

# Cadre de cohérence technique du système d'information de l'Assistance Publique – Hôpitaux de Paris

Normes et standards d'architecture technique

Décembre 2019

Version 4.0

DSI / Cellule Architecture Technique

### SUIVI DES VERSIONS

Version	Date	Auteur	Objet de la modification
1.0	28/10/04	P. BRILLANT	Création du document
2.0	17/12/04	P. BRILLANT	
3.0	21/12/2015	F.PERRIN	
3.3	04/01/2017	Responsables des pôles du département Infrastructures et Services (ATI)  F.PERRIN	Avant dernière version
4.0	05/12/2019	Equipe Architecture DIS David Porte Vincent Fetter Fabrice Turbault  Equipe Sécurité Didier Perret  Contributions des équipes DSI (DIS) et GH	Restructuration majeure <ul style="list-style-type: none"> <li>• Renvoi des documents référencés en Annexe</li> <li>• Organisation en règles</li> <li>• Nouvelle rédaction de l'ensemble des chapitre</li> <li>• Présentation de modèles d'architecture</li> </ul>

# Sommaire

---

<b>SOMMAIRE.....</b>	<b>3</b>
<b>INDEX DES FIGURES .....</b>	<b>6</b>
<b>PREAMBULE.....</b>	<b>7</b>
<b>OBJET DU DOCUMENT .....</b>	<b>8</b>
1. LES PRINCIPAUX OBJECTIFS .....	8
2. LES BENEFICIAIRES DU CADRE DE COHERENCE TECHNIQUE .....	8
a. <i>Maîtrise d'ouvrage et maîtrise d'œuvre</i> .....	8
b. <i>Les applications et les systèmes</i> .....	9
3. APPLICATION DES REGLES.....	9
4. DESCRIPTION DES CLASSIFICATIONS DES REGLES.....	9
5. VALIDATION DE L'ARCHITECTURE TECHNIQUE .....	10
a. <i>Rédaction et validation du CCT</i> .....	10
b. <i>Conception et validation de l'architecture technique</i> .....	10
<b>ARCHITECTURE D'EXECUTION .....</b>	<b>11</b>
1. LES COMPOSANTS D'INFRASTRUCTURE.....	11
a. <i>Le réseau</i> .....	11
Les zones de sécurité homogène du SI AP-HP.....	11
Interconnexion des sites AP-HP .....	12
Les services hébergés sur le réseau ELICE .....	13
Les Datacenters.....	14
Accès Internet.....	15
Passerelle d'interconnexion filtrée (DMZ).....	16
Connexions avec les partenaires .....	17
Le réseau BBS (zone serveurs centrale).....	18
Les réseaux LAN Ethernet des établissements .....	27
WLAN .....	27
La qualité de service (QoS).....	27
Connexions .....	28
Livrables .....	29
b. <i>Les serveurs</i> .....	30
Les systèmes Mainframe .....	30
Les serveurs physiques .....	30
La virtualisation .....	32
Les systèmes d'exploitation.....	41
c. <i>Le stockage</i> .....	42
Concepts.....	42
Le stockage primaire .....	43

Le stockage secondaire .....	45
d. <i>Les hébergements</i> .....	46
Hébergement propre .....	46
cloud public.....	47
e. <i>Le poste de travail</i> .....	49
Matériel .....	49
Système .....	49
Sécurité.....	50
Logiciels .....	50
f. <i>Les services d'infrastructure</i> .....	51
La répartition de charge.....	51
La haute disponibilité .....	53
L'authentification.....	56
2. LES SERVICES APPLICATIFS .....	57
a. <i>Les bases de données</i> .....	57
Les bases de données relationnelles .....	57
Les bases de données nosql.....	57
La réplication des données.....	59
b. <i>Les échanges inter-applicatifs</i> .....	60
Les solutions de gestion des flux.....	60
c. <i>La planification des traitements</i> .....	64
d. <i>Orchestration</i> .....	64
e. <i>Serveur de publication</i> .....	64
<b>ARCHITECTURE D'ADMINISTRATION .....</b>	<b>65</b>
1. LA SECURITE DES SYSTEMES D'INFORMATION.....	65
a. <i>Principes généraux de la PGSSI</i> .....	65
b. <i>Environnement technique de sécurité du SI de l'AP-HP</i> .....	65
Poste de travail windows .....	65
Messagerie électronique.....	65
c. <i>Exigences techniques de sécurité</i> .....	66
Poste de travail informatique .....	66
Navigateurs.....	66
Serveurs informatiques.....	67
Configuration du système d'exploitation linux .....	67
Annuaire active directory microsoft .....	67
journalisation.....	67
téléassistance informatique .....	68
cryptographie .....	68
applications web .....	68
réseaux.....	68

téléphones multifonctions.....	69
téléphonie sur ip .....	69
sécurité physique et dispositifs de vidéo protection .....	70
lutte contre les codes malfaisants .....	70
2. LA PROTECTION DES DONNEES.....	71
3. LA SUPERVISION .....	71
<b>ANNEXES.....</b>	<b>72</b>
Annexe 1 - Documents de référence.....	72
Annexe 2 - Glossaire .....	73
Annexe 3 – Processus de conception et de validation de l’architecture technique .....	76

