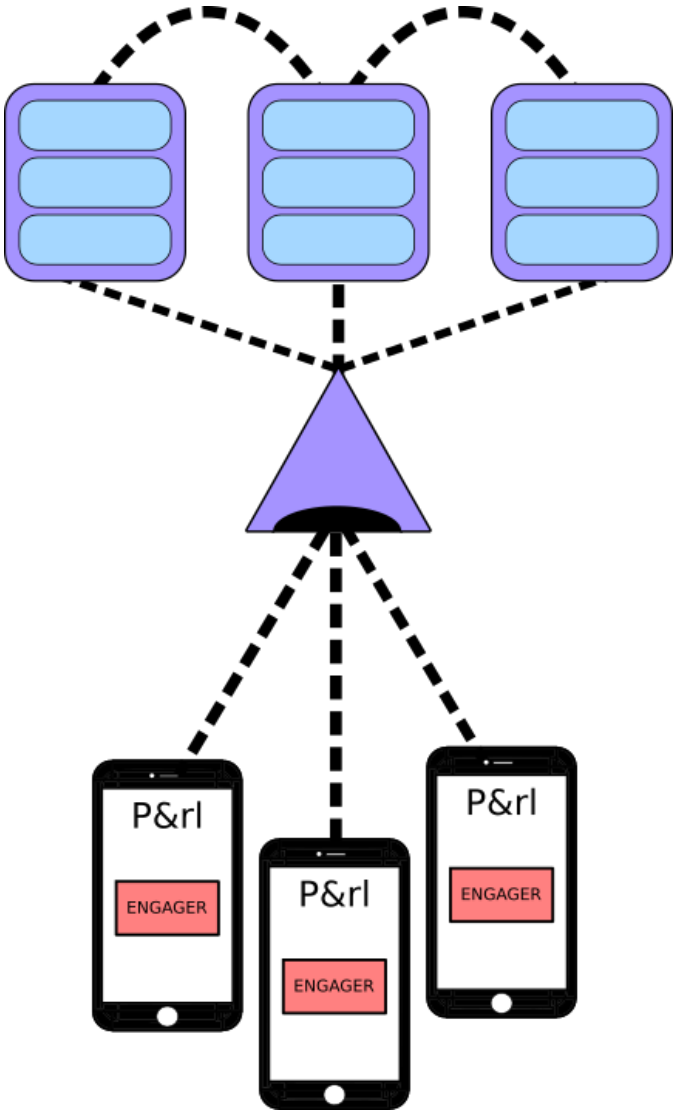
Système informatique de P&rl - ajouts 2021



Date : 08.06.2021

Examens 2021

Diplôme d'administrateur systèmes et réseaux

IDEC, Renens

Documentation des ajouts au
système informatique de P&rl
Solution de haute-disponibilité pour SQL Server

Conçu par *Alain Philip Despont*

1. Concept

1.1. Besoins de P&rl

La société P&RL de Paola Riggio-Liguri s'est bien développée et est devenue un modèle de start-up réussie en Romandie. L'entreprise est active du jet d'eau de Genève aux bords du Rhône, et emploie maintenant des milliers d'étudiants. Grâce à une application pour smartphones, les gens pressés peuvent d'un clic commander un service à P&rl qui leur envoie une *Perle* pour l'exécuter. P&rl a aussi rapatrié une partie des services hébergés à l'externe tel que le serveur web et le mail selon la volonté Mme Riggio-Liguri.

Grâce au catalogue complet et accessible par tout client potentiel par internet ou par l'application mobile, catalogue qui peut être agrandi au gré des créations des clients, P&rl bénéficie de commandes constantes. Mme Riggio-Liguri n'ayant jamais imaginé que son affaire marcherait aussi vite et bien, commence à recevoir des retours de clients qui se plaignent de la lenteur des opérations lorsqu'ils passent commande pour un service sur l'application mobile.

Après une étude des deux gestionnaires permanents du SI, Yohann Ferreiro et Phil Legrand, développeur de l'application mobile, le problème ne vient ni de l'application mobile, ni du réseau dont la bande passante est encore performante, mais du serveur hébergeant la base de données. Celle-ci est gérée par Bertrand Robert, un administrateur de base de données à temps partiel.

Mme Riggio-Liguri souhaite préparer l'avenir en augmentant la capacité de la base de données, assurer la sauvegarde des données de son entreprises, et organiser la gestion de la base de façon rationnelle. Un cahier des charges a été préparé avec Mme. Riggio-Liguri qui est résumé ci-après.

1.2. Cahier des charges

« Il faut augmenter et assurer la disponibilité à long terme pour les clients, je ne veux pas qu'ils attendent une heure pour réserver un service, c'est vital pour l'entreprise »

Exigences fonctionnelles :

- Configurer de nouveaux serveurs SQL.
- Assurer la tolérance de panne et la balance des charges sur l'application.
- Assurer une disponibilité maximum.

« J'ai de la concurrence et j'ai peur qu'on nous vole, ou pire, qu'on perdre nos clients et notre catalogue dû à un bug technique ou une panne. »

Exigences fonctionnelles :

- La base de données doit se répliquer sur un second serveur.
- La base de données doit être sauvegardée automatiquement à intervalle régulière.
- La sécurité doit être assurée aux niveaux des droits d'accès.

« L'administrateur de la base de données à fait le souhait de diminuer encore ses heures, j'ai peur qu'il parte et qu'on soit bloqué dans le futur. »

Exigences fonctionnelles :

- Aménager les rôles sur le serveur de façon sécurisée et ouverte aux changements.

