PSA PEUGEOT CITROËN

Déploiement de l'infrastructure SOA

Retour d'expérience

Août 2013

Agenda

- **Contexte et constats**
  - Existant chez PSA
  - Cible du chantier SOA
  - Passerelle de sécurisation des services
- Les offres de service de la Passerelle
  - Fonctions principales
  - Exemple d'offre de service
- Les contrats de service
  - Contrats applicatifs
  - Contrats techniques
- IBM Datapower XC10
  - Description
  - Test de la solution de cache SOA

Contexte et constats

Ouverture vers l'extérieur

- Une multiplication des besoins du 'canal' internet :
  - De nombreux projets concernés : Citroën.<pays>, pages perso, etc.
  - Des prises de service des sites Internet vers le SI de front et de back office à destination des réseaux de distribution, des entités/filiales et centrales
  - Des prises de service du navigateur vers les sites web PSA
  - Des prises de service depuis des applications partenaires hébergées à l'extérieur

Urbanisation du SI

- Un plan d'urbanisation du SI Commerce est envisagé chez PSA
- Objectif : rationnaliser le SI et, à terme, mettre en place une architecture mutualisée permettant :
  - Un échange de flux entre systèmes au fil de l'eau
  - Un monitoring et un suivi des flux efficaces

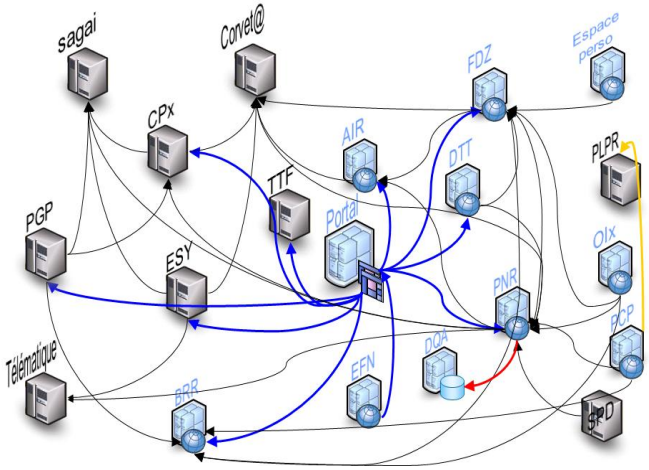
Risques

- Des risques liés à internet
  - Activité / charge non prévisible de façon fiable
  - Sécurité
  - Maîtrise des indisponibilités des systèmes en back end (plages de disponibilités, incidents…)
- Des risques liés à la mutualisation
  - La complexification de l'architecture
  - La cohérence entre les études menées et l'infrastructure sous-jacente

Existant chez PSA

Portail du « service après-vente"

- L'« après-vente » est une activité primordiale dans le système d'information de PSA
  - ✓ Les applications liées à cette activité sont accessibles depuis un portail web par plus de 90000 personnes chaque jour
  - ✓ Les applications communiquent entre elles via des prises de service :
    - Un appel sur le portail web se traduit par l'appel d'une application interne exposant des services nécessaire au portail
    - Ces services sont eux-mêmes clients d'autres services hébergés par des applications en back-end



Le constat

- La complexité des échanges entre applications et la volumétrie des prises de service conduis à des **dysfonctionnements** dans des périodes de pics de charge
- Le SI ne répond plus aux **exigences de sécurité et disponibilité**

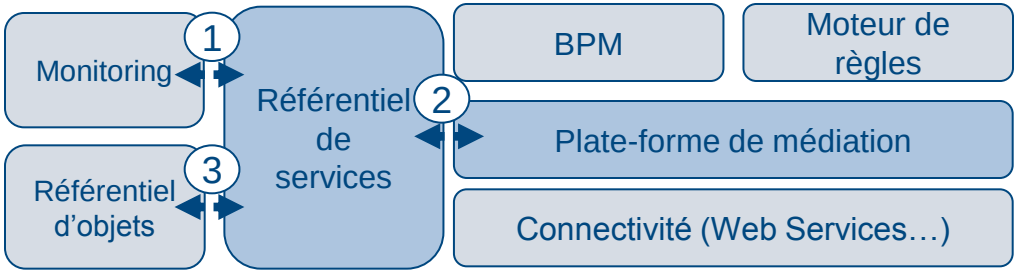
Enjeux PSA

- Assurer une **ouverture organisée et sécurisée** de son SI vers l'extérieur
- **Allier** à la fois **les enjeux des consommateurs et des fournisseurs** de service. Une offre de service favorisant une application aux détriments d'une autre pourrait ralentir de manière significative l'adhésion autour de la passerelle de sécurisation.
- Assurer une **régulation du trafic en production** en évitant les pics de charge mettant en danger les serveurs du back end

Approche SOA

Positionnement des différentes briques dans une approche SOA

- **Dans une architecture de service, la multiplication des services et l'ouverture du SI aux partenaires impliquent une normalisation de l'accès aux services.**
  - Afin de contenir la bonne gestion des services, de garantir leur interopérabilité et leur pérennité, il faut mettre en place une brique transverse rationnalisant l'usage de ces services.
- **Notre vision de la composition du socle technique SOA est la suivante :**
  - **Le référentiel** constitue un des éléments favorisant **la gouvernance des services.** Au delà de la fiche d'identité du service, ce référentiel doit contenir les contrats associés (de niveau de service, de fraicheur de la donnée) ainsi que les règles d'accès en termes de sécurité.
  - **La plate-forme de médiation**, couche d'intermédiation, orchestre les services et **fédère leur accès.**



1. Remontée des informations de monitoring (Temps de réponse, respect des contrats de services, alertes…)
2. Application des règles RunTime configurés dans le référentiel de services.
3. Synchronisation des métadonnées liées aux services, applications, consommateurs, fournisseurs…

Référentiel

Axes d'amélioration

Visibilité des services

- Référentiel **centralisé** des services
- **Documentation** pour un premier niveau de découverte
- Support de **l'animation** autour des services

Maîtrise de l'infrastructure

- **Cartographie** de l'implémentation des services
- Cartographie des **dépendances** Producteurs-Consommateurs
- **Suivi** de l'activité