# Index des figures

---

Figure 1 - Les niveaux de règle .....	9
Figure 2 - Réseau de transport .....	12
Figure 3 - Le réseau Elice .....	12
Figure 4 - Services hébergés ELICE .....	13
Figure 5 - Proxification .....	14
Figure 6 - Interconnexion Datacenters .....	15
Figure 7 - Les principaux sites d'hébergement .....	15
Figure 8 - Accès Internet .....	16
Figure 9 - WAF .....	17
Figure 10 - Filtrage (I) .....	19
Figure 11 - Filtrage (II) .....	19
Figure 12 - Séparation des flux .....	20
Figure 13 - Interfaces réseau d'un serveur .....	21
Figure 14 - Flux métier entre serveurs .....	21
Figure 15 - Flux d'infrastructure depuis un serveur métier .....	22
Figure 16 - Flux d'administration vers un serveur métier .....	22
Figure 17 - Flux de sauvegarde et de restauration d'un serveur .....	23
Figure 18 - Découpage en couches .....	24
Figure 19 - Séparation des fonctions .....	24
Figure 20 - Flux entrant et reverse-proxy .....	27
Figure 21 - Interfaces réseau d'un serveur .....	32
Figure 22 - Cluster Kubernetes .....	36
Figure 23 - Accès à un service conteneurisé .....	37
Figure 24 - Réseau de conteneurs (CNI) .....	38
Figure 25 - Création des images .....	40
Figure 26 - Catégories de stockage .....	42
Figure 27 - Multipathing SAN .....	44
Figure 28 - Utilisation du stockage secondaire .....	45
Figure 29 - Stratégie d'hébergement .....	46
Figure 30 - Cloud public Architecture Hub & Spoke .....	48
Figure 31 - Evolutivité horizontale .....	51
Figure 32 - Gestion des VIP (I) .....	51
Figure 33 - Gestion des VIP (II) .....	52
Figure 34 - Consommation d'un service redondé .....	52
Figure 35 - Principes RPO / RTO .....	53
Figure 36 - Haute-disponibilité .....	54
Figure 37 - Haute disponibilité (II) .....	55
Figure 38 - Flux inter-applicatifs .....	61
Figure 39 - Puit de fichiers pour les flux .....	63

# Préambule

---

Le Cadre de Cohérence Technique (CCT) du Système d'Information (SI) de l'Assistance Publique – Hôpitaux de Paris (AP-HP) tient compte d'un ensemble de recommandations des référentiels publiés par différentes structures publiques. Ces documents sont référencés dans l'Annexe 1 - Documents de référence, de ce présent document. Tous les acronymes utilisés sont référencés dans l'Annexe 2 - Glossaire.

Les normes et standards référencés dans le Cadre de Cohérence Technique du SI de l'AP-HP sont à prendre en considération lors de la préparation de tout projet technique apportant des modifications au Système d'Information de l'AP-HP, y compris dans les échanges de données avec ses partenaires.

***Il est demandé aux soumissionnaires de préciser et justifier les écarts éventuels entre les solutions proposées et les normes et standards du Cadre de Cohérence Technique du SI de l'AP-HP.***

\* \*

\*

Les choix effectués correspondent à l'état de l'art, dont on sait que l'environnement législatif, réglementaire ou technique est évolutif. Ainsi, le Cadre de Cohérence Technique du SI de l'AP-HP est actualisé régulièrement.

Toute difficulté rencontrée lors de la mise en œuvre du Cadre de Cohérence Technique devra être signalée à la Direction des Systèmes d'Information (DSI) de l'AP-HP, via l'adresse [dsi-dis-ppa-archi@aphp.fr](mailto:dsi-dis-ppa-archi@aphp.fr).

\* \*

\*

Les prescriptions suivantes sont respectées (celles-ci sont transposées des recommandations figurant dans les référentiels RGI, RGAA et RGS) :

- a. Le Cadre de Cohérence Technique est référencé en annexe des cahiers des clauses techniques particulières des appels d'offres et marchés publiés par l'AP-HP ;
- b. Une attestation de conformité est intégrée à la réponse du soumissionnaire. A défaut, il faudra indiquer les raisons pour lesquelles il a paru nécessaire de s'en écarter, ainsi que le calendrier envisagé pour assurer la mise en conformité ;
- c. Pour le bon fonctionnement, il sera nécessaire de veiller tout particulièrement à ce que ne soient pas utilisés d'autres formats de documents que ceux référencés dans le cadre commun d'interopérabilité: c'est une condition nécessaire pour assurer la pérennité des documents informatisés et garantir la possibilité d'un accès aux informations qu'ils contiennent ;
- d. Les recommandations contenues dans les référentiels qui accompagnent les services opérationnels pour l'interopérabilité sont mises en œuvre; l'évaluation de conformité est réalisée par audits périodiques ;
- e. Des dispositions sont prises afin que, dans les meilleurs délais, l'ensemble des référentiels de données et des composants logiciels librement réutilisables dont la nature présente un intérêt général soient répertoriés ;
- f. L'utilisation du répertoire de schémas XML de l'administration est conforme aux modalités énoncées dans le référentiel. La méthode de conception retenue privilégie l'utilisation de schémas existants par rapport au développement de nouveaux schémas, sauf dérogation expressément accordée ;
- g. Une consultation systématique du service de ressources numériques est envisagée à l'occasion de tout projet d'échanges entre les services de l'Etat ou avec des tiers, afin de privilégier la réutilisation de modèles, de référentiels de données et de composants logiciels existants.