1.3. Aide à la décision

En 2020, P&rl a décidé de rester sur une infrastructure OnPremises, soit sur place, Mme Riggio-Liguri préférant garder le contrôle sur l'infrastructure. Au vu des implications de la mise en place d'une nouvelle infrastructure informatique, il a fallu expliquer à Mme. Riggio-Liguri les possibilités et les implications de ce choix, ainsi que les solutions alternatives pour ce cahier des charges.

<table>
<tr><th>Exigences fonctionnelles</th><th>Solution
Sur site</th><th>Solution
Hybride</th><th>Solution
Cloud</th></tr>
<tr><td>Meilleure disponibilité du serveur SQL</td><td>Ajouter des serveurs supplémentaires</td><td rowspan="5">Machines virtuelles avec SQL Server sur le cloud Azure (IAAS)</td><td rowspan="5">Machine virtuelle
OU
Pool SQL partagé</td></tr>
<tr><td>Tolérance de panne du serveur SQL</td><td rowspan="4">Fonctionnalités incluses des serveurs existants (Clustering, Availability Group, job)</td></tr>
<tr><td>Réplication du serveur SQL</td></tr>
<tr><td>Sauvegarde régulière de la base de données</td></tr>
<tr><td>Balance de charge</td><td colspan="2">Réseau virtuel Azure</td></tr>
</table>

Sur site : Plus rapide à mettre en place, plus simple à entretenir avec les employés actuels. Il s'agit d'agrandir l'infrastructure en se basant sur l'existant. Coût plus important en matériel, mais maîtrise complète de l'infrastructure.

Hybride : Grâce à l'infrastructure louée, le coût d'entretien des serveurs peut être diminué et ajusté au pourcent près, les fonctionnalités du cloud Azure, pour ne citer que lui, permet de répondre à toutes les demandes liées à l'infrastructure SQL. Cependant, cela demande de mettre à jour les compétences des employés pour utiliser Azure. On notera tout de même un avantage certain vu le marché sur lequel l'entreprise se positionne, qui bénéficierai de l'élasticité d'une infrastructure cloud.

Cloud : Pari sur l'avenir, le cloud inquiète Mme Riggio-Liguri. En effet, et a raison, le périmètre de l'entreprise sort des cadres habituels. Cela impose certains coûts de migration et de formation des employés. Il faut aussi assurer par divers contrats de service, la performance des biens loués. En raison de la dynamicité de l'entreprise et des services qu'elle offre, le cloud se trouve en réalité totalement aligné avec les besoins de l'entreprise. En effet, on peut considérer le cloud comme une infrastructure rapide, élastique, et qui donc répond aux besoins modernes induis par les nouvelles plateformes comme l'application de Perl.

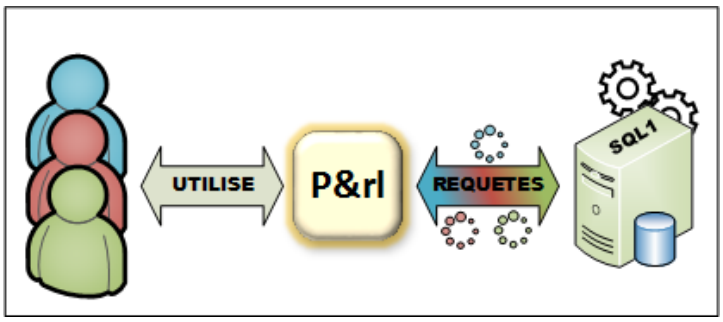
Solution	Rapidité de mise en œuvre	Fonctionnalités	Coûts
OnPremises	😊	+ +	+ + +
Hybride	☹	~	+ + ~
Cloud	☹	+ + +	~

1.4. Décision

P&rl a décidé de rester sur une infrastructure interne, privilégiant de faire avec qui existe déjà et de répondre au plus vite aux plaintes des clients. Le coût n'est pas un problème, l'entreprise est en essor et ils n'ont pas besoin de fonctionnalités supplémentaires offertes par le Cloud.

1.5. Infrastructure actuelle

L'entreprise possède plusieurs serveurs différents, dont un serveur SQL sur lequel toutes les requêtes provenant de l'application mobile atterrissent, le serveur étant au maximum de ses capacités il s'ensuit une latence pour les utilisateurs de l'application.



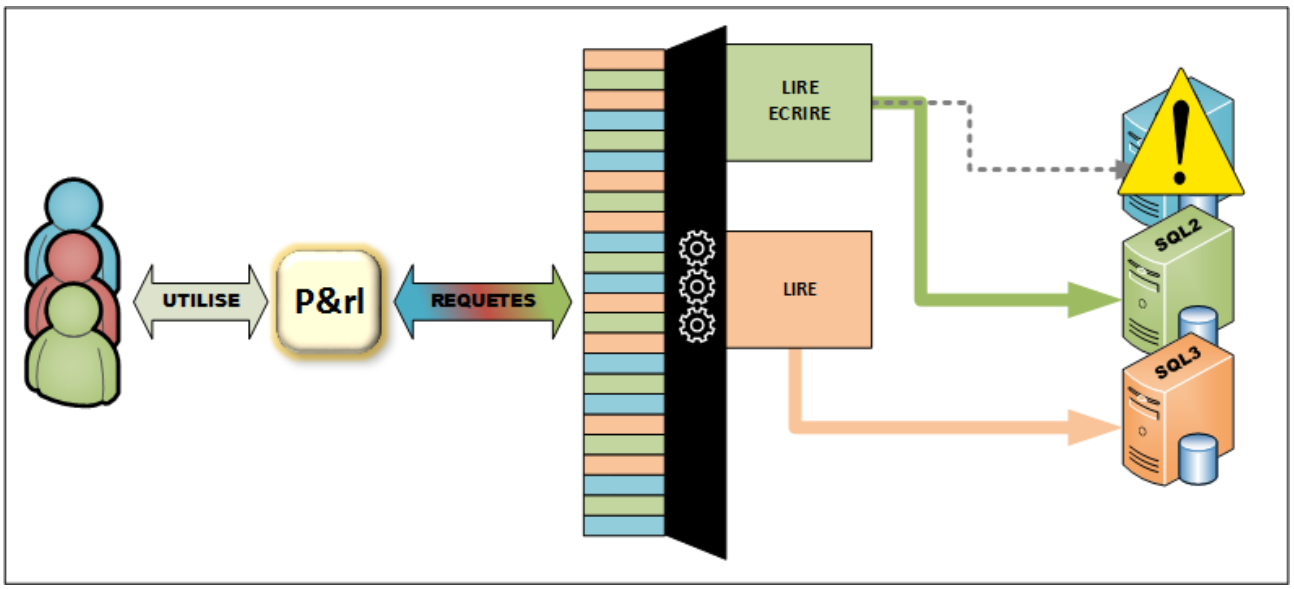
1.6. Concept d'infrastructure et schéma de principe

