolètes, pour les données structurées en base de données ou pour les données non structurées.
Il devra fournir les scripts de purge permettant de supprimer les données obsolètes.

5 - Données temporaires

Les données temporaires (dumps, exports, extractions, chargements ponctuels, …) devront être déposées dans des FileSystems dédiés. L'éditeur devra fournir la liste et le volume de ces données.

F) Sécurité

L'éditeur devra donner la liste des protocoles et services utilisés (sftp, sendmail, https …). Tout autre protocole ou service non-spécifié sera désactivé.
Les règles de sécurité basiques sont imposées :
- Pas de connexion directe à la VM Linux avec l'utilisateur root;
- Pas de user=password et un minimum de 12 caractères pour le mot de passe ;
- Utilisation du protocole ssh pour la connexion et le transfert de données entre les serveurs ;
- Utilisation des protocoles non sécurisés (rsh, rcp, ftp, telnet, …) interdite ;

H) Annexe

OS UNIX	
Type	Linux
Version	RedHat 8/9 ou debian 11/12 ou Ubuntu 20/22
FS	Xfs ou Ext4
Utilisateurs applicatifs Linux	Fournir la liste des utilisateurs applicatifs et leurs caractéristiques
Type d'environnement	Production Test
Norme de nommage du serveur	svlxxx (xxx=sigle application ; plateforme de production) svlxxxtst (xxx=sigle application ; plateforme de test dédiée)
Exploitation	Reboot mensuel ou hebdomadaire Fournir les éléments d'arrêt/démarrage applicatif
Charge applicative	Fournir une estimation du nombre de processus clients
SAUVEGARDE OS	
Outil	Rubrik
Version	9.2
SUPERVISION OS	
Outil	EyesOfNetwork
Version	5.0

PARTIE 3

STANDARD TECHNIQUE D'ARCHITECTURE WINDOWS ET BASES DE DONNEES SQL

A) Environnement Windows et bases de données SQL

1- Serveur

Les OS sur les serveurs ou sur les postes doivent être en langue française ou anglaise.

Windows

- Windows Server 2019 ou 2022 avec derniers patchs de sécurité
- Si serveur virtualisé, la solution doit être compatible avec VMware VSphere 7 ou 8
- Le CHU ne fait pas de réservations de ressources sur les environnements virtuels. Les VMs doivent être compatibles, snapshot, vmotion, storage vmotion.
- Serveur Web -> IIS7 ou supérieur
- Pas de solution type Deviguard empêchant l'installation des outils du CHU
- Le client SCCM sera installé sur les serveurs pour : installation des mises à jour, reboot, déploiement de packages
- Un reboot hebdomadaire est nécessaire : les applications doivent pouvoir redémarrer après le reboot sans intervention humaine
- Pas d'autologon sur les serveurs, les applications doivent se lancer par des services windows

Configuration si le serveur est fourni avec l'application (ce choix est à justifier pour être accepté)

- Alimentation électrique redondante.
- 2 cartes réseaux. Gigabits + port iLO.
- Disques Hot Plug en Raid 1 ou Raid 5
- 16 GO de RAM minimum

Si serveur au Centre de traitement Informatique DSN -> format rack 19'' obligatoire et 2 serveurs pour assurer le service sur les 2 salles informatiques.

Solution Antivirus

Solution antivirus du CHU de Toulouse : Palo Alto Cortex
Console d'administration centralisée : Palo Alto Cortex

Fonctionnalités activées :

- Mise à jour automatique
- Contrôle sur accès
- Surveillance des comportements
- Contrôle programmé périodique
- Scan complet des disques chaque samedi.

Des exclusions peuvent être mises en place sur :

- des fichiers
- des dossiers
- des extensions
- des processus
- des sites web

Ces exclusions devront être précisées avant l'installation du serveur.

2 - Système de gestion de Base de données SQL

Le serveur Windows héberge un système de gestion de base de données en version 2019 ou 2022 comprenant le dernier CU supporté.

