|  |  |
| --- | --- |
| P:\Etude BDD open source\Image PostgreSQL.PNG | **Offre de Service**  **PostgreSQL CORE**  **(GTS/RET)** |

# **PostgreSQL As A Service :**

**Merci de privilégier l’utilisation de PGaAS (** [**http://go/doitnow**](http://go/doitnow) **) avant d’utiliser l’offre Core décrite dans ce document.**

1. Introduction

L’offre de service est réalisée autour de la version Open Source REDHAT/CENTOS soumis à une licence libre Open Source similaire à une licence BSD ou MIT.

L’utilisation de cette base est conforme aux architectures C1 et 3A.

L‘OS éligible est LINUX RedHat/Centos (et non sur Windows ou IBM AIX)

PostgreSQL est une base de données relationnelle ayant vocation à proposer une alternative Open Source à Oracle RDBMS et à Microsoft SQL server.

L’offre est accessible pour les environnements de développement, d’homologation et de production.

1. Bénéfices – Avantages

* Mettre à disposition une solution alternative de base de données relationnelle à nos DSI partenaires par rapport aux éditeurs traditionnels (Oracle, Microsoft, IBM et SAP)
* Réduire nos coûts de licences tout en conservant un support
* S’adapter à un marché qui est en pleine évolution
* Langage SQL normalisée ANSI
* Architecture haute-disponibilité libre de droits

1. Bénéficiaires

L’offre est disponible pour tous les partenaires GTS/RET.

1. Comment faire une demande de création de base PGSQL ?

Suivre le lien suivant : <http://go/pgcreation>

1. Comment faire l’exploitation d’une base PGSQL ?

Suivre le lien suivant : <http://go/pgexploitation>

1. Offre de service
   1. Niveau de Support

Support produit

Support RedHat : Si la distribution PostgreSQL de RedHat est déployée, RedHat fournit alors un support ; ce support se limite à la fourniture de correctifs de sécurité sur la version.

Support Centos : Pas de support défini pour l’instant.

Support GTS : 7/7j, 24h/24h

* 1. Tarif

Build : Sur devis de l’équipe RET/MDB/DBA, à intégrer dans les coûts projet

Run : Sur le principe de -30% de l’offre Oracle

* 1. Niveaux de service technique
     1. Supervision

Supervision via KM Patrol commun (non fourni par BMC) depuis la console centralisée Patrol

* + 1. Sauvegarde

Une sauvegarde complète de la base est générée localement avec une rétention des deux dernières sauvegardes et ordonnancée sur Crontab.

**Il faut que chaque projet s’assure qu’une solution de sauvegarde externe est disponible sur ses machines PostgreSQL (contacter l’équipe Backup : RESG/GTS/IAS/SBS/RES ou l’équipe VM Cloud : RESG/GTS/IAS/CTS/RES)**

* + 1. Normes

Plage de port : TCP 12400 à 12420 (attention non inclus dans les bouquets pour le moment)

Nommage des DNS applicatifs : cf ce qui est fait pour Oracle.

Port 22 pour du logshipping

* 1. Cycle de vie

Politique de versions majeures, mineures et support étendu :

|  |  |  |  |
| --- | --- | --- | --- |
| Produit | Version majeure | Date de fin de support | Statut |
| PostgreSQL | 9.4 | 09/2019 | Disponible |
| PostgreSQL | 9.5 | 01/2021 | Disponible |
| PostgreSQL | 9.6 | 09/2021 | Disponible |
| PostgreSQL | 10 | 10/2022 | Disponible |

La politique de gestion de version du produit est décrite ici : <http://www.postgresql.org/support/versioning/>

Version packagée par Redhat via Software Collection

|  |  |
| --- | --- |
| Version BDD | Version OS |
| PostgreSQL 9.4.x | Red Hat/Centos 7.x via SCL |
| PostgreSQL 9.5.x | Red Hat/Centos 7.x via SCL |
| PostgreSQL 9.6.x | Red Hat/Centos 7.x via SCL |
| PostgreSQL 10.x | Red Hat/Centos 7.x via SCL |

L’installation des binaires est aussi disponible via HP-CSA.

Matrice de compatibilité complète : <https://www.postgresql.org/download/linux/redhat/>

* 1. Description des fonctionnalités disponibles

|  |  |
| --- | --- |
| Fonctionnalité | Statut |
| Exploitation : Installation / Sauvegarde / Supervision / Intégration à la CMDB du Concentrateur | Disponible |
| Jeu étendu de caractères | Disponible |
| Les migrations depuis Oracle avec ORA2PG | Disponible |
| Gestion des habilitations (locale à la BDD) | Disponible |
| Réplication distante | Disponible |
| La sécurité (Chiffrement du transport via SSL) | Disponible |
| Cryptage des données avec l’extension pgCrypto (Password Encryption/GPG Encryption) | Disponible |
| Automatisation de l’installation de Postgres et création de base de données standalone via HPCSA | Disponible |
| Authentification délégué à l’OS pour les batchs | Disponible |
| Pooling de connection avec PgBouncer | Disponible |
| Failover automatique mono-site avec Repmgr et Pgbouncer | Disponible |