Pour répondre au cahier des charge et en respectant l'envie de rester avec une infrastructure sur site, je propose la mise en place des deux nouveaux serveurs SQL, le schéma ci-dessous expliquant le concept sous-jacent des « Groupes de disponibilité » de SQL Server.

Les groupes de disponibilités forment un ensemble proposant une seule entrée aux requêtes SQL (l'écouteur). L'écouteur se charge de recevoir et trier les requêtes selon leur entête (lire/écrire OU lire uniquement) et les transmets au serveur. Par exemple, un outil de Business Intelligence (BI) qui ne fait que de lire des données, n'ira pas surcharger le serveur de production puisqu'il n'a pas besoin d'écrire dans la base de données.

Ceci permettra d'alléger la charge sur le réseau en séparant une partie des requêtes sur le serveur adapté au travail demandé, tout assurant également une très haute disponibilité en assurant la réplication entre serveurs secondaires et le basculement (failover) si l'un des serveurs devait tomber.

Dans un tel cas, le serveur secondaire devient primaire (failover, synchrone), et le troisième serveur peut continuer à s'occuper des requêtes en lecture seule.



1.7. Variante d'infrastructure : le cloud

Comme expliqué à Mme Riggio-Liguri, pour répondre à la demande de disponibilité importante, on pourrait migrer une partie de l'infrastructure dans le cloud, ou plus simplement chez un hébergeur externe.

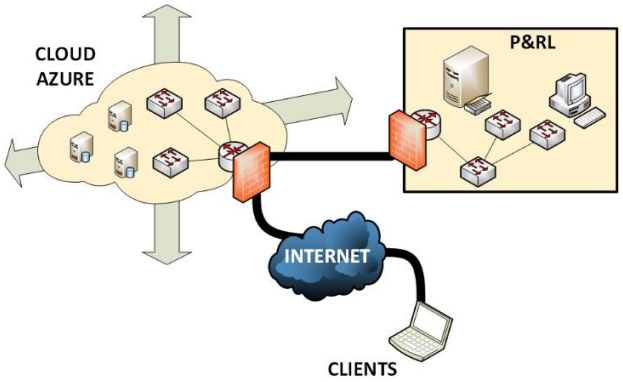
Le cloud Azure, par exemple, permettrait d'adapter très rapidement la capacité de la base de données SQL, ce qui permettrait de faire face à une demande accrue sans grands changements d'infrastructure. Il y'a le choix entre louer directement le serveur comme s'il existait physiquement (*SQL Server sur machine virtuelle*), ou louer directement un emplacement pour une base de données (*Azure SQL Database*), dans ce cas, il n'y a plus besoin de gérer le serveur, juste la base de données.

Etant donné le modèle d'entreprise de P&rl, il peut être très profitable d'opter pour un modèle *Azure SQL Database*. En plus de réduire les couts et les affiner à la demande réelle, la facturation est prévisible et peut être limitée pour éviter des trop gros pics. En terme simples, Perl louerait une « capacité » et y hébergerait ses données. Perl ne paierait que pour l'utilisation effective, c.à.d. lors d'une transaction : lorsqu'un client commande, s'enregistre, ou que l'on effectue une recherche dans la base de données.

Il n'y aurait plus besoin de serveur physique, et la redondance est inclue par défaut dans les produits Azure. Il faut cependant prendre toutes les précautions et ne pas mettre ses œufs dans le même nuage.A terme, le mail et le site internet de l'entreprise peuvent être également déployés depuis le cloud, dans une offre comme *Microsoft 365 Business*, qui, couplée avec *Power Plateform*, permet d'automatiser des processus d'entreprise, permettant de gagner du temps sur les opérations usuelles (mailings, facturation, appels des perles).

Le cloud Azure permettrait à P&rl de faire de substantielles économies, étant très dépendante des besoins et commandes fluctuants des clients. Cela coûterait moins cher à l'entreprise, que de déployer une lourde infrastructure au gré de son évolution.

Bénéfice supplémentaire, P&rl profiterait d'une sécurité accrue et d'une augmentation de bande-passante : le trafic client ne passant plus sur le réseau de P&rl, mais sur celui de *Microsoft Azure*, qui est extrêmement sécurisé, comme le sont les serveurs et centre de données de l'entreprise. Comme avec toutes les solutions Cloud, l'on peut résumer les avantages et inconvénients ainsi : gain de flexibilité et coûts prévisibles, contre le besoin d'employés qualifiés et le déplacement du périmètre de l'entreprise et la nécessité d'avoir un contrat solide avec le fournisseur de la solution.