# Objet du document

---

## 1. Les principaux objectifs

Le Cadre de Cohérence Technique du SI de l'AP-HP présente les normes et standards privilégiés par l'AP-HP afin de :

- Permettre aux applications et aux systèmes
  - de partager dans de bonnes conditions l'infrastructure matérielle et l'infrastructure de communication ;
  - d'inter-opérer entre eux et avec les partenaires extérieurs. Sur ce dernier point, le CCT s'appuie sur, complète et précise le Référentiel Général d'Interopérabilité ;
- Garantir la sécurité du SI de l'AP-HP ;
- Favoriser une bonne pérennité des composants de base par la mise en œuvre de démarches de choix instrumentées, et limiter la variabilité des plates-formes et des configurations par une évolution concertée des composants ;
- Maîtriser les coûts d'acquisition des progiciels et des composants logiciels ainsi que ceux des services d'intégration et d'administration en évitant que chaque application n'impose ses propres composants de base (outils bureautiques, multimédia, de gestion des sauvegardes, de gestion des impressions, couches de communications, bases de données locales, gestion des habilitations ...).

## 2. Les bénéficiaires du Cadre de Cohérence Technique

### *a. Maîtrise d'ouvrage et maîtrise d'œuvre*

Le CCT du SI de l'AP-HP est :

- Visible pour pouvoir être respecté par les maîtrises d'ouvrage et les maîtrises d'œuvre. Il est donc mis en ligne sur l'intranet de la DSI de l'AP-HP. Il peut éventuellement être repris dans l'espace départemental de la Direction Spécialisée des Finances Publiques (DSFP) pour les informations relevant de processus où l'intérêt est commun ;
- Evolutif et à l'état de l'art grâce à une mise à jour régulière. Les orientations figurant dans ce document sont enrichies en particulier à partir des travaux mis en ligne par le SGMAP (Secrétariat Général pour la Modernisation de l'Action Publique).

Le CCT doit faciliter la mise en œuvre des évolutions futures liées à l'urbanisation du SI en permettant aux acteurs du changement d'effectuer des choix respectant les normes et standards privilégiés par l'AP-HP en accord avec la DSFP pour les domaines communs.

Les maîtres d'ouvrage (MOA) contribuent à la cohérence technique du SI en réclamant dans leurs cahiers des charges l'utilisation de produits conformes aux recommandations préconisées par le CCT.

Les maîtres d'œuvre (MOE), concepteurs et développeurs, fournissent des services et outils informatiques conformes aux normes et standards recommandés dans le CCT, facilitant ainsi :

- leur intégration dans le SI de l'AP-HP ;
- la sécurité du SI de l'AP-HP ;
- l'interopérabilité avec les partenaires extérieurs qui appliquent les standards.



### **b. Les applications et les systèmes**

Les applications et les systèmes doivent se conformer au CCT; ne peuvent en déroger que ceux dont la non-conformité n'a pas d'impact sur des infrastructures partagées ou sur les activités de structures informatiques mutualisées.

Une application ou un système qui n'est pas conforme au CCT doit satisfaire au minimum les propriétés suivantes :

- Il doit fonctionner sur des postes de travail dédiés afin de ne pas risquer de perturber les systèmes de communication et les applications et les systèmes conformes au CCT;
- Il ne pourra utiliser une infrastructure mutualisée (WAN de l'AP-HP, serveur local de ressources...) qu'à la seule condition d'avoir fait l'objet d'un rapport d'expertise technique favorable du Département Infrastructures et Services et du Département de la Sécurité du SI de la DSI de l'AP-HP

Dans le cadre d'une mutualisation des expériences, la description d'application à contexte innovant est remontée à la DSI de l'AP-HP. Si une application utilise un composant logiciel ou technique non référencé dans le CCT, une déclaration doit être adressée à la DSI de l'AP-HP et peut aboutir à une évolution du CCT.

### **3. Application des règles**

Les règles et les normes décrites dans le CCT s'appliquent à tous les projets visant

- À mettre en œuvre une nouvelle solution informatique
- À faire évoluer une solution informatique existante (extension du périmètre, ajout de services techniques, changement de version ...)

dans le SI de l'AP-HP.

### **4. Description des classifications des règles**

Les règles décrites dans le Cadre de Cohérence Technique présentent trois niveaux de classification schématisés selon trois codes couleur différents :

<b>O</b>	<b><u>Obligatoire</u></b> La règle décrite constitue une exigence à respecter absolument. Aucun écart n'est toléré.
<b>R</b>	<b><u>Recommandé</u></b> La règle décrite constitue une recommandation qui devrait être respectée autant que faire se peut. Néanmoins, il peut être toléré de ne pas suivre une recommandation dans des cas exceptionnels, dûment justifiés et mesurant les impacts d'un tel choix.
<b>I</b>	<b><u>Interdit</u></b> La règle décrite constitue une interdiction de mise en œuvre à respecter absolument.

*Figure 1 - Les niveaux de règle*

## **5. Validation de l'architecture technique**

### **a. Rédaction et validation du CCT**

Le CCT est un document de synthèse auquel contribuent les différentes équipes de la DSI de l'AP-HP. Les informations techniques et les recommandations qu'il contient ont été validées par les participants et sont mises à jour :

- Régulièrement à partir des propositions de modification des contributeurs ;
- Après chaque événement ayant un impact majeur sur l'évolution de l'architecture technique du SI.

### **b. Conception et validation de l'architecture technique**

La conception de l'architecture technique d'une solution informatique mise en œuvre dans le cadre d'un projet suit un processus bien précis. Ce processus est décrit dans l'Annexe 3 – Processus de conception et de validation de l'architecture technique.

Cette phase de conception réunit un ensemble d'acteurs (architectes, experts techniques, experts sécurité, exploitants, chef de projet, intégrateurs ...) sous forme d'ateliers de travail.