Gestion de la relation Producteur-Consommateur

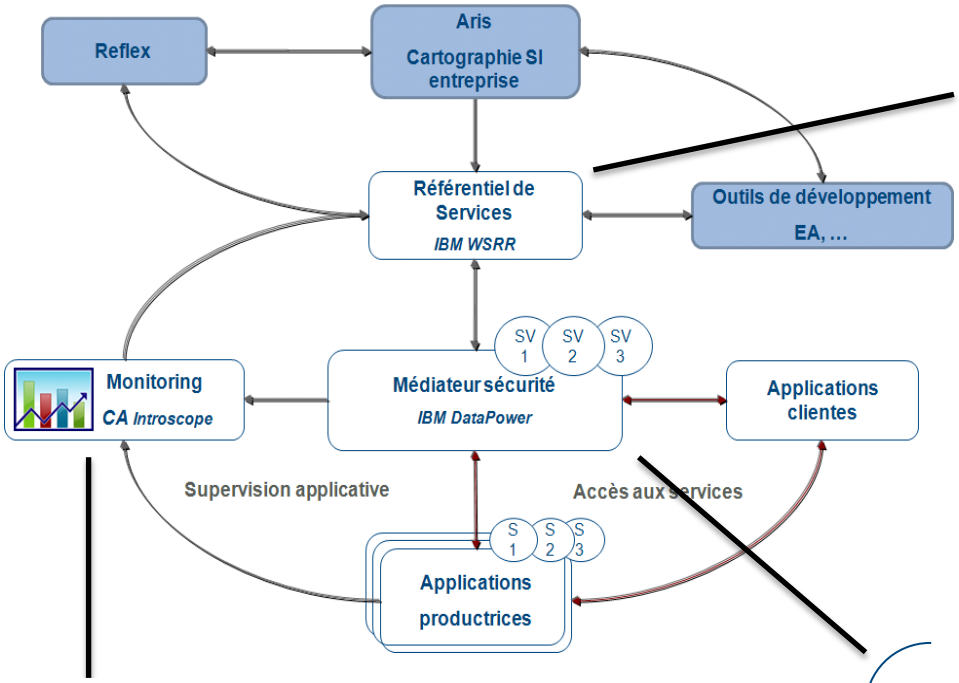
- Gestion du **cycle de vie** du service
- Aide à la relation (premier pas vers des « CNF » des **services réutilisables**)

Qualité des services

- Eligibilité technique & fonctionnelle
- Règles de développement / règles de sécurité / respect normes & méthodes

Cible du chantier SOA

- Proposer une gouvernance de la SOA basé sur un ensemble de briques techniques



Référentiel des services WEB

- Dresser la **cartographie** de tous les services WEB disponibles ou en cours de réalisation
- Fournir une cartographie des applications fournissant une implémentation "technique" d'un service métier
- Améliorer la **relation entre producteurs et consommateurs** (gestion des contrats de partenariat, gestion des mécanismes de notifications…)
- Proposer un outil d'**analyse d'impact** lors de la modification d'un service
- Gérer le **cycle de vie** des services

Monitoring

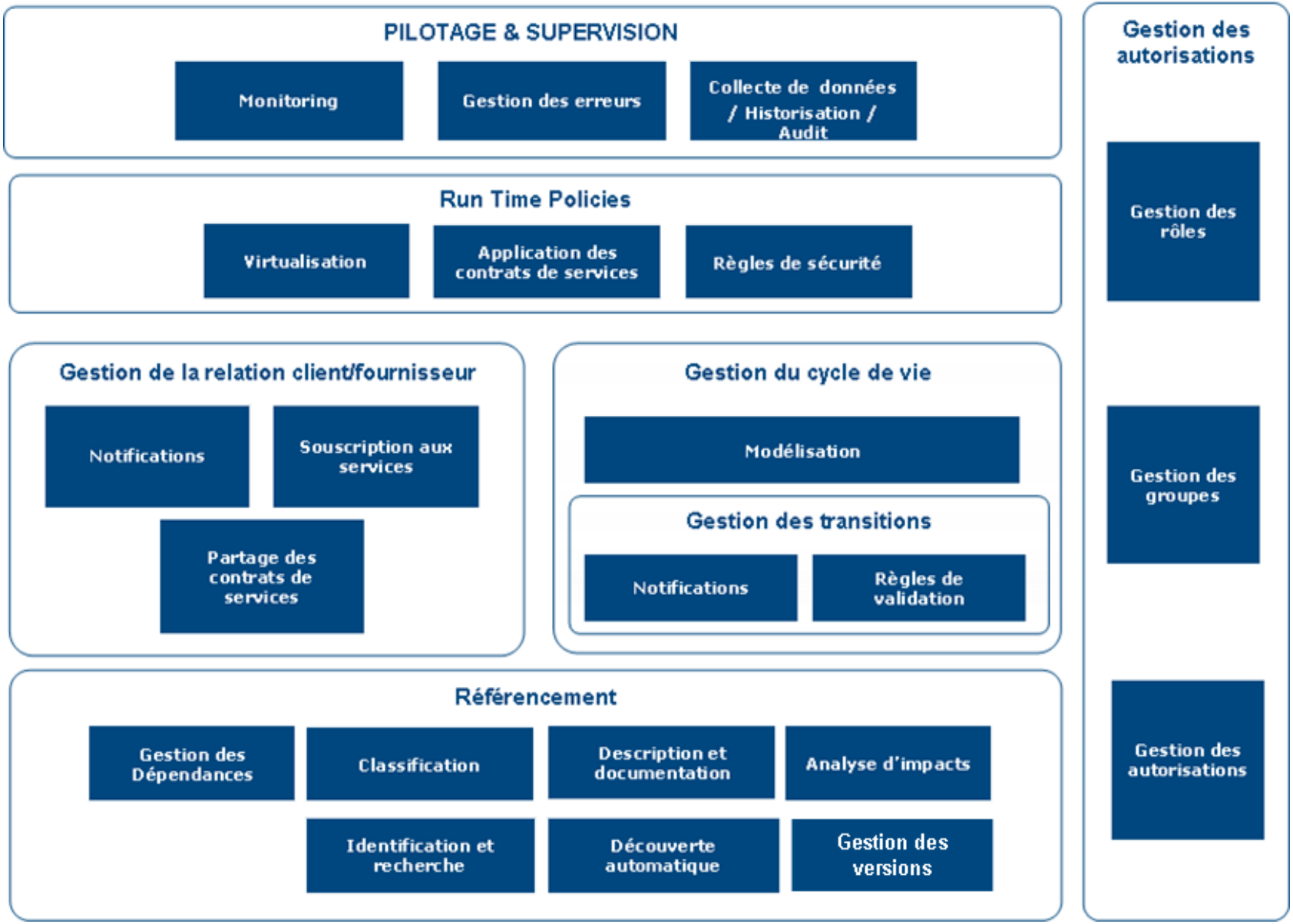
- **Superviser** les services
- **Gérer les alertes** sur l'atteinte ou le dépassement de seuils de consommation
- **Réconcilier** la cartographie "déclarative" du référentiel des services avec la cartographie "réelle" basée sur la consommation effective de services