2. Généralités

2.1. Résumé

En mars 2021 sur mandat de Perl, j'ai installé et configuré la mise en place d'une solution de haute disponibilité pour SQL Server selon le cahier des charges discuté avec Mme. Riggio-Liguri.
Ci-joint dessous un bref résumé des opérations effectuées et des faits, sur l'infrastructure de Perl.

1) **Infrastructure**
- Trois serveurs SQL ont été installés, avec la fonctionnalité *Cluster de basculement*.
- Un cluster de basculement a été créé pour joindre les serveurs et assurer le fonctionnement des *Groupes de disponibilité (Availability Group)* de SQL Server.
- Des remaniements des partages et d'unités d'organisations ont eu lieu.

2) **Sécurité**
- Les utilisateurs font partie de groupes globaux spécifiques à SQL Server.
- De nouvelles stratégies ont été mises en place et/ou modifiés.

3) **SQL Server**
- Les données de l'application, les logs transactionnels et la base tempdb sont sur des disques en Raid 1.
- Les sauvegarde et les bases utilisateurs sont sur des disques en RAID 5.
- Les sauvegardes et logs transactionnels sont déplacés automatiquement sur le NAS de l'entreprise à la fin du processus de sauvegarde.
- Jobs de maintenance et alertes permettent de surveiller l'infrastructure.

2.2. Limites d'application

La documentation du système se limite aux serveur AD1, SQL1, SQL2, SQL3, ainsi qu'au partages, groupes et utilisateurs et groupes modifiés, aux droits d'accès et rôles lié à l'application SQL Server, aux stratégies de groupes, ainsi qu'à la fonctionnalité de Windows Server : cluster de basculement et la fonctionnalité de SQL Server : *Groupes de disponibilité (Availability Group)*.

2.3. Plan des hôtes et entités logiques

Nom d'hôte complet	Rôle de l'hôte	Adresse IP
AD1.ad.perl.com	Serveur contrôleur de domaine principal DNS | DHCP	192.168.0.10
SQL1.ad.perl.com	Premier serveur SQL	192.168.0.11
SQL2.ad.perl.com	Second serveur SQL	192.168.0.12
SQL3.ad.perl.com	Troisième serveur SQL	192.168.0.13
ClusterSQL.ad.perl.com	Cluster rassemblant les trois serveurs SQL	192.168.0.30
SQLAlwaysOn1.ad.perl.com	Groupe de disponibilité SQL Server	
AGListener1.ad.perl.com	Ecouteur du groupe de disponibilité / point de terminaison, port 14000	192.168.0.31

3. Domaine AD

3.1. Nouveaux partages

La mise en place de nouveaux serveurs implique quelques changements dans les partages de l'entreprise P&rl. Principalement pour différencier les documents usuels, des documents du service informatique, ainsi que pour l'accès des applications (cluster et jobs de SQL Server).

Racines des dossiers				Chemin réseau	Contenu
NAS					
	Dossiers IT			\\AD1\Dossiers IT	
		DBA			
			Backup		Backups des bases de données
			Tools		Outils de base de données
		Sauvegardes			Sauvegardes des serveurs
			AD1…		
		Applications			Logiciels déployés
	Dossiers administratifs			\\AD1\Dossier administratifs	Documents de l'entreprise
	Dossiers perles			\\AD1\Dossiers perles	Documents pour les perles

3.2. Nouveaux groupes globaux

Les groupes globaux **glb_SQL_** sont utilisés pour l'accès à l'application SQL Server.
Cela permet à tous les membres d'un groupe (par exemple tous les développeurs) à se connecter à l'application et obtenir les mêmes droits.

Chaque groupe à un ensemble de droits sur les serveurs, sur les bases de données, et schémas spécifiques à SQL Server expliqué dans le chapitre 6 : Droits d'accès et rôles.

Compte AD	Groupe global	Fonction
AD/Administrateur	-	Administrateur système
AD/BeRo1	glb_SQL_Admin	Administrateur(s) de la base de données
AD/PhLe1	glb_SQL_Dev	Développeur(s) de l'application mobile
AD/YoFe1	glb_SQL_Operateur	Opérateur(s) de maintenance du serveur
SQL1, SQL2, SQL3	glb_SQL_Ordinateurs	Pour que les serveurs puissent copier les sauvegardes dans le dossier du NAS
AD/serviceMSSQL	-	Compte de service pour la gestion des groupes de disponibilité dans un domaine. Essentiel à la connexion entre répliques.

3.3. Arborescence du domaine et application des stratégies des groupes du domaine

ad.perl.com				
Arborescence des OU				Stratégies de groupes sur l'UO
PERL				**GPO_Securite_RenameAdmin**
	Groupes			
	Utilisateurs			**GPO_Securite_UsersPasswordPolicy**
		Superusers		**GPO_Securite_SuperusersPasswordPolicy**
		Administratifs		**GPO_Securite_NoCommandPrompt** **GPO_Securite_NoCustomSoftwareInstall**
		Perles		**GPO_Securite_NoCommandPrompt** **GPO_Security_NoCustomSoftwareInstall**
	Ordinateurs			**GPO_Securite_NoGuestAccount**
		Serveurs		**GPO_Securite_Audit** (GPO préexistante)
			Serveurs SQL	**GPO_Firewall_SQLPorts** **GPO_Securite_USBInterdit**
		Postes fixes		
		Postes mobiles		
	Imprimantes			
	Partages			

3.4. Stratégies de groupe du domaine

Stratégies d'applications et utilisateurs

GPO_Deploy_LecteurMappé	Ajout d'un lecteur Z pour les Dossiers IT pour le service informatique

Stratégies de sécurité globale

GPO_Securite_NoCommandPrompt	Désactive le command prompt chez les utilisateurs.
GPO_Securite_NoCustomSoftwareInstall	Empêche l'installation de logiciels chez les utilisateurs.
GPO_Securite_NoGuestAccount	Désactive le compte invité sur les machines et le renomme.
GPO_Securite_UsersPasswordPolicy	Politique de mot de passe pour les utilisateurs (min 12 caractères).
GPO_Securite_SuperusersPasswordPolicy	Politique de mot de passe pour les super-utilisateurs (min 14 caractères).
GPO_Securite_RenameAdmin	Renomme le compte administrateur local.