Toutes les problématiques d'architecture, de sécurité et d'intégration de la future application dans le SI doivent être abordées au cours de ces ateliers afin de garantir le respect des normes et standards de l'AP-HP, de vérifier leur applicabilité dans le contexte du projet et de faire évoluer si nécessaire le CCT et les autres documents de référence de l'AP-HP.

Ces ateliers conduisent à la rédaction du livrable d'architecture : le Dossier d'Architecture Technique (DAT).

La rédaction du DAT est de la responsabilité de l'intégrateur retenu par l'AP-HP pour mettre en œuvre la solution informatique. Le DAT doit faire l'objet d'une validation de la part de la Cellule Architecture Technique de la DSI de l'AP-HP. Cette validation

- S'accompagne de la production de trois documents
  - Une fiche de relecture consignait l'ensemble des remarques émises par la Cellule Architecture Technique de la prise de connaissance du DAT livré par l'intégrateur
  - Un PV de validation statuant de la décision prise par la Cellule Architecture Technique
    - Architecture validée
    - Architecture validée avec des réserves
    - Architecture non validée
  - Une cartographie technique contextualisée à l'environnement AP-HP sous forme d'un fichier Visio élaboré par la Cellule Architecture Technique de la DSI de l'AP-HP
- Conditionne la mise à disposition des infrastructures de production et de pré-production de la solution informatique

Il est également à noter que toute application et tout module d'interface sont déclarés et décrits dans la cartographie applicative du SI de l'AP-HP. De ce fait, le fournisseur et /ou le chef de projet transmettent toutes les informations utiles au département de la DSI en charge de la cartographie applicative.

# Architecture d'exécution

---

Le présent chapitre vise à décrire les normes et standards à respecter, pour chacun des composants suivants :

- Les composants d'infrastructure sur lesquels s'appuient les services applicatifs, les systèmes et les applications génériques : réseau et protocoles, serveurs, systèmes d'exploitation, postes de travail ;
- Les services applicatifs : les bases de données, la gestion des flux, la planification ...

## 1. Les composants d'infrastructure

### *a. Le réseau*

#### LES ZONES DE SECURITE HOMOGENE DU SI AP-HP

---

Le SI de l'AP-HP se découpe en zones de sécurité distinctes. Celles-ci regroupent des éléments de nature et de fonctions différentes. Les zones de sécurité représentent un ensemble d'éléments protégés par une même politique de filtrage (zone serveurs BBS, DMZ ...) instanciée sur des matériels physiques dédiés. Ces zones de sécurité sont au nombre de six actuellement :

- La DMZ a pour but d'héberger les éléments de filtrage afin de protéger le SI des attaques venant de réseaux extérieurs. Ceux-ci sont listés et décrits dans les paragraphes ci-après
- La zone BBS est la zone de sensibilité la plus forte du SI AP-HP car elle héberge l'ensemble des ressources centralisées informatiques de l'AP-HP
- La zone Elice est une zone de transit, plus spécifiquement un réseau d'échange et de raccordement entre les autres zones de sécurité de l'AP-HP (BBS, les hôpitaux, la DMZ).
- Les Groupements Hospitaliers (GH) sont des zones de sécurité représentant les ressources propres aux hôpitaux.
- Le wifi public est une zone de sécurité propre car elle permet de proposer un accès internet aux étudiants et patients
- L'hébergement Cloud public

**I** Un équipement, une ressource physique ou virtuelle ne peut pas appartenir à deux zones de sécurité différentes en même temps

Tous les sites de l'AP-HP sont interconnectés par un réseau fédérateur ELICE (Elément de Liaison et d'Inter Connexion entre les Etablissements).

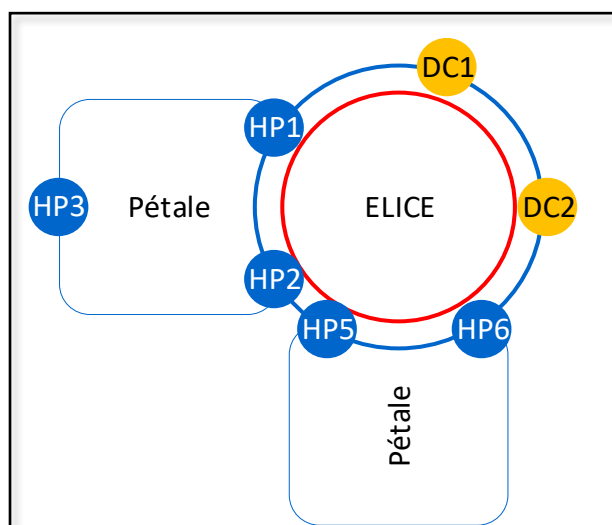


Figure 2 - Réseau de transport

Ce réseau est composé d'une double boucle fibre opérateur dédiée. Il est de très haut débit et dispose d'une haute disponibilité (redondant).

Il est construit autour d'une boucle doublée et de « pétales » rattachés à celle-ci. Cet ensemble s'appuie sur le protocole MPLS et permet de réaliser des liaisons niveau 3 VPN et VPLS pour des besoins spécifiques. Tous les équipements de routage et de filtrage, constituant le réseau ELICE, sont doublés afin d'assurer la redondance en cas de défaillance d'un équipement.