Médiateur orienté Sécurité

- **Gérer les échanges XML** entre les différentes zones réseaux (DMZ – SGP – Intranet)
- Identifier le consommateur et vérifier ses **habilitations** pour l'accès au service Web demandé
- **Faire respecter les contrats** définis entre le client et le fournisseur de service au niveau du référentiel de services WEB
- **Bloquer la consommation** d'un service sans définition préalable d'un contrat
- **Renforcer la sécurité** des flux XML

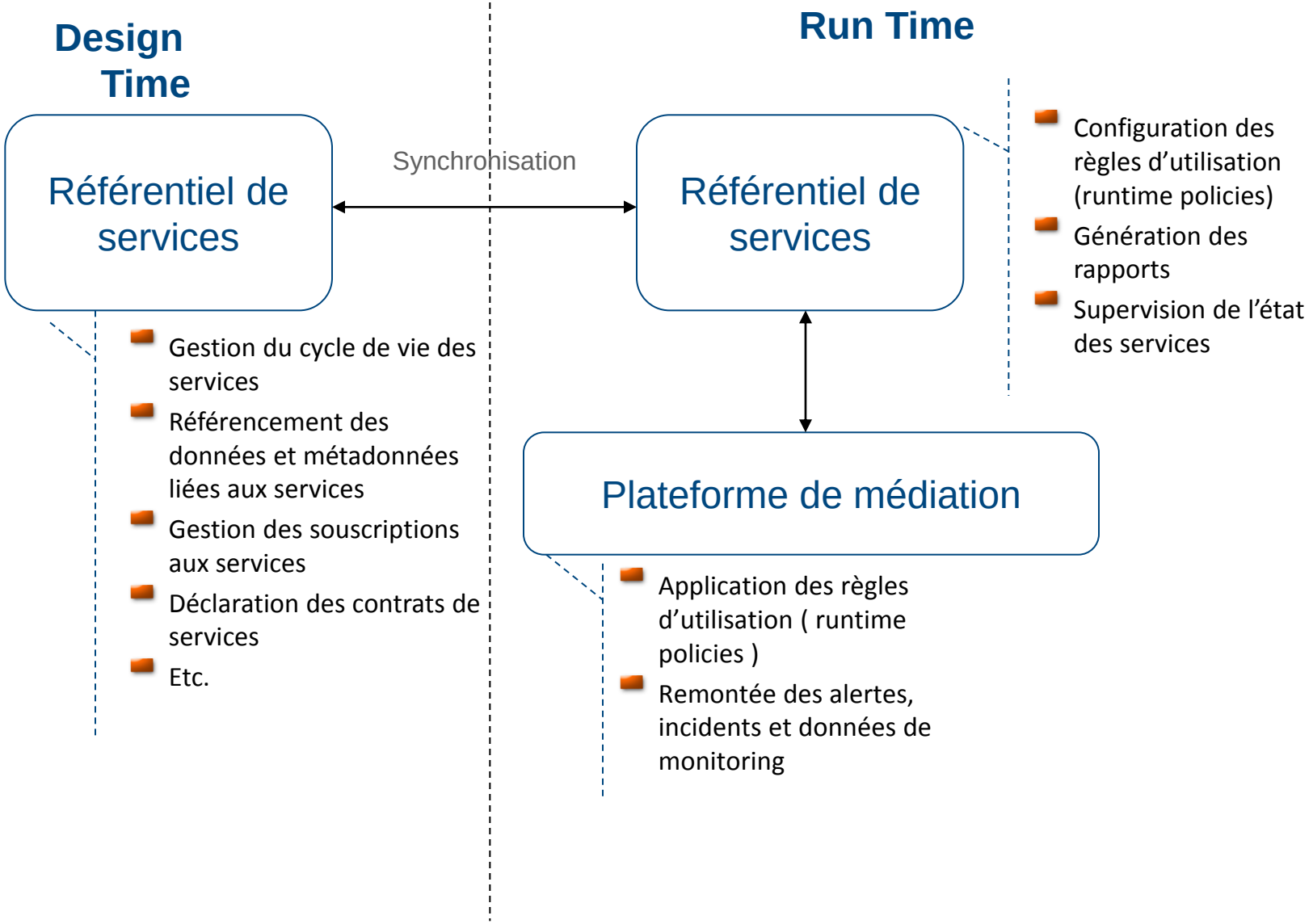
Référentiels de services

Fonctionnalités à l'état de l'art



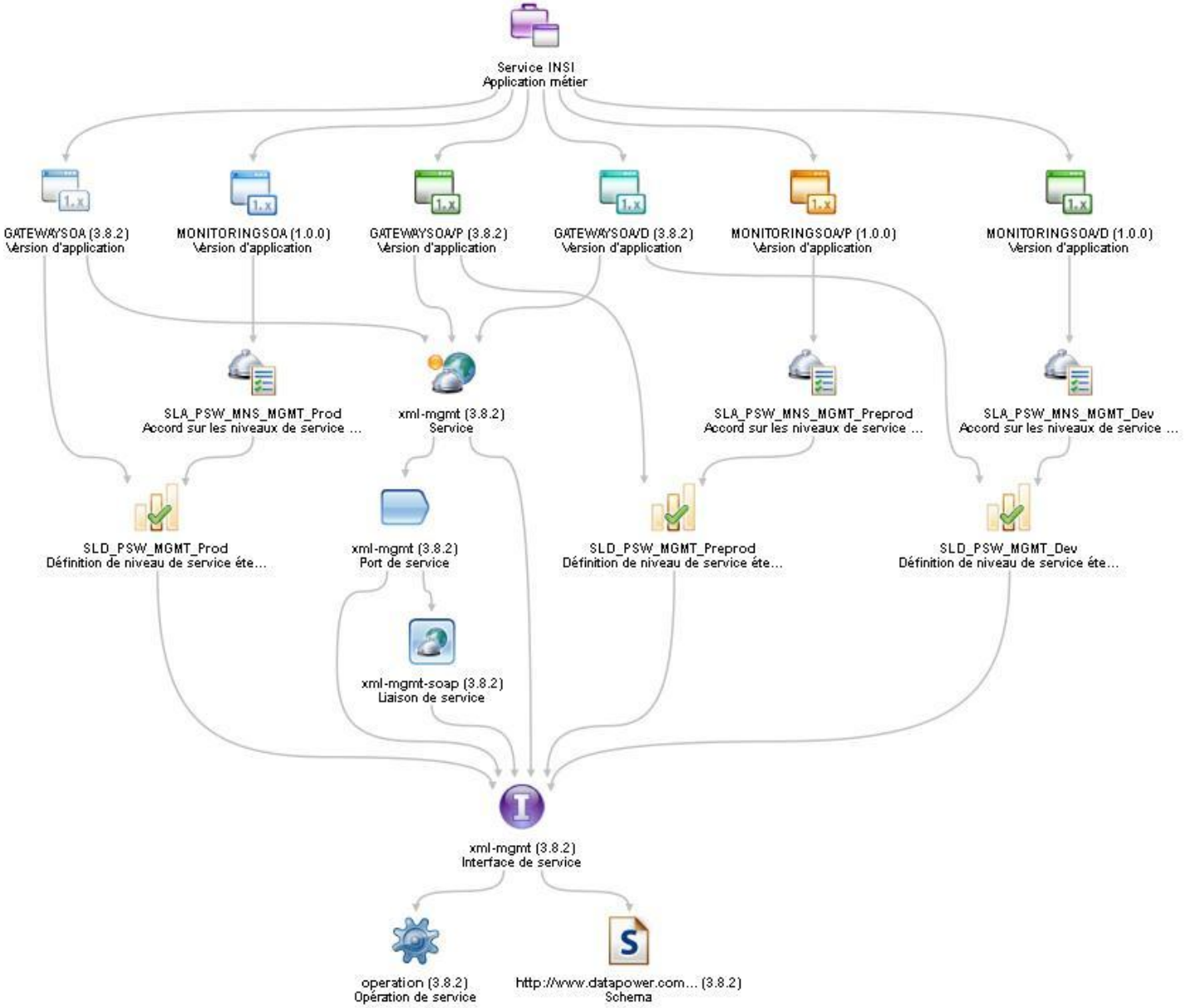
Référentiel de services

Aspect Run Time / Design Time

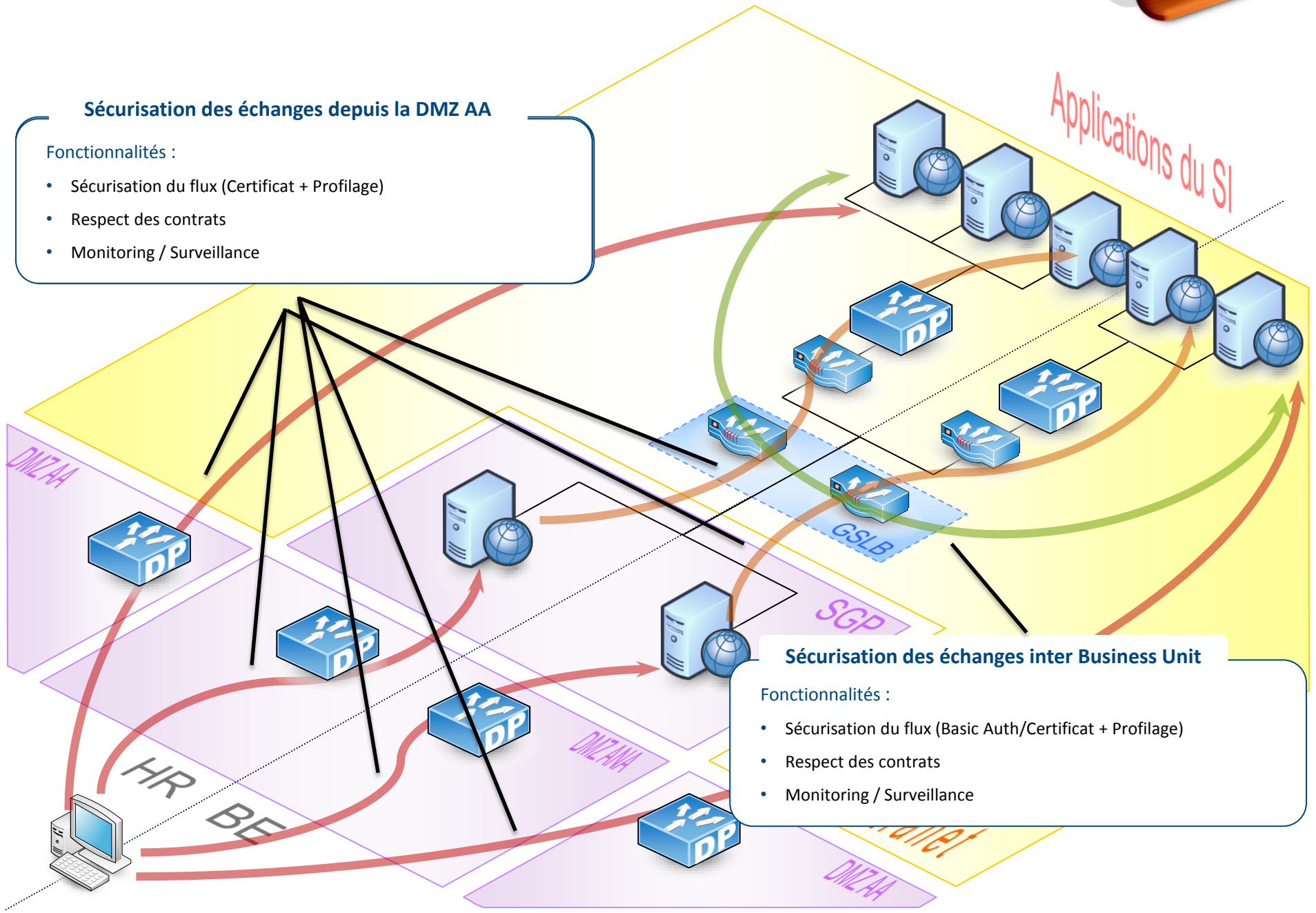


Passerelle de Sécurisation des Services WEB

Référentiel des services : Représentation d'un service WEB

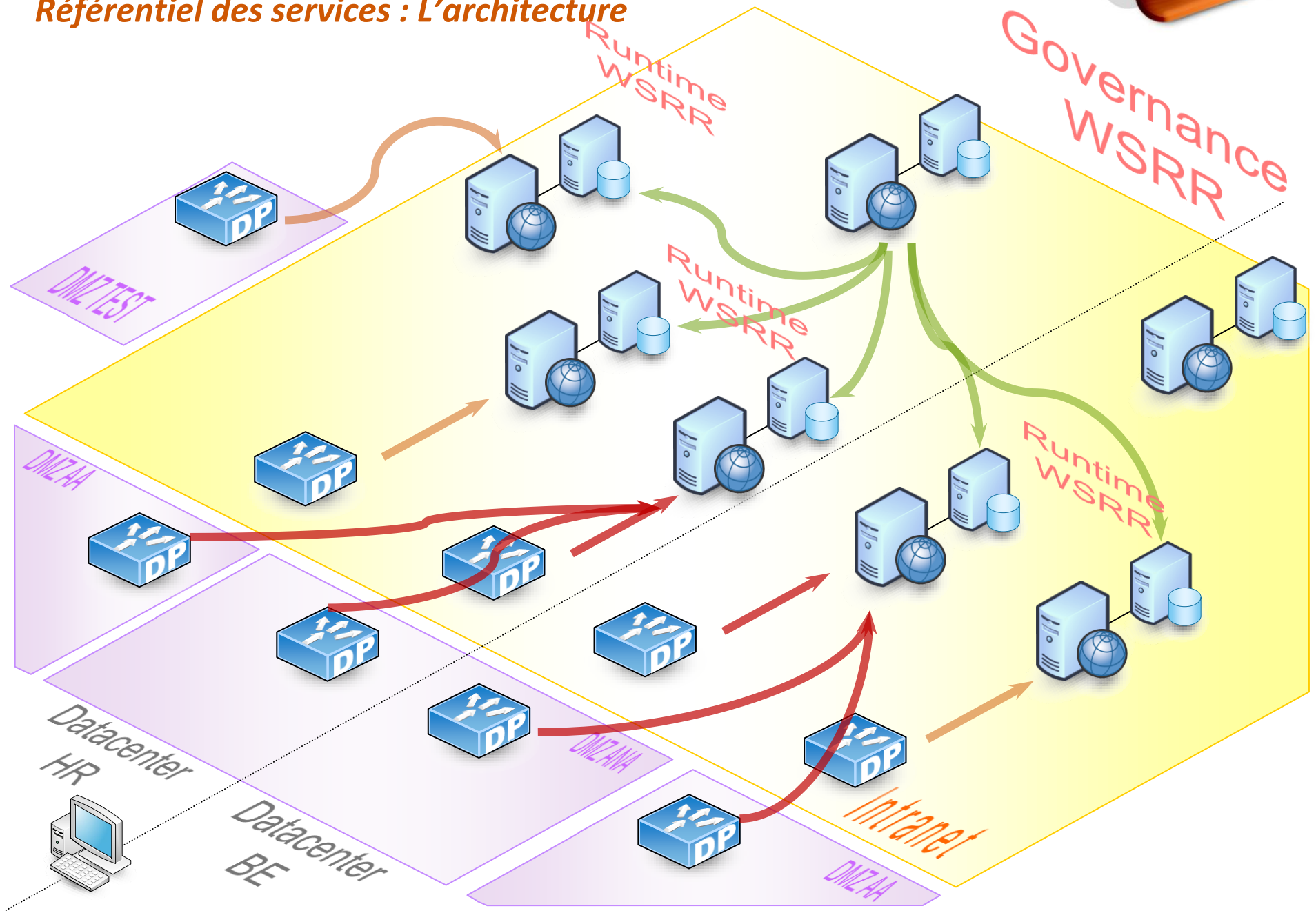


Gestion des échanges entre les zones de sécurité



Passerelle de Sécurisation des Services WEB

Référentiel des services : L'architecture



Agenda

- Contexte et constats
  - Existant chez PSA
  - Cible du chantier SOA
  - Passerelle de sécurisation des services
- **Les offres de service de la Passerelle**
  - Fonctions principales
  - Exemple d'offre de service
- Les contrats de service
  - Contrats applicatifs
  - Contrats techniques