Stratégies spécifiques à SQL Server

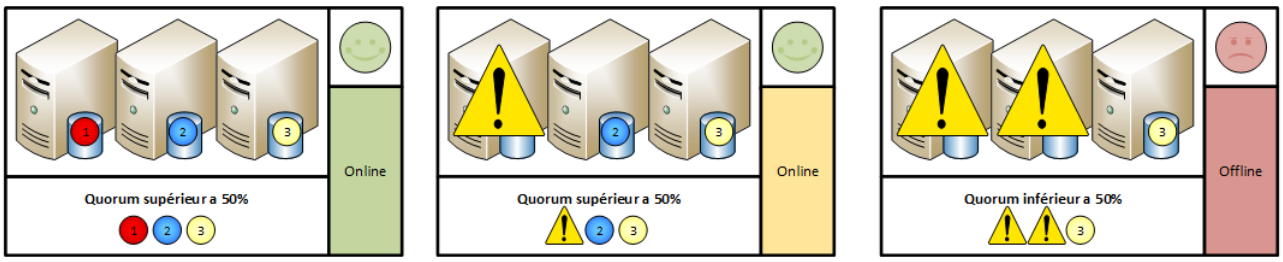
GPO_Firewall_SQLPorts	Ouvre les ports pour les accès SQL Serveur et le mail SQL TCP 5022, 1433, 1434, UDP 1434 TCP 25 ouvert sortant, fermé entrant
GPO_Securite_USBInterdit	Désactive les lecteurs externes (USB, CD).

4. Cluster de basculement et Groupes de disponibilités

4.1. Schéma de fonctionnement du cluster de basculement

Lorsqu'un hôte appartenant à un cluster de basculement devient hors-service, les hôtes restants peuvent voter pour reprendre le rôle et assurer la disponibilité d'un service.
Si le total des votes est inférieur à la moitié du total d'hôtes, le cluster se met hors ligne.

- Le cluster bascule automatiquement lors de défaillance.
- Le client ne voit qu'un seul serveur à la fois.



4.2. Configuration du cluster de basculement

Le cluster ne demande aucune configuration particulière, il faut créer le cluster et joindre les trois machines.

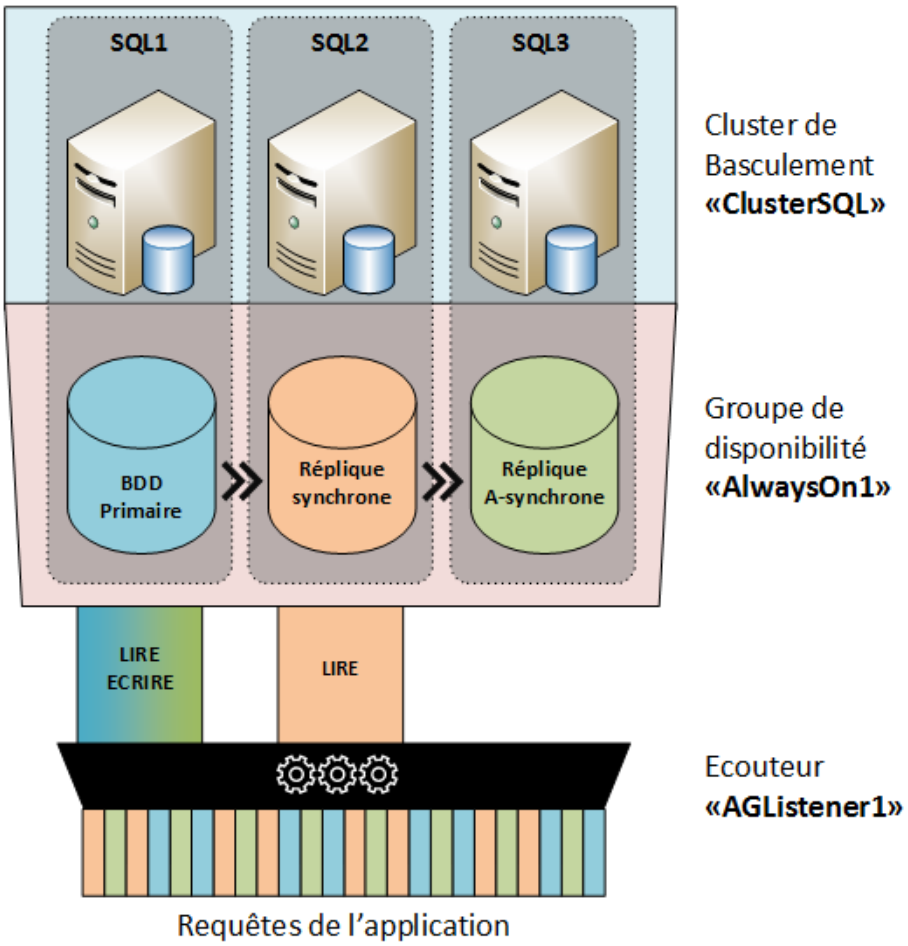
Quorum

- **[Cas actuel]** Sur un cluster à nœud impair, le droit de vote ne nécessite pas de témoin.
- Sur un cluster à nœud pair, il faut configurer un témoin de vote via un dossier partagé.
    - Gestionnaire du cluster de basculement, actions
    - Autres actions, configurer les paramètres du quorum de cluster

4.3. Schéma de fonctionnement des groupes de disponibilité SQL Server

Les groupes permettent la réplication, synchronisation et équilibrage de charges de SQL Server et ne peuvent être mis en place que dans un cluster de basculement.