Environnements
Deux environnements sont mis à disposition : un serveur de production dédié et un serveur de test soit dédié soit mutualisé.

Nommage de l'instance
Le nom de l'instance SQL Server doit être sous la forme : SQL<code appli>01

Arborescence des binaires
Les binaires SQL Server en version 2017 et 2019 seront installés sur C:\.

Arborescence de la base de données
Les fichiers de base de données seront hébergés de cette façon :
- Fichier de data => D:\
- Fichier de transaction logs => L:\
- Fichier de la base temporaire => T:\

Mode de récupération
Le mode de récupération par défaut est le mode COMPLET (transaction logs gardés jusqu'à la sauvegarde de ceux-ci), les instances de test sont en mode de récupération SIMPLE (transaction logs purgés automatiquement)

Jeu de caractères
Les jeux de caractères nationaux de base de données installé par défaut sera FRENCH_CI_AS. L'éditeur devra préciser quel jeu de caractères est nécessaire pour son application.

Rôles et privilèges
L'utilisation du rôle sysadmin sera réservé au groupe AD admins des membres DSN infrastructure du CHU prévu à cet effet, le compte SA sera désactivé.
La gestion des droits applicatifs doit si cela est possible être gérée via des comptes AD. Deux groupes seront créés pour accéder aux bases applicatives (Lecture et écriture). Des comptes SQL peuvent être créés si la solution ne supporte pas l'authentification Windows.

Taille de la base de données
L'éditeur devra fournir la taille de la base de données nécessaires et un pourcentage annuel d'accroissement du volume des données (données structurées et non structurées).

3 - Sécurité

- Antivirus : Sophos Endpoint Security and Control **(analyse « temps réel » et mises à jour automatiques)**.
- Le serveur sera maintenu à jour mensuellement au niveau patchs de sécurités Windows par SCCM ou, **exceptionnellement**, de façon manuelle.
- Les serveurs sont équipés du logiciel d'inventaire/télédistribution/télé-intervention du CHU (SCCM)
- Les comptes utilisateurs devront être en priorité des comptes de domaine, avec un mot de passe complexe.
- Les comptes utilisateurs n'ont pas de droits « Administrateur » sur les serveurs et/ou postes de travail
- La sécurité des partages devra s'appuyer sur les groupes globaux du domaine.
- Le compte Administrateur devra être utilisé de façon restreinte.
- Les prestataires se voient attribuer un compte CA (compte administrateur) qui leur permettra d'effectuer les tâches demandées mais pas plus

4 - Surveillance Serveur

Un descriptif du fonctionnement de l'application doit être fourni à l'équipe système, ainsi que les éléments (logs, services etc.) à surveiller pour une future intégration dans EON pour les alertes standard (CPU, RAM, disque).
SCOM est également utilisé pour la supervision des rôles et services Microsoft (Active Directory, SQL, …)

5 – Intégration

Le logiciel doit s'intégrer ou s'appuyer sur Active Directory pour l'authentification (actuellement AD2016)

B) Sauvegardes

Le système proposé doit permettre d'effectuer des sauvegardes sans arrêter les utilisateurs.
La sauvegarde de données doit pouvoir être déclenchée automatiquement à une heure déterminée par l'administrateur du système.
La durée de la sauvegarde, en fonction du volume à sauvegarder doit être précisée dans l'offre.
L'enregistrement sur stockage dédié sera réalisé avec le système préconisé par le CHU (Rubrik)
La restauration d'une partie ou de la totalité sera réalisée à la demande en vue de remettre le système opérationnel.
Des procédures de remise en état de marche seront fournies par le soumissionnaire.
La VM hébergeant l'application devra être compatible avec les snapshots VMware.

1 – Sauvegarde SGBD SQL Server

La sauvegarde de la base de données SQL Server est gérée par l'outil Rubrik (proposé en natif avec le SGBD).

2 - Arborescence

Les fichiers de sauvegarde sont générés sous des points de montage NFS Rubrik.