- IBM Datapower XC10
  - Description
  - Test de la solution de cache SOA

Fonctions principales

La fourniture du service « Passerelle de sécurisation » s'organise en 3 catégories

Sécurisation des backends

- Gérer les échanges XML entre les différentes zones réseau
- Identifier le consommateur et vérifier ses habilitations pour l'accès au service Web demandé
- Renforcer la sécurité pour garantir la cohérence entre le niveau de confidentialité des données et le niveau de la sécurité effectif au niveau du service WEB

Monitoring des flux

- Superviser les services
- Remonter les écarts par rapports aux seuils fixés par les contrats de service
  - Nombre de requêtes par jour
  - Temps de réponse
- Alerter sur l'atteinte ou le dépassement de seuils de consommation

Contractualisation avec les fournisseurs

- Faire respecter les contrats définis entre le client et le fournisseur de service au niveau du référentiel de services WEB
- Bloquer la consommation d'un service sans définition préalable d'un contrat (pour garantir la disponibilité du back office)

Détail des fonctionnalités

Sécurisation

Objectif	*Assurer la pérennité des backends fournissant des services entre différentes zones réseaux*
Authentification	*Basic Authentication (HTTP/HTTPS), certificat (HTTPS)*
Habilitation	*Vérification des droits à la consommation d'un service*
Sécurité	*Détection d'attaque*

Contractualisation

Objectif	*Garantit la disponibilité du service web selon les termes de son contrat*
Principe	*A la réception d'une requête, la passerelle exécute les opérations suivantes :* • *Récupération de l'ID du consommateur du service* • *Récupération du contrat associé au consommateur (Service Level Agreement – SLA) et du contrat associé au service requêté (Service Level Definition – SLD)* • ***Application des clauses du contrat consommateur (SLA)*** • ***Application des clauses du contrat fournisseur (SLD)*** → *Lorsqu'aucune SLA n'est définie pour un consommateur donné, le contrat par défaut est appliqué*

Monitoring

Objectif	*Superviser les flux de services web et les contrats associés aux consommateurs et fournisseurs de ces services*
Principe	*Le monitoring fournit l'outillage nécessaire pour déterminer :* • *Le nombre d'accès à un service web* • *Les identifiants des consommateurs d'un service web donné (sauf pour le monitoring de la zone ANA)* • *Les réponses fournies par la passerelle ou par le backend au consommateur (nombre de requêtes en succès, nombre de requêtes en échec…)* • *Les temps de réponse du backend (temps de réponse min, max, moyen)* • *Les tailles des requêtes et des réponses …*