- C'est un cluster de basculement propre à SQL Server.
- Il assure la réplication synchrone et asynchrone des bases de données sélectionnées.
- Il permet la balance de charge du réseau en partageant les requêtes de lecture et écriture sur un serveur disponible.
- Il fournit un seul point de contact pour les applications (Ecouteur).



4.4. Configurations des groupes de disponbilité "AlwaysOn"

- La machine **ClusterSQL** doit rester dans l'OU **Computers.**
- Autoriser *Validated write to MS DS Additionnal DNS Host Name* à **ClusterSQL** sur **AGListener1**

Instance	Rôle	Failover automatique	Synchronisation automatique	Lecture seule
SQL1	Primaire	OUI	Synchrone	NON
SQL2	Secondaire	OUI	Synchrone	OUI
SQL3	Secondaire	NON	Asynchrone*	OUI

* Il n'attendra pas de confirmation de livraison des données, solution d'urgence après sinistre

4.5. Point d'accès au groupe de disponibilité et accès individuels

A fournir aux applications externes [dont SSMS]

AGListener1	192.168.0.31:14000
SQL1 Endpoint	TCP://SQL1.ad.perl.com:5022
SQL2 Endpoint	TCP://SQL2.ad.perl.com:5022
SQL3 Endpoint	TCP://SQL3.ad.perl.com :5022

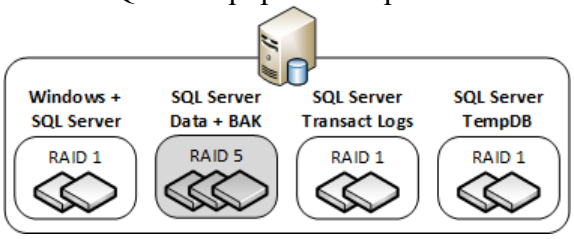
4.6. Propriétés du groupe de disponibilité : Read-Only Routing

SQL1	TCP://SQL1.ad.perl.com:1433	SQL2
SQL2	TCP://SQL2.ad.perl.com:1433	SQL1
SQL3	TCP://SQL3.ad.perl.com:1433	

5. SQL Server

5.1. Disques et redondance raid

Afin d'accroitre la capacité de récupération physique des données, et comme sécurité supplémentaire, chaque serveur SQL est équipé de disques en raid 1 ou 5.



Formatage : NTFS, 64Ko d'unité d'allocation

Avantages du RAID 1	Inconvénients
Possibilité de perdre un disque.	Si perte du second disque, perte complète des données
Rapidité de la lecture des données.	Ecriture plus lente (doit écrire deux fois)
Avantages du RAID 5	**Inconvénients**
Possibilité de perdre un disque.	Si perte des 2/3 des disques, perte complète des données.
Possibilité de reconstruire les données	Ecriture plus lente (écriture de la parité)

5.2. Configuration SQL Server Manager

Configuration identique sur chaque serveur, pour les configurations, jobs, alertes, mails…

SQL Server Services			
SQL Full-text Filter	Automatic (**différé**)*		
SQL Server (MSSQL)	Automatic (**différé**)	Log as **AD/serviceMSSQL**	Enable Always On
SQL Server Browser	Automatic (**différé**)		
SQL Server Agent	Automatic (**différé**)		

* A modifier dans services.msc

SQL Server Network + SQL Native Client
Tous les protocoles ENABLED

5.3. Sauvegarde de la base de données SQL

Dans une installation individuelle de SQL Server, il n'existe qu'un ensemble de fichiers de base de données et de logs à sauvegarder. **Dans un groupe de disponibilité, il existe autant de copies de ces fichiers que de serveurs répliqués (réplication inter-serveurs).**

La sauvegarde s'effectue :

- Sur le serveur ayant le rôle PRIMARY uniquement, et sur le disque local.
- Job: 1_Full Backup *(Sauvegarde complète chaque lundi minuit)*
- Job: 2_Differential Backup *(Sauvegarde complète et différentielle chaque 2h)*
- Job: 3_TransactLog Backup *(Sauvegarde des transactions chaque 15 minutes)*

Step 1 - Script de vérification :
Source : https://stuart-moore.com/making-sql-agent-jobs-availability-group-aware-with-dbatools/

Soit le step échoue avec succès (ce n'est pas le primary) soit il réussit et passe au prochain step.

```
IF (SELECT
repstate.role_desc
FROM sys.dm_hadr_availability_replica_states repstate
INNER JOIN sys.availability_groups ag
ON repstate.group_id = ag.group_id AND repstate.is_local = 1) != 'Primary'
BEGIN
RAISERROR ('Not Primary', 2, 1)
END
```

Step 2 -Scripts des jobs de sauvegarde :

FULL BACKUP

```
BACKUP DATABASE
master
TO DISK
='D\backup\1_Full
Backup\FullBackup_master
.BAK
GO
```

DIFFERENTIAL BACKUP

```
BACKUP DATABASE
master
TO DISK ='D\backup\2_Diff
Backup\DiffBackup_perl_db
.BAK
WITH DIFFERENTIAL
GO
```

TRANSACTION LOG

```
BACKUP LOG perl_db
TO DISK
='D\backup\3_TransactLogs\TransactLog_perl
_db.BAK
GO
```

Step 3 – Script powershell de déplacement sur le NAS:

```
# Variables de date
$mois = get-date -uformat %m
$jour = get-date -uformat %d
$annee = get-date -uformat %y

# Fichiers de backup à déplacer
$Source = "D:\backup\1_Full Backup"
$Destination = "\\AD1\Dossiers IT\DBA\Backups\1_Full Backup_"+"$jour."+"$mois."+"$annee"

# Copie des fichiers dans la destination
Robocopy $ource $Destination * /e /r:1 /w:1
```

5.4. Droits d'accès au logiciel SQL Server

La stratégie d'authentification de SQL Server utilise l'authentification Windows, et donc permet d'authentifier et régir les droits des utilisateurs du domaine selon leur groupe global (ou local si besoins très spécifiques).