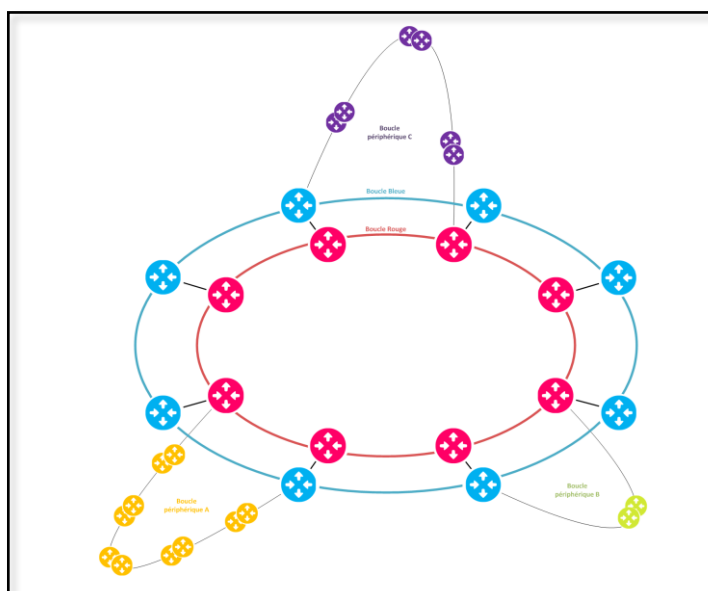


Figure 3 - Le réseau Elice

La plupart des sites bénéficient d'une sécurisation de niveau 3 (double adduction, double pénétration sur le site). 4 sites bénéficient d'une sécurisation de niveau 2 (double adduction, simple pénétration sur le site). 3 des 5 sites de Province bénéficient d'une sécurisation d'accès au réseau ELICE via liaisons opérateurs.

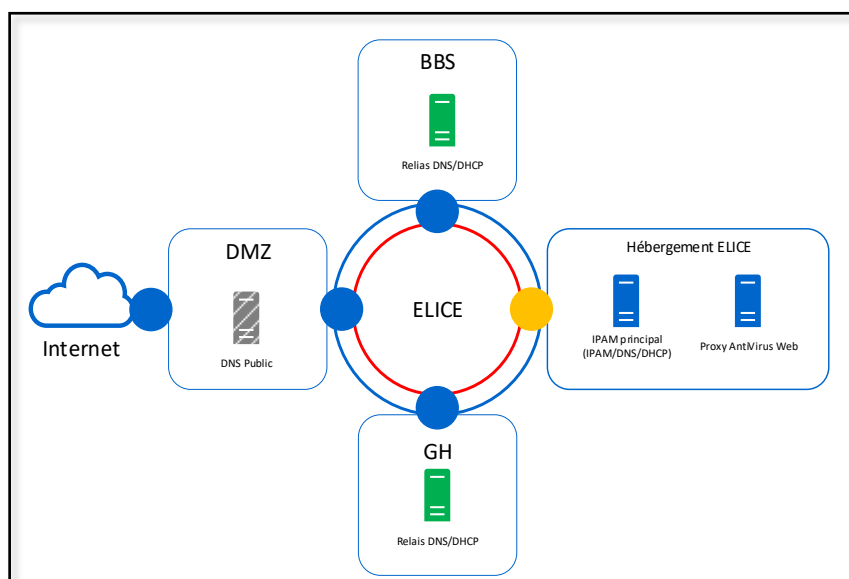
Les débits d'accès des sites sur ce réseau varient de 100Mb/s à 1Gb/s selon les sites. Les deux sites Datacenter disposent d'accès redondé à 10Gb/s. Un troisième site (salle serveurs) hébergeant les éléments de synchronisation ou d'arbitrage pour les solutions en haute disponibilité dispose d'un accès 10Gb/s pour l'extension niveau 2 des deux datacenters principaux.

Les très petits sites annexes (ex : Centres Médicaux Psychologiques) sont interconnectés au SI de l'AP-HP via MPLS opérateur. Les débits d'accès varient selon le besoin de chaque site dans la limite de l'éligibilité du site. Les flux transitant sur les réseaux de l'AP-HP sont uniquement des flux IP dont le filtrage est réalisé par des firewalls en haute disponibilité au niveau des différentes zones de sécurité : Internet, DMZ, zone serveurs BBS, GH/Sites, ....).

## LES SERVICES HEBERGES SUR LE RESEAU ELICE

Le réseau ELICE héberge des services communs aux différents hôpitaux et à la zone serveurs BBS :

- La **solution IPAM** (IP address management) en haute disponibilité avec des satellites locaux sur les GH. Celle-ci regroupe les fonctionnalités IPAM, DNS et DHCP. Chaque GH a la délégation sur son sous-ensemble pour les fonctionnalités DNS et DHCP exclusivement.
- La **solution de proxification** des flux HTTP/HTTPS pour l'ensemble des utilisateurs des sites/GH. Cette proxification est utilisée afin d'accéder à des ressources web disponibles sur Internet et sur les différents sites hospitaliers. Celle-ci porte en complément une analyse antivirus des flux.



*Figure 4 - Services hébergés ELICE*

**O** L'ensemble des flux web échangés entre un site et une ressource internet en HTTP/HTTPS doit utiliser la solution de proxification.