Exemple d'offre de service

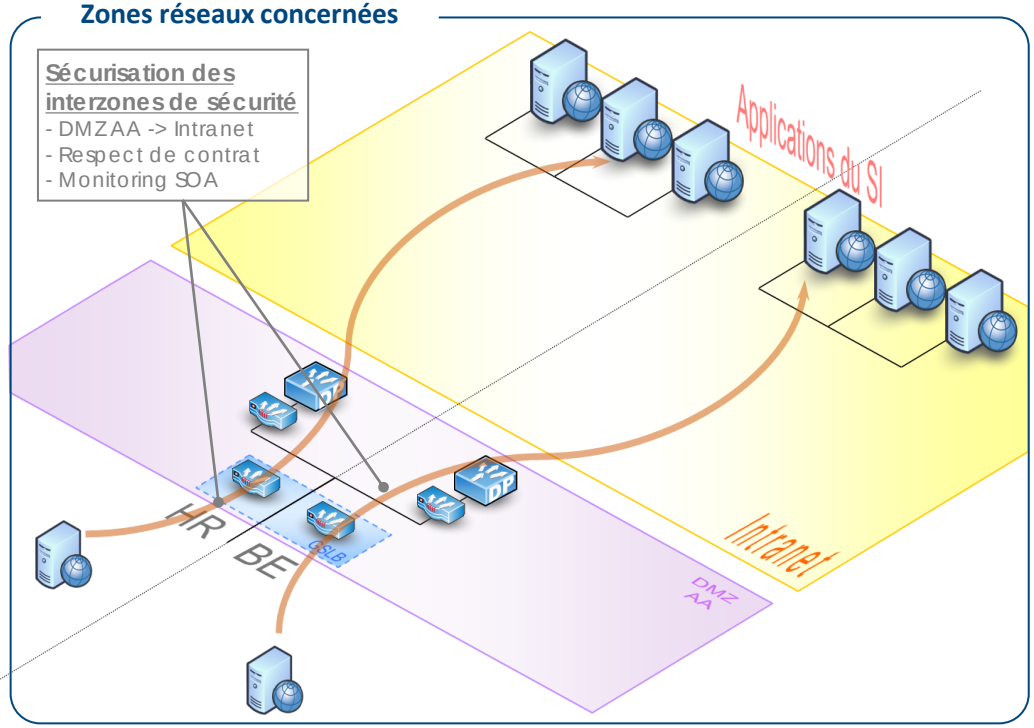
PS-01 Passerelle SOAP

Zones réseau :
AA → Intranet

	Non disponible
c	En cible
d	Dérogation
x	Inclus dans l'offre
o	Selon le besoin

Offres Serveur Web	Ref	Description	Niveau de service couvert				Limites d'usage	Liens		Type Service			Fonctionnalités												Zones réseaux			Coût	Coût	Dispo
			Disponibilité	Intégrité	Confidentialité	Traçabilité	Nombre d'accès simultanés max.	Gouvernance	Supervision	XML / HTTP	SOAP	REST / HTTP	Protection Attaques XML	Validation de la requête	Validation de la réponse	Contrôle SLD	Contrôle SLA	Monitoring	Tableaux de bord de suivi	Remontées d'alerte	Authentification par Basic Auth	Authentification par certificat	Contrôle des habilitations	Support WS-Security	EndPoint WS-Security	Internet > Intranet	Internet > SGP	SGP > Intranet	Coût de fonctionnement	Coût de mise en œuvre	Disponibilité de l'offre
Passerelle SOAP (Internet > Intranet)	PS-01	AA vers Intranet	3	3	3	3	≈ 2400 par seconde	c	x		x		x	o	o	x	x	x	o	o		x	x	c	c	x			*	*	x

Zones réseaux concernées



Prérequis de l'offre

- Consommateur :
  - Authentification du client
    - Le client devra consommer le service en soumettant un certificat à chaque requête
    - Un compte technique devra être rattaché au projet
  - Gestion des droits
    - Le compte technique utilisé devra posséder le service applicatif
  - Le service devra être appelé en HTTPS en passant par le nom de domaine de la passerelle (ne pas passer par l'adresse IP)
- Fournisseur :
  - Le web service doit respecter les standard SOAP pour permettre une validation des requêtes
  - En environnement de production, les ports d'exposition des services sur les backend doivent être : 80 pour de l'HTTP et 443 pour de l'HTTPS.

Agenda

- Contexte et constats
  - Existant chez PSA
  - Cible du chantier SOA
  - Passerelle de sécurisation des services
- Les offres de service de la Passerelle
  - Fonctions principales
  - Exemple d'offre de service
- **Les contrats de service**
  - Contrats applicatifs
  - Contrats techniques
- IBM Datapower XC10
  - Description
  - Test de la solution de cache SOA

Gestion des contrats applicatifs et techniques

PSA PEUGEOT CITROËN

Datapower

SLA : Service Level Agreement

Objectif : Clauses par client

SLD : Service Level Definition

Objectif : Clauses par service WEB

SLM : Nb Appels / min

SLA : 500 Appels / min

SLA : 400 Appels / min

SLA : 200 Appels / min

SLA : 50 Appels / min

SLA : 120 Appels / min

SLD : 3000 Appels / min

Monitoring

WSRR

Description: La description des SLA et SLD est contenue et gérée à partir de WSRR

Les producteurs et les consommateurs sont autonomes pour y négocier et définir leurs clauses.

Contrats applicatifs
SLD - Service Level Definition

PSA PEUGEOT CITROËN

Définition

Description des capacités intrinsèques d'un service (i.e. en dehors de toutes considérations clientes) en termes de fréquence d'accès, de temps de réponse, de volume de message, plage de disponibilité, etc.

Les SLD ne sont pas associés à chaque consommateur.

Offre	Clauses des SLD	Actions possibles	Sur une plage horaire	Pour un niveau donné *
XML	Nombre de requêtes par intervalle de temps	Rejet, lissage, notification	✓	✗
	Temps de réponse moyen par intervalle de temps	Notification	✓	✗
	Temps de réponse maximum par intervalle de temps	Notification, **rejet, lissage**	✓	✗
	Taille maximum de la requête	Rejet, lissage, notification	✓	✗
	Taille maximum de la réponse	Rejet, lissage, notification	✓	✗
	Taille moyenne de la requête par intervalle de temps	Notification	✓	✗
	Taille moyenne de la réponse par intervalle de temps	Notification	✓	✗
SOAP	Nombre de requêtes par intervalle de temps	Rejet, lissage, notification	✓	✓
	Temps de réponse moyen par intervalle de temps	Notification	✓	✓
	Temps de réponse maximum par intervalle de temps	Notification, **rejet, lissage**	✓	✓
	Taille maximum de la requête	Rejet, lissage, notification	✓	✓
	Taille maximum de la réponse	Rejet, lissage, notification	✓	✓
	Taille moyenne de la requête par intervalle de temps	Notification	✓	✓
	Taille moyenne de la réponse par intervalle de temps	Notification	✓	✓

* Les différents niveaux proposés sont : *service*, opération

Plage de maintenance

Un fournisseur peut mettre en place une plage de maintenance pour ses équipements en définissant une clause de SLD spécifiant un nombre de requêtes nul sur une plage horaire donnée.

Contrats applicatifs
SLA - Service Level Agreement

PSA PEUGEOT CITROËN

Définition

Contrat de partenariat, négocié entre un producteur de service et un consommateur, définissant les modalités de consommation du service ainsi que les engagements associés des 2 parties en termes de fréquence d'accès, de temps de réponse, de volume de message, etc.

Les SLA sont associés à chaque consommateur authentifié.