Login SQL accordé à | sur SQL1, SQL2, SQL3	Sans login
glb_SQL_Admin glb_SQL_Dev glb_SQL_Operateur AD/Administrateur AD/serviceMSSQL	Utilisateurs du domaine hors des groupes SQL prévus

6. Droits d'accès et rôles

6.1. Rôles de serveur SQL

LOGIN ET ROLES DE SERVEUR DOIVENT ETRE INSCRITS SUR CHAQUE SERVEUR

L'*administrateur* possède tous les droits pour gérer le serveur SQL.
L'utilisateur *serviceMSSQL* a seulement besoin d'un login pour gérer le groupe de disponibilité.
Les opérateurs (service informatique) peuvent faire des opérations d'entretien, comme sauvegarder les bases de données ou gérer les processus du serveur.

	Administrateur	glb_SQL_Admin	serviceMSSQL	glb_SQL_Dev	glb_SQL_Operateur
Bulkadmin					
Dbcreator					**X**
Processadmin					**X**
Public	**X**	**X**	**X**	**X**	**X**
Securityadmin					
Serveradmin					**X**
Setupadmin					
Diskadmin					**X**
Sysadmin	**X**	**X**			

6.2. Rôles sur la base de données SQL

Le développeur peut lire et écrire sur la base de données. Les opérateurs peuvent créer des bases de données et les sauvegarder uniquement.

	Administrateur	glb_SQL_Admin	glb_SQL_Dev	glb_SQL_Operateur
Db_owner	X	X		X
Db_securityadmin	X	X		
Db_accessadmin	X	X		
Db_backupoperator	X	X		X
Db_ddladmin	X	X	X	
Db_datawriter	X	X	X	
Db_datareader	X	X	X	
Db_denydatawriter				
Db_denydatareader				

6.3. Permissions sur les schémas

Les schémas servent de fiche de contrôle d'accès a plusieurs objets, cela permet d'assigner des règles spécifiques à certains objets, comme une base de données, une table, ou un champ spécifique.

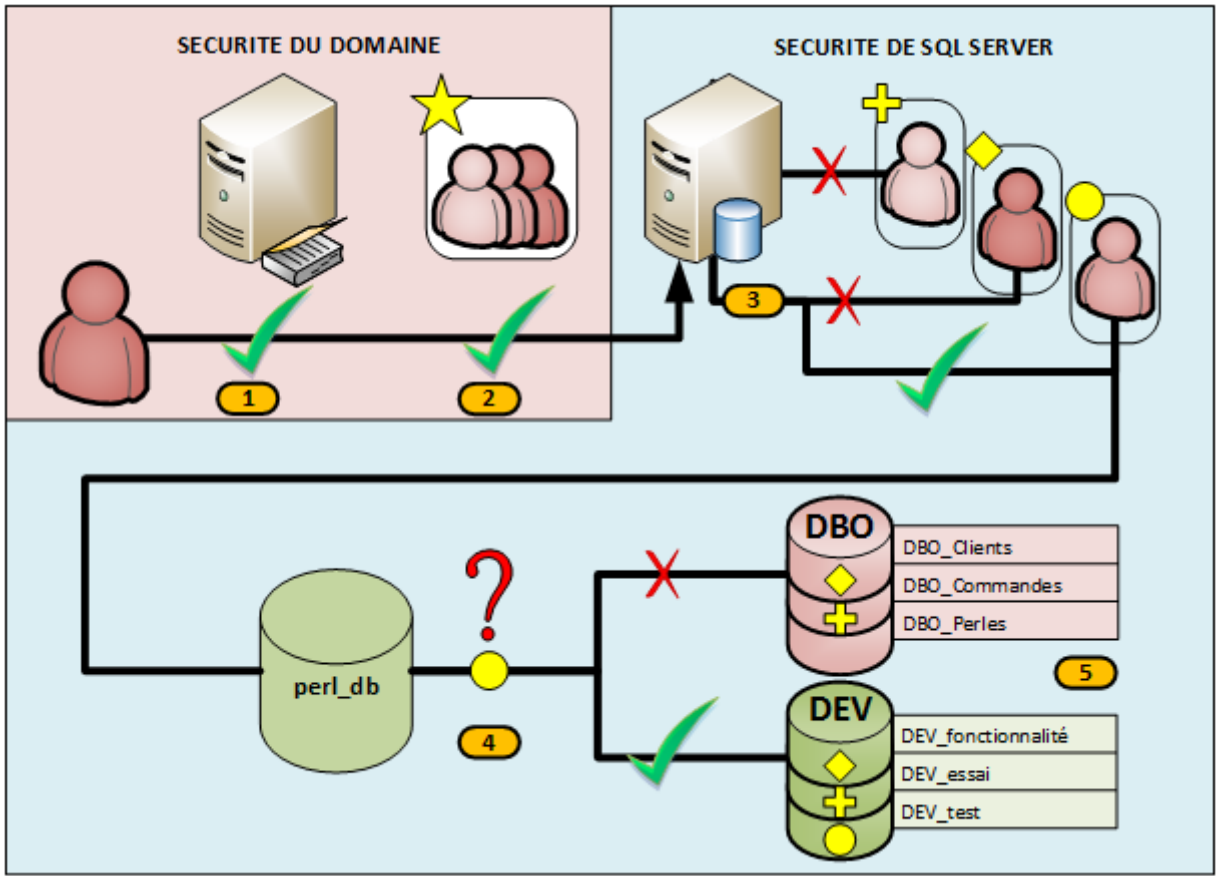
dbo	dev
Schéma de production, contient les bases de données en service. **Inaccessible aux développeurs.** = Permissions sur le schéma dbo = deny all	Schéma de tests et développement de nouvelles solutions. **Accessible aux développeurs.** = Permissions sur le schéma dev = grant all