3 - Ordonnancement

Save/purge Transaction logs toutes les 2H par toutes les SLA MSSQL Rubrik.
Via SLA Rubrik :
- SLA Infrastructures Prod déclenche une save 20h – 07h
- SLA SQL Appli Patient Prod déclenche une save 20h-07h
- SLA SQL Appli Administratives Test déclenche une save 20h – 07h
- SLA SQL Appli Patient Test déclenche une save 20h – 07h

La nécessité de synchroniser la sauvegarde de la base de données et la sauvegarde de données applicatives externes devra être spécifiée et décrite par l'éditeur.

4 – Méthode

Le backup se lance via le compte de service Rubrik, celui-ci doit disposer de droits restreint : dbcreator au niveau serveur, db_backupoperator sur chaque base de données.

Dans le cas d'une instance en AlwaysON, le compte de service Rubrik devra être sysadmin de l'instance.

Sécurité d'accès et confidentialité

Pour s'authentifier sur le domaine, chaque utilisateur est identifié par un nom et un mot de passe
La gestion du profil des différents utilisateurs de la solution devra être précisée

C) Maintenance

Le système proposé doit accepter une fenêtre de maintenance hebdomadaire (2 heures minimum) afin que les serveurs soient mis à jour et redémarrés. Les reboots et mises à jour nécessaires au bon fonctionnement du serveur auront lieu durant cette fenêtre de maintenance.

PARTIE 4

DESCRIPTION DE L'ARCHITECTURE DE STOCKAGE

Cette partie du document décrit l'architecture de stockage installée au CHU
Il y a 2 types de stockage:

- Stockage SAN principalement pour les données structurées
- Stockage NAS pour les données non structurées

A) Stockage SAN

1 - Matériel

Le SAN est composé de :

- 2 switchs SAN de 96 ports chacun (vitesse des ports 16Gbs) par datacenter sur 2 fabrics différentes
- 2 liens FC 16 Gb entre les 2 datacenters
- 2 baies de stockage SAN Huawei Dorado 5000 V6 full NVME.

2 – Organisation du stockage SAN

L'ensemble de la volumétrie est sécurisé de site à site par la technologie Hypermétro.
Les outils associés Huawei permettent de réaliser le monitoring et le reporting de l'ensemble des données du SAN

B) Stockage NAS

1 - Matériel

Le stockage NAS est organisé avec :

- 2 baies NETAPP FAS800 sur 2 sites différents
  - Metrocluster IP sur des liens dédiés
- Un stockage objet Scality
  - 9 nœuds répartis sur 3 sites (Mipih, IUC, Purpan)

2 – Organisation du stockage NAS

Le NAS NETAPP héberge les données métiers et les met à disposition via les protocoles nfs et cifs.
Le stockage DELL ECS permet le stockage de masse de données qui ne nécessite pas de performances accrues : Backup, Archives Imagerie, exports oracle, vidéosurveillance. Les données hébergées sont disponibles via les protocoles nfs, cifs et S3

C) Stockage des données pour une application

Les solutions de stockage du CHU permettent de répondre de manière adaptée aux différents besoins de stockage de la donnée, aussi bien en termes de performance que de sécurité.

Il est donc nécessaire que l'éditeur décrive exactement les types de données (structurées, non structurées), leurs volumes, la classe de service souhaitée et nécessaire au bon fonctionnement de l'applicatif (performance et sécurité) dans le contexte d'utilisation du CHU.

PARTIE 5

STANDARD TECHNIQUE D'ARCHITECTURE APPLIDIS FUSION 5 HF23

Cette partie du document décrit la norme des spécificités techniques définie pour intégrer une nouvelle application

A) Architecture

1 – Système d'exploitation

Les 2 systèmes d'exploitation hébergeant des applications et qui sont validés en production au CHU : windows 2019 standard et windows 2022 standard

2 - Compatibilité

L'application doit être multi utilisateurs

L'application doit être compatible pour une utilisation en mode bureau à distance (anciennement TERMINAL SERVER)

L'application doit être compatible avec les systèmes d'exploitation windows 2019 standard et windows 2022 standard.