Offre	Clauses des SLA	Actions possibles	Sur une plage horaire	Pour un niveau donné *
XML	Nombre de requêtes par intervalle de temps	Rejet, lissage, notification	✓	✗
	Temps de réponse moyen par intervalle de temps	Notification	✓	✗
	Temps de réponse maximum par intervalle de temps	Notification, **rejet, lissage**	✓	✗
	Taille maximum de la requête	Rejet, lissage, notification	✓	✗
	Taille maximum de la réponse	Rejet, lissage, notification	✓	✗
	Taille moyenne de la requête par intervalle de temps	Notification	✓	✗
	Taille moyenne de la réponse par intervalle de temps	Notification	✓	✗
SOAP	Nombre de requêtes par intervalle de temps	Rejet, lissage, notification	✓	✓
	Temps de réponse moyen par intervalle de temps	Notification	✓	✓
	Temps de réponse maximum par intervalle de temps	Notification, **rejet, lissage**	✓	✓
	Taille maximum de la requête	Rejet, lissage, notification	✓	✓
	Taille maximum de la réponse	Rejet, lissage, notification	✓	✓
	Taille moyenne de la requête par intervalle de temps	Notification	✓	✓
	Taille moyenne de la réponse par intervalle de temps	Notification	✓	✓

* Les différents niveaux proposés sont : *service*, opération

SLA par défaut

Un fournisseur de service a la possibilité de définir une SLA par défaut pour un ensemble de consommateurs du service.

Après la phase d'authentification du client, la SLA par défaut est appliquée si il n'y a pas de contrat liant directement le fournisseur et le consommateur.

Contrats applicatifs

Extensions

Routage applicatif

Possibilité de router les consommateurs vers différents producteurs ou « backend » d'après des règles métiers définies dans le référentiel des services

- Les règles métiers sont définies par les projets
- Elles sont attachées au contrat du service
- Elles peuvent prendre en compte n'importe quel partie du contenu du service WEB

Chiffrement (à venir)

Gestion du chiffrement/déchiffrement des messages (WS-Security) à partir des Datapower en fonction de la nature du consommateur (Intranet/Internet, etc..)

Possibilité de chiffrer les pièces jointes en provenance ou à destination d'un tiers

Cache de services

Réduction de la charge des producteurs

Stabilisation des performances et amélioration de la qualité de service

Activation du cache sans modification des clients et serveurs

Applicable aux clients légers (navigateurs)

Politique de cache est directement définie dans le référentiel des services

Contrats applicatifs

Extensions

Service WEB Internet

Possibilité d'exposer en Intranet un service WEB exposé sur Internet

- Transparent pour les consommateurs
    - Le service est vu comme un service local
- Passage par le proxy de surf avec utilisation de l'authentification du client
- Authentification possible auprès du service extérieur avec certificat
    - Attention : Seulement si le certificat est déclaré dans les Datapowers
- Bénéficie de l'offre de service complète
- A disposition des consommateurs situés en zone Intranet et SGP

Service REST

Création d'un canal dédié aux services REST

Disponible sur toutes les zones réseaux (Intranet, SGP, DMZ AA et DMZ ANA)

Même niveau de service que pour les services WEB « classiques » avec un traitement particulier par la gestion des codes erreurs HTTP

- Par défaut les Datapower réécrivent les codes erreurs, il est nécessaire de « brider » ce comportement pour les services REST

Agenda

- Contexte et constats
  - Existant chez PSA
  - Cible du chantier SOA
  - Passerelle de sécurisation des services
- Les offres de service de la Passerelle
  - Fonctions principales
  - Exemple d'offre de service
- Les contrats de service
  - Contrats applicatifs
  - Contrats techniques
- **IBM Datapower XC10**
  - Description
  - Test de la solution de cache SOA

IBM Datapower XC10

Description

- Le Datapower XC10 est un équipement hardware
  - Capacité total de 240 Go
  - 8 interfaces ethernet Gigabit et 2 interfaces ethernet 10 Gigabits
    - Possibilité de coupler les interfaces pour augmenter la bande passante

- Nature du cache
  - Cache simple de type ObjectMap (principe de clef/valeur comme Memcached)
    - Méthodes CRUD sur les objets (read, create, update, delete)
  - Les objets ont une durée de vie définie à l'insertion

- Grilles
  - Peuvent être réparties et/ou répliquées sur plusieurs boîtiers
  - Peuvent avoir des configurations différentes (répartion, réplication, sécurité)
  - Possibilité de créer une grille sur plusieurs datacenter
    - Gestion du mode multi-maître

IBM Datapower XC10

Description

- Fonctionnalités
  - Monitoring via SNMP
  - Administration via script et interface WEB
  - Sécurisation sur LDAP
    - Pour l'administration
    - Pour l'accès aux grilles de données ainsi que pour le type d'accès sur les données de la grille
      - Basé sur l'identifiant ou sur l'appartenance à un groupe LDAP

- Compatibilité
  - Datapower XI50/52, WebSphere Message Broker, WebSphere ESB
  - Websphere v6.1 et supérieurs (dont v8.0 et Liberty Profile)
    - Partage de session HTTP
    - Dynacache (cache de contenu généré, html, etc.)
  - Il offre des APIs d'accès pour les applications JAVA et .Net
  - Interface HTTP/REST pour les applications non-JAVA
  - Spring 3.1 Cache

IBM Datapower XC10

Test de la solution de cache SOA

PSA PEUGEOT CITROËN

Objectifs

Tester l'intégration du Datapower XC10 en tant que solution de cache dans les traitements actuels des services WEB

- Evaluer les modifications à apporter à la configuration actuelle

Estimer les gains en termes de performance pour le service WEB

Déterminer les limites de la solution (exemple : nombre de requêtes par secondes)

Cas d'usage retenu

Service WEB Corvet@

- Temps de réponse moyen de 150 ms
- Taille des échanges : ~700 octets / question, ~7ko / réponse
- **Augmentation du nombre de requêtes par secondes** provoque
  - des pics de **temps de réponse à plusieurs secondes**
  - une **augmentation du taux d'erreur**
- **1 100 000** appels par jour alors qu'il n'y aurait que **150 000** véhicules différents consultés par jour
  - Réduction potentielle d'un **facteur 7** avec une mise en cache ?