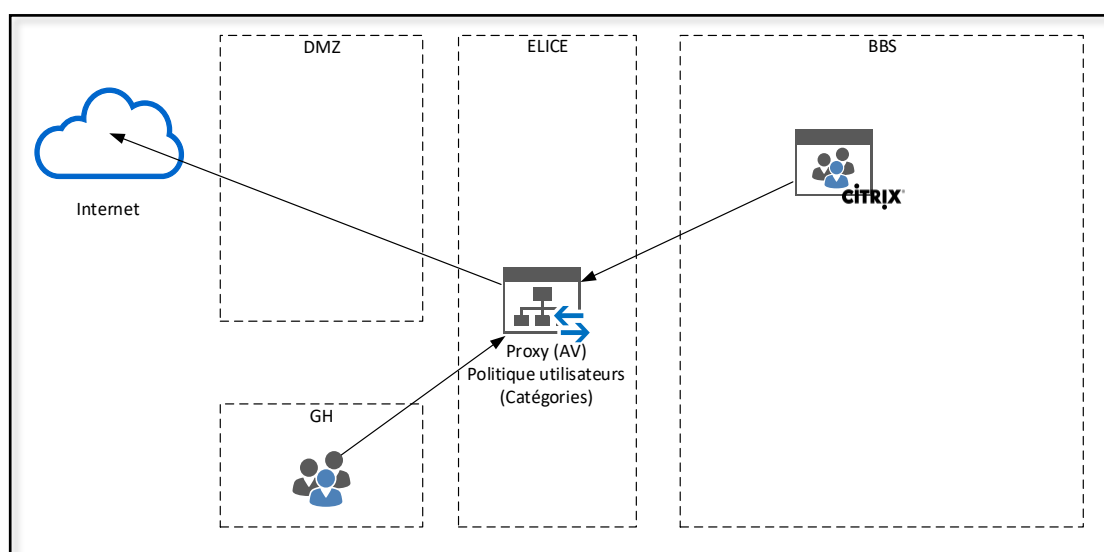
**O** Tous les flux web sortant du SI de l'AP-HP vers Internet doivent passer par un proxy assurant la rupture du flux et l'analyse antivirus.

Les utilisateurs ou serveurs Citrix hébergeant des contextes utilisateurs doivent obligatoirement passer par les proxy hébergés dans la zone d'hébergement ELICE.

**I** Les infrastructures hébergées dans la zone BBS ne peuvent accéder à Internet à l'exception de serveurs explicitement identifiés et dédiés à cette action.

A titre d'exemple, les procédures de mise à jour des systèmes et des applicatifs ne doivent pas récupérer les composants logiciels chez les éditeurs depuis les infrastructures sources de l'AP-HP mais doivent passer par des infrastructures intermédiaires de dépôts habilitées à communiquer avec ces éditeurs.

Tout accès à une URL non référencée en liste blanche et ne provenant pas d'un serveur identifié et légitime de la zone BBS est interdit et bloqué.



*Figure 5 – Proxification*

## LES DATACENTERS

L'architecture d'hébergement de l'APHP est composée de deux réseaux physiques distribués sur deux sites :

- Datacenter 1
- Datacenter 2

L'interconnexion entre les deux Datacenters est composée de deux liaisons fibre optique empruntant un chemin totalement distinct. Chacune des fibres optiques est éclairée à chaque extrémité par des équipements Dense Wavelength Division Multiplexing (DWDM) délivrant les services suivants :

- 2 Fiber Channel (FC) 8/16 Gb/s
- 14 Ethernet 10 Gb/s

Chaque chemin est redondé par l'autre avec une bascule automatique en moins de 50ms en cas d'incident et avec le maintien de la bande passante.

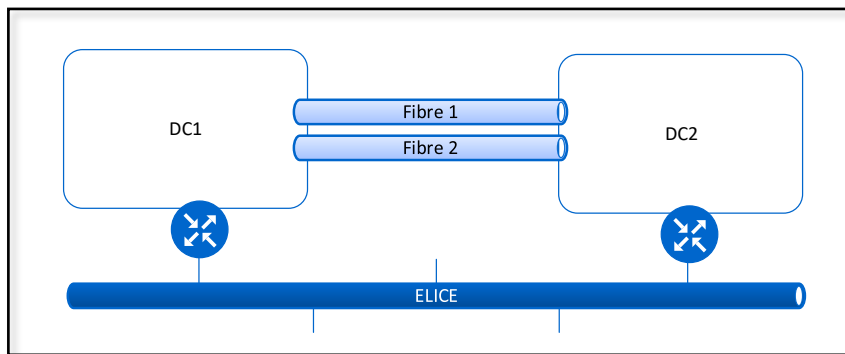


Figure 6 - Interconnexion Datacenters

Les deux Datacenters hébergeant les applications et les services centralisés ont un débit d'accès principal redondé à 10Gb/s.

Une troisième salle serveurs héberge les éléments de synchronisation ou d'arbitrage pour les solutions en haute disponibilité, ainsi que des environnements de qualification. Ce troisième site dispose d'un accès à 10Gb/s redondé et d'une infrastructure réseau hautement disponible. Ce site est accessible au travers du réseau Elice uniquement via un niveau 2 VPLS actif/passif vers les deux autres Datacenters.

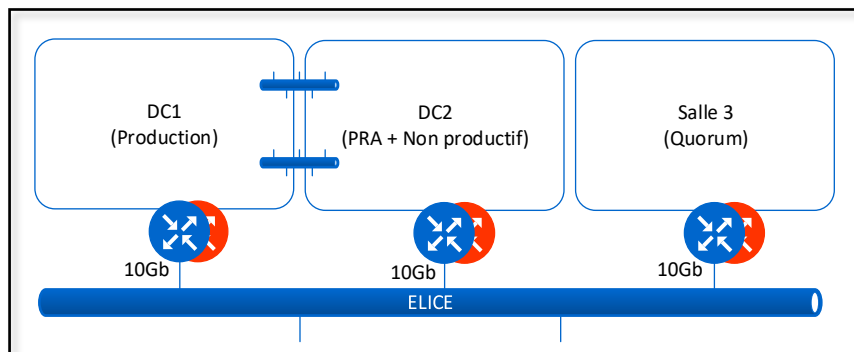


Figure 7 - Les principaux sites d'hébergement

## ACCES INTERNET

L'AP-HP dispose d'un accès Internet à 3 Gb/s. Cet accès est redondé sur les deux Datacenters. Il est en actif / passif. Il peut être évolutif jusqu'à 16 Gb/s. Il est utilisé :

- par l'ensemble des personnels de l'APHP pour accéder ou recevoir des données d'Internet
- par des solutions exposées sur Internet
- par les solutions échangeant des données avec des partenaires
- par le réseau WIFI public/écoles

L'accès Internet est protégé par deux Firewalls et deux routeurs (FAI) qui sont doublement connectés sur les cœurs de réseau de la Zone Intranet.