L'application doit être en capacité d'actualiser dynamiquement les informations de session de bureau à distance notamment les imprimantes clientes

3 - Environnement

Deux environnements sont mis à disposition : l'environnement de PROD et l'environnement de QUALIF/TEST.

L'éditeur devra fournir les préconisations dans le cadre de l'utilisation de la solution antivirale Cortex

L'éditeur devra fournir les préconisations dans le cadre de l'utilisation des solutions de monitoring Microsoft à savoir SCCM et SCOM version CB

L'éditeur devra fournir toutes les sources nécessaires à l'installation de l'application

L'éditeur devra spécifier les prérequis applicatifs nécessaires à l'installation et au fonctionnement de l'application

L'éditeur devra spécifier les prérequis système nécessaires à l'installation et au fonctionnement de l'application

L'éditeur devra indiquer les ports à ouvrir au niveau du pare-feu qui sont nécessaires au fonctionnement de l'application

4 - Charge applicative

L'éditeur devra fournir les infos ci-dessous dans le cas d'usage de l'application par une seule personne :

- % CPU max utilisé
- % RAM max utilisé

5 - Exploitation

Les serveurs d'applications publiées Applidis redémarrent une fois par semaine.
L'éditeur devra spécifier s'il y a des particularités à respecter lors de ces redémarrages programmés (service à arrêter au préalable, vérification à effectuer avant remise à disposition du serveur aux utilisateurs)
L'éditeur devra fournir les procédures de mise à jour de l'application lors des changements de version, et ce que le changement soit majeur ou mineur

6 - Ressources système

L'éditeur devra spécifier les ressources systèmes nécessaires pour son application (CPU, RAM, stockage) dans le contexte de l'utilisation de l'application en mode bureau à distance.

B) Sauvegarde

1 – Système de modèle de serveur d'application

Tous les serveurs d'application publiées Applidis au CHU ont un modèle, depuis lequel ils sont déployés, donc pas besoin de sauvegarder le serveur d'application en lui-même

2 – Sauvegarde applicative

L'éditeur devra spécifier les éléments à sauvegarder de son environnement applicatif, ainsi que la politique de sauvegarde associée, et tout cela en dehors de la publication Applidis

C) Supervision OS

1 - Outil et version

La supervision des serveurs de publication Applidis est assurée par les outils Microsoft SCOM et SCCM

2 - Alertes

Les alertes de type "système" sont définies par l'équipe INFRA CHU : surveillance du taux d'utilisation des ressources systèmes (%RAM utilisée, %CPU utilisé, file d'attente CPU, file d'attente disque, bande passante, etc …)
L'éditeur devra indiquer quels sont les processus de l'application à surveiller et, le cas échéant, quelles actions doivent y être associées.

E) Architecture globale et exploitation de l'application

1 - Architecture

L'éditeur devra fournir un document d'architecture et un document décrivant l'interaction et/ou dépendance entre les différents composants de l'architecture globale. Il inclura le(s) serveur(s) de base de données, le(s) serveur(s) frontal(aux), le(s) serveur(s) applicatif(s), les postes clients (lourd ou léger), le(s) flux de données, ...

2 - Contraintes d'exploitation

L'éditeur devra fournir les contraintes de disponibilité de service pour chaque environnement. Notamment les créneaux horaires d'interruption où des interventions de type "maintenance" pourraient être réalisées.

3 - Consignes de reprise

L'éditeur devra donner des consignes de reprise de l'application après un arrêt anormal.

F) Sécurité

L'éditeur devra donner la liste des protocoles et services utilisés (ftp, sendmail, http …). Tout autre protocole ou service non-spécifié sera désactivé.