Démarche adoptée pour les tests

Capture des requêtes d'une journée type en production

Construction d'un injecteur capable de rejouer les requêtes enregistrées

- Permet de rejouer à l'identique 24H d'activité de production
  - En respectant l'intervalle de temps entre 2 requêtes consécutives
- Permet de rejouer un journée en « accélérée »
  - En réduisant cet intervalle d'un facteur « x » paramétrable

IBM Datapower XC10

Test de la solution de cache SOA

PSA PEUGEOT CITROËN

Principe

Le cache peut être activé par service WEB

On peut définir une configuration par client du service WEB

On peut définir une configuration par défaut qui s'applique à tous les clients qui n'ont pas une configuration spécifique

Configuration du cache

Pour chaque configuration de cache il est possible de :

- Choisir la durée de rétention de la donnée
    - La durée de rétention est définie, dans le boîtier XC10, au moment de l'insertion
        - Les données expirées sont donc automatiquement supprimées
- Choisir l'algorithme de calcul de la clef de hachage (sha256, md5, etc.)
- Définir la ou les règles XPATH définissant le contenu utilisé pour le calcul de la clef
    - La clef peut être calculée à partir d'une partie ou de l'ensemble de la question
- Indiquer si les données doivent être cloisonnées par client ou non

Intégration avec les Datapower XI52

L'intégration est faite en ajoutant des feuilles de style au traitement existant des services WEB

L'appel au cache est réalisé en utilisant l'API REST (HTTP) fournie par le XC10

Les accès peuvent être sécurisés (HTTPS, authentification mutuelle, Basic Authentication)

IBM Datapower XC10

Test de la solution de cache SOA

PSA PEUGEOT CITROËN

Etape 2

Traitement standards de la requêtes (Sécurité, Monitoring, etc.)

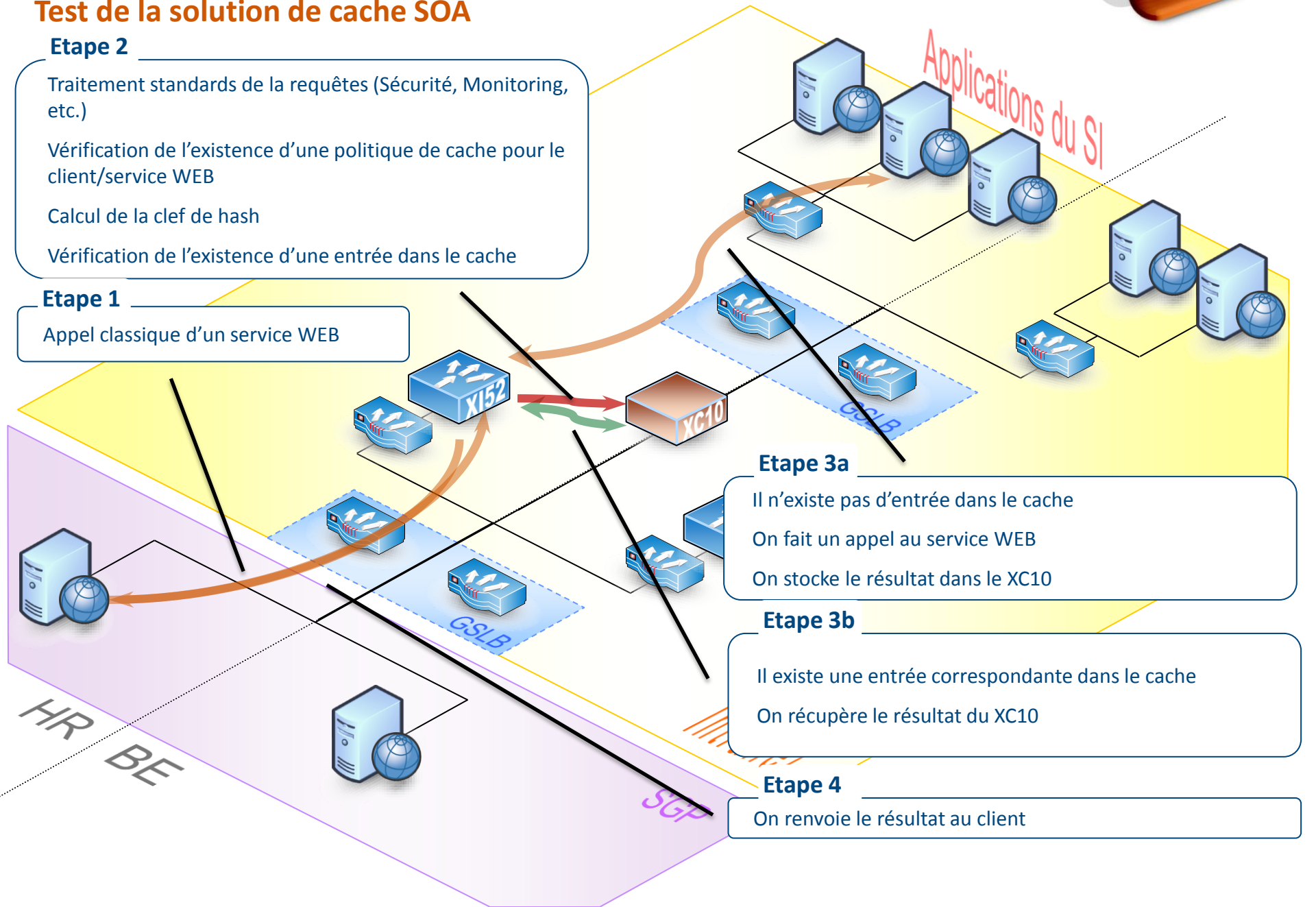
Vérification de l'existence d'une politique de cache pour le client/service WEB

Calcul de la clef de hash

Vérification de l'existence d'une entrée dans le cache

Etape 1

Appel classique d'un service WEB



Etape 3a

Il n'existe pas d'entrée dans le cache

On fait un appel au service WEB

On stocke le résultat dans le XC10

Etape 3b

Il existe une entrée correspondante dans le cache

On récupère le résultat du XC10

Etape 4

On renvoie le résultat au client

IBM Datapower XC10

Test de la solution de cache SOA

PSA PEUGEOT CITROËN

Intégration

La solution a été **rapidement opérationnelle**

- La mise en œuvre du cache avec l'intégration à la configuration existante a été réalisée en 1 semaine

Qualité de service

Taux d'erreur nul sur les accès au cache

Allongement des temps de réponse en cas de très forte charge

- Origine précise indéterminée (2 patchs déjà livrés)
- Ce problème se présente bien après la limite acceptable, sans solution de cache, par le producteur de service
    - Problème rencontré en injectant en 30min l'équivalent de l'activité d'une journée entière

Performance

60,85% de hit dans le cache sur une journée

- Divise par 2,5 le nombre d'appels au producteur de service

Temps moyen d'un appel avec données dans le cache : **< 13 ms**

- Par rapport à ~**150 ms** sans cache

Sur une journée, le temps de réponse moyen avec le cache est donc ramené à **~67ms**

- Avec 1 100 000 transactions / jour -> **25 heures gagnées par jour**

Bilan
et
Questions ?