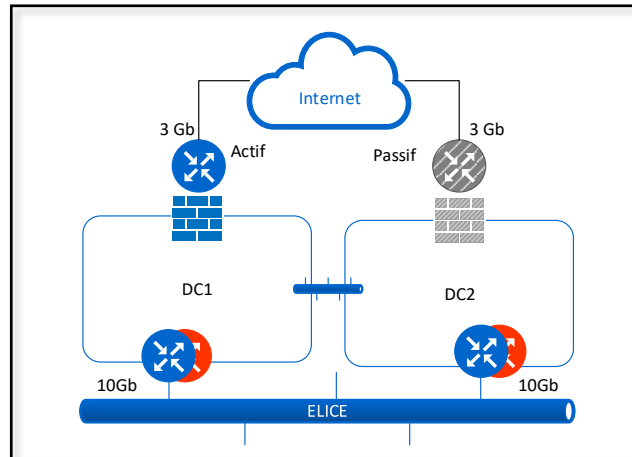


Figure 8 - Accès Internet

L'opérateur Internet fournit une protection contre les attaques par déni de service (Distributed Denial Of Service – DDOS). Celle-ci est directement portée par l'infrastructure de celui-ci.

### PASSERELLE D'INTERCONNECTION FILTREE (DMZ)

L'interconnexion entre Internet et le réseau de l'AP-HP est effectuée grâce à une zone physiquement dédiée et hébergeant des équipements de filtrage de flux.

Cette zone est étendue sur les deux emplacements physiques via des équipements de commutation en full-mesh.

Cette passerelle d'interconnexion nommée DMZ héberge les équipements de filtrage permettant de dépolluer les flux entrants et de maîtriser les flux sortants.

**O** Tout flux venant de l'extérieur du SI passe obligatoirement par des éléments de filtrage hébergés en DMZ.

**I** Aucun flux venant de l'extérieur du SI AP-HP et allant directement vers la zone sécurisée BBS n'est autorisé

Aucun flux initié depuis la DMZ et allant vers la zone sécurisée BBS n'est autorisé sauf exception explicitement validée par le RSSI de l'AP-HP

Le filtrage des accès depuis l'extérieur ou avec les DMZ est assuré par des Firewalls redondés pour le niveau 3 et 4 (modèle OSI). De plus ceux-ci assurent une analyse au niveau 7 (OSI) au travers de la fonctionnalité embarquée de prévention des intrusions (Intrusion Prevention System – IPS).

L'AP-HP dispose d'une infrastructure de Firewall Applicatif Web (WAF) permettant de sécuriser les accès aux services WEB hébergés dans le SI de l'AP-HP et exposés sur Internet.

**O** Tous les flux web provenant d'Internet et entrant dans le SI de l'AP-HP doivent être analysés par la solution de firewall applicatif (WAF) de DMZ.



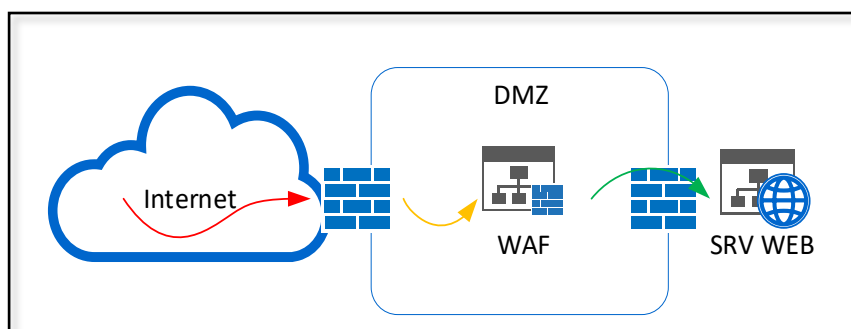


Figure 9 – WAF

## CONNEXIONS AVEC LES PARTENAIRES

Les partenaires ou prestataires de l'AP-HP peuvent accéder aux équipements et applications de l'AP-HP, pour en assurer la télémaintenance ou pour des échanges nécessaires avec le SI de l'AP-HP, par l'intermédiaire de plusieurs types de connexion :