L'éditeur n'aura pas les droits d'administration sur les serveurs d'applications Applidis, toute demande de modification passera par la mise à disposition d'une procédure que l'équipe système Applidis appliquera pour appliquer la modification

H) Annexe

OS WINDOWS	
Type	Windows Server
Version	2019 ou 2022 Standard
Type d'environnement	Production Test
Norme de nommage du serveur	Svm-sxxf5-pxx (xx=silo application ; plateforme de production) Svm-sxxf5-txx(xx=silo application ; plateforme de test) Svm-sxxf5-qxx(xx=silo application ; plateforme de qualif)
Exploitation	Reboot hebdomadaire Fournir les spécificités d'arrêt/démarrage applicatif
Charge applicative	Fournir une estimation du % MAX CPU et RAM dans le cas d'usage de l'application par une seule personne
SAUVEGARDE	
Outil	Pas de sauvegarde côté publication Applidis. Sauvegarde de l'environnement applicatif à spécifier par l'éditeur
Version	
SUPERVISION OS	
Outil	SCOM , SCCM
Version	

PARTIE 6

STANDARD TECHNIQUE D'ARCHITECTURE POSTE DE TRAVAIL

1 – Système d'exploitation

Voici la liste des OS client autorisé sur le CHU :

Windows 10 64 bits
Windows 11 64 bits
MAC OS > 10.15
Android > 9.X
IOS

L'éditeur devra fournir l'ensemble des OS compatibles à sa solution.

2 – Outil de gestion

2.1 - Windows

Les terminaux installés avec un OS Windows sont gérés par l'outil MECM (anciennement SCCM) de manière centralisée.
Cet outil gère l'inventaire, le déploiement d'application, d'OS et de mise à jour de sécurité, gère la conformité, l'antivirus et les politiques d'alimentation.

2.2 – MAC OSX – IOS – Android

Les terminaux installés avec un OS Apple ou Android sont gérés par l'outil WorkSpaceOne de VMWare.

3 – Sécurité

- L'Antivirus installé sur les postes de travail Windows est Cortex. L'éditeur devra fournir la liste des fichiers ou dossiers à exclure si le besoin est exprimé. **Ce logiciel est obligatoire**
- Les comptes utilisateurs ne sont pas administrateur des postes de travail
- Les mises à jour de sécurité Windows sont déployés tous les mois sur l'ensemble des postes de travail.
- Les protocoles utilisés par la solution doivent être supporté par l'éditeur de ces derniers.
- Les composants systèmes utilisés par la solution doivent être supporté par l'éditeur de ces derniers.

4 – Configuration matérielle

La configuration standard du poste de travail au CHU de Toulouse est :

- Processeur : Equivalent Intel Core i3 ou AMD Ryzen 3
- RAM : 8 Go
- Disque : 250Go SSD
- Connectique : USB-C ou USB 3.1, Ethernet, Display Port, HDMI
- Affichage : Résolution FHD 1920x1080 (PC portable et écran externe)
- Graphique : Utilisation du chipset graphique interne

Les prérequis matériels de la solution doivent être délivré dans tous les cas.

5 - Sauvegarde

PC fixe :
Les terminaux Windows de type PC fixe sont configurés avec la redirection de données du profil utilisateur. Les dossiers redirigés sont : Bureau, Mes documents, Favoris, Téléchargement. De plus cette configuration cache le lecteur « C : ».

PC portable :

Pas de solution de sauvegarde officielle pour ce type de matériel.

6 – Navigateurs

Le navigateur Officiel du CHU de Toulouse est EDGE Chromium pour les terminaux Windows et Safari pour les terminaux Apple.
Les autres navigateurs utilisés au CHU sont Firefox ESR et Google Chrome Entreprise dans leurs dernières versions

7 – Client lourd

Dans le cas où la solution proposée nécessite l'installation d'un client lourd sur les machines clientes, l'éditeur doit être en capacité de fournir un fichier exécutable de type exe, msi ou autre format compilé capable de s'exécuter de manière autonome et silencieuse sur les OS compatibles citées plus haut.

8 – Périphériques

Dans le cas où la solution nécessite l'utilisation de périphérique de type imprimante, scanner ou douchette, elle devra être compatible avec au moins 3 marques différentes du type utilisés.