6.4. Ressources et droit d'accès des groupes globaux d'utilisateurs du domaine

Groupes globaux	glb_SQL_Admin	glb_SQL_Dev	glb_SQL_Operateur	glb_SQL_Ordinateurs	Ordinateurs du domaine	Groupes locaux
Applications	**RWX**	**RWX**	**RWX**		**RWX**	**loc_ApplicationsIT**
DBA	**RWX**	*-Afficher-*	*-Afficher-*	*-Afficher-*		**loc_dbaRWX**
Backups			**RWX**	**W**		**loc_dbaBackupRWX** **loc_dbaBackupW**
Tools		**RWX**	**RWX**			**loc_dbaToolsRWX**
Sauvegardes	*-Afficher-*		*-Afficher-*			**loc_SauvegardesRWX**
AD						
SQL	**RWX**		**RWX**			**loc_SauvegardesSQL**

6.5. Sécurité de l'accès au serveurs et données

L'accès aux données passe par plusieurs couches :



1) Utilisateurs authentifiés du domaine

Seuls les utilisateurs authentifiés du domaine peuvent accéder aux ressources du domaine.

2) Groupe global spécifique à l'application

Voir *: Droits d'accès au logiciel SQL Server*

Seuls les utilisateurs appartenant à un des groupes globaux ayant un login sur SQL Server, peuvent se connecter à l'application SQL Server (*Authentification Windows de SQL Server*).

3) Rôles

Voir : *Rôles de serveur SQL*, *Rôles sur la base de données SQL*

Une fois connecté au serveur SQL, les utilisateurs obtiennent un rôle particulier sur l'application (admin, développeur, opérateur).

En plus de pouvoir se connecter (login), ils peuvent effectuer des actions (rôles sur le serveur, rôle sur les bases de données).

4) Schémas de sécurité

Un schéma de production (dbo) et un schéma de développement (dev) garanti que certaines parties de la base de données soient bloquées selon les rôles.

5) Non applicable – Permissions

Il est possible d'affiner le contrôle via des permissions spécifiques sur des tables, colonnes ou champs spécifiques, ce qui n'a pas été mis en place dans cette solution.

7. Sécurité de l'infrastructure

7.1. Analyse de la sécurité et propositions d'améliorations

Identité et rôle
La sécurité actuelle repose sur la bonne attribution aux groupes définis dans l'Active Directory. L'identité des utilisateurs est assumée être correcte et leur rôle leur alloue un champ d'utilisation défini sur le système et sur les applications.

Assumer que l'identité de l'utilisateur est toujours correcte n'est plus une protection suffisante. Dans une optique moderne il faut assumer que chaque connexion est une intrusion, et s'assurer par plusieurs moyens que celle-ci est légitime. Je propose qu'à l'avenir P&rl mette en place une solution d'authentification double (MFA) via un fournisseur cloud comme Azure.

Pare-feu
P&rl a bien configuré les pares-feux de chaque machine dans le périmètre de l'entreprise, cependant le domaine reste vulnérable. Je propose donc de mettre en place une solution de pare-feu applicatif à l'entrée du domaine de l'entreprise afin de réduire la surface d'attaque à celui-ci et de pouvoir mieux contrôler les flux liés aux applications entrants.

Proxy
Dans une optique de sécurité mais aussi de performance, je propose la mise en place d'un serveur de proxy, afin de faire l'intermédiaire entre l'application mobile et l'écouteur lié au groupe AlwaysOn.

Stratégies
Les stratégies de sécurisation sont basiques mais devraient limiter les possibilités d'une attaque conventionnelle et/ou interne.

Sauvegarde
En l'état actuel, toutes les données de l'entreprise sont à risque puisqu'elles sont toutes dans le même bâtiment. Il faut absolument sortir les données de l'entreprise et du NAS, organiser une procédure de sauvegarde 3-2-1 (trois copies, deux supports différents, dont un à l'extérieur de l'entreprise). Si localement les serveurs SQL ont une redondance des données physique (RAID5) et logicielle (Réplication AlwaysOn), les sauvegardes se font sur un NAS à quelques mètres.

Je propose dans un premier temps de mettre en place une procédure de sauvegarde externe dans le Cloud, pour assurer un troisième niveau de sauvegarde (2 locale, 1 externe), puis dans un deuxième temps, de faire sortir le NAS des locaux de P&rl. Une solution supplémentaire sur bande serait bienvenue.

7.2. Risques résiduels

Vulnérabilités	Mesures à mettre en place
Identité volée	Identification multi-facteur
Pénétration du domaine	Pare-feu applicatif, détection d'intrusions
Attaques par déni de service	Serveur de proxy
Malveillance interne	Stratégies d'audit, contrôle stricte des machines
Catastrophes naturelles	Extraction des données des locaux de l'entreprise