* 1. Architectures disponibles

Typologie d’architectures disponibles :

* Standalone
* Réplication asynchrone avec du log shipping
* Réplication asynchrone en Streaming (avec ou sans failover automatique)

Le niveau de service sera assuré au niveau composant.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Standalone | Log shipping | RepMgr avec un witness et PgBouncer (\*\*) |
| RTO | 24h | RTO local/distant = 4 h (non automatique) | RTO local = 5 mn  RTO distant = 4h |
| RPO | 20 min (\*) | ~ 5 mn  Fonction du délai de latence de réplication (paramétrable) | ~ 5 mn  Fonction du délai de latence de réplication (mode de réplication Streaming) |
| Résilience locale | Non | Oui | Oui et automatique |
| Résilience distante | Non | Possible | Possible mais pas automatique |

(\*) Si TSM n’est pas disponible alors RPO de 24h.

(\*\*) RepMgr ainsi que PgBouncer ne sont pas inclus dans le support Redhat. Tout projet demandant à utiliser ces produits nécessitera une étude avec les architectes APS. Attention, le failover automatique ne garantit pas une synchronisation totale entre la primaire et les secondaires avant la bascule. Potentiellement, une perte de données doit être acceptable par le projet avant l’utilisation de cette fonctionnalité.

PgBouncer n’est utilisable que sur des VM Core.

* 1. Limites et Contraintes
* Criticité STAMP : les applications métiers qualifiées vitales ou critiques ne sont pas éligibles.
* Limites par rapport à la matrice DICP ((Disponibilité, Intégrité, Confidentialité, Preuve - <https://itim.safe.socgen/fr/analyse-de-risques> - <https://itim.safe.socgen/documents/5402732/12540873/ITIM-DARSP.docx>)

|  |  |  |  |
| --- | --- | --- | --- |
| D | I | C | P |
| 2 | 3  Pas de limite connue | 3 | Non défini, capacité d’audit à évaluer |

**ANNEXE**

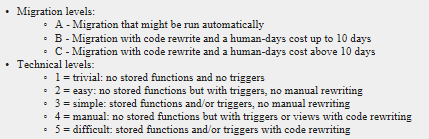
Pack DBA

Le pack DBA à destination des bureaux techniques est disponible. Il comprend les fonctions suivantes :

* Arrêt / démarrage de la base de données
* Sauvegarde complète de la base de données
* Sauvegarde des fichiers journaux (wal)

Outils de Migrations

L’outil ora2pg : Il est possible de générer un rapport avant migration afin de mesurer le taux de compatibilité et l’effort à produire pour migrer d’Oracle vers PostgreSQL. Le rapport évalue un niveau de complexité de migration suivant 2 axes :



Afin de mesurer l’effort de migration il est nécessaire de se rapprocher des équipes DBA étude.

L’outil EDB Migration Toolkit permet de migrer des bases :

* Oracle
* SQL Server
* MySql et
* Sybase

vers PostgreSQL en version communautaire ou en version PPAS (Postgres Plus Advanced Server) qui nécessite de contracter un support chez Entreprise DB afin de pouvoir utiliser cette version. Cette version PPAS utilise des OCI Oracle qui permettent de faciliter la [migration](http://www.enterprisedb.com/solutions/oracle-migration-assessment) et de rendre compatible plus d’objets qui proviennent d’une base Oracle et qui n’existent pas sur la version communautaire de PostgreSQL ([Dct](https://www.enterprisedb.com/docs/en/9.5/migrate/toc.html) de migration vers Postgres avec EDB Migration Toolkit).

Attention la migration de la base de données implique également de la réécriture côté code applicatif et ce de façon indépendante de l’outil choisi.

PgCrypto :

Il y’a deux mode de cryptage sur pgcrypto, one way et two way encryption. Dans le premier mode, seul le client possède le mot de passe qui permet de crypter/décrypter une donnée en md5 ou en crypt.

Le deuxième mode utilise une clé PGP public pour crypter les données et une clé PGP privé pour la décrypter. Le client doit être capable de fournir ces clés afin d’insérer ou de lire une donnée crypter. La base postgreSQL ne les héberge jamais et n’interagira pas avec le boîtier HSM.

Pour résumer, Le boîtier HSM doit pouvoir stocker les clés PGP et l’application doit être capable de les récupérer de ce boîtier lors de ces requêtes SQL.

Description des architectures :

|  |  |
| --- | --- |
|  | Architecture type avec un besoin d’hébergement dans une seule salle (résilience locale uniquement). La bascule sur le secondaire n’est pas automatique |
|  | Architecture type dual-room. La bascule sur le secondaire n’est pas automatique. |
|  | Combinaison des deux architectures ci-dessous. Le failover entre la primaire et le premier secondaire peut être automatisé avec repmgr. Cela dit la couche applicatif doit passer par une vip basculable ou un pgbouncer locale à la machine applicatif afin de rediriger les nouvelles connections au nouveau primaire. |