Type de connexion	Cas d'usage
<b>VPN SSL</b>	<p>Le VPN SSL est utilisé notamment pour des échanges qui ne nécessitent pas de connexions initialisées depuis le réseau AP-HP</p> <p>L'accès au VPN SSL est soumis à l'authentification. Les comptes d'accès doivent être nominatifs. Les comptes génériques ne sont plus supportés hormis dérogation pour des cas particuliers après validation de l'équipe Sécurité Opérationnelle de la DSI de l'AP-HP</p>
<b>VPN Site - Site</b>	Il permet de répondre au besoin d'échanges initiés depuis l'AP-HP vers le partenaire et inversement.
<b>MPLS Partenaires</b>	<p>Il répond au besoin d'échange avec qualité de service (QoS)</p> <p>Toutes les connexions distantes sont centralisées en un point unique et redondé de l'AP-HP.</p> <p>Un VPN Partenaire est construit sur une architecture de type Hub &amp; Spoke. La partie Hub (point d'accès central à 10Mb/s en actif/passif) est réalisée au niveau des deux Datacenters. Les sites partenaires sont les Spokes. Les partenaires ne se voient pas entre eux et ne peuvent communiquer entre eux. Toutes leurs communications se font uniquement avec la partie Hub.</p> <p>L'accès MPLS Partenaires bénéficie de QoS (transport de flux de données et de voix).</p>
<b>MPLS APHP</b>	<p>Les sites clients raccordés au réseau MPLS de l'AP-HP sont principalement mis à disposition des hôpitaux. Ils sont au nombre de 15 à ce jour et sont raccordés au réseau MPLS APHP.</p> <p>Tous ces sites distants sont raccordés en un point unique et redondé de l'AP-HP.</p> <p>Ce MPLS AP-HP est construit sur une architecture de type Hub &amp; Spoke. La partie Hub (point d'accès central à 90Mb/s en actif/passif) est réalisée au niveau des deux Datacenters. Les sites distants sont les Spokes. Ils ne se voient pas entre eux et ne</p>

	peuvent communiquer entre eux. Toutes leurs communications se font uniquement avec la partie Hub. L'accès MPLS AP-HP bénéficie de QoS (transport de flux de données et de voix).
<b>MPLS 3G</b>	Le VPN MPLS 3G permet aux détenteurs de clés 3G SFR de l'AP-HP de se connecter au réseau APHP sans passer par l'accès internet. Ce réseau est raccordé sur les firewalls de la DMZ du SI de l'AP-HP.
<b>MPLS ADMIN</b>	Cet accès permet de se connecter aux équipements réseaux des Datacenters sans passer par les équipements de routage quel que soit l'état du réseau.
<b>ROSES</b>	ROSeS (Réseau Optique Sécurisé pour la E-Santé) fédère tous les types d'établissements de santé en Île-de-France, du Cabinet Privé au Centre Hospitalier, autour d'un réseau de télécommunication sécurisé et à haut débit. Le réseau de l'AP-HP dispose d'une interconnexion avec le réseau ROSeS, à 1Gb/s et redondée au niveau des deux Datacenters.

## LE RESEAU BBS (ZONE SERVEURS CENTRALE)

Le réseau BBS hébergeant les serveurs centraux du SI de l'AP-HP est étendu sur les deux Datacenters de l'AP-HP, et dispose d'un double raccordement au réseau d'interconnexion ELICE. L'infrastructure de ce réseau de production est redondée.

La zone BBS n'inclut pas la zone DMZ qui est une zone de sécurité spécifique et indépendante.

### Adressage et routage réseau

Le réseau BBS est défini sur un réseau privé faisant référence à la RFC 1918 en classe B.

**I** Ce réseau est dédié à cette zone et ne peut être utilisé autre part au sein du SI de l'APHP.

**O** Un VLAN doit être dimensionné selon des plages d'adresses IP soit en /24, soit en /23.  
Un VLAN est de classe C

**R** Les plages d'adresses IP en /24 (256 adresses) sont recommandées  
Il est recommandé de dimensionner les sous-réseaux d'interconnexion sur des plages IP restreintes (/27, /28, /29).

### Filtrage

Tous les segments réseaux de BBS sont distribués par des switchs de niveau 2.

Les VLANs routés sont acheminés aux firewalls pour assurer une meilleure maîtrise des flux échangés au sein de la zone. Certains réseaux sont distribués sur les deux datacenters. D'autres sont spécifiques à chaque site.

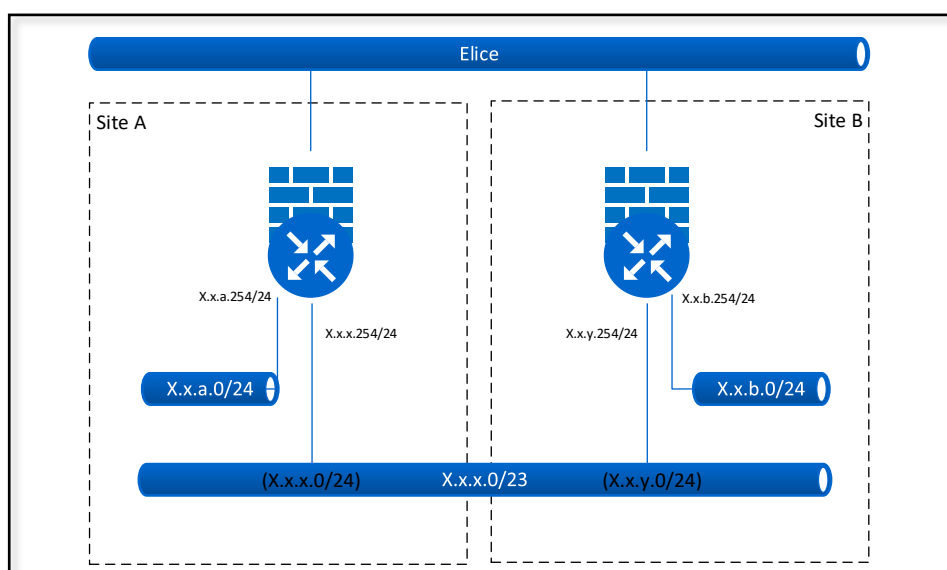


Figure 10 – Filtrage (I)

Des VLANs non routés sont présents au sein de la zone et ne sont donc portés que par les équipements de niveau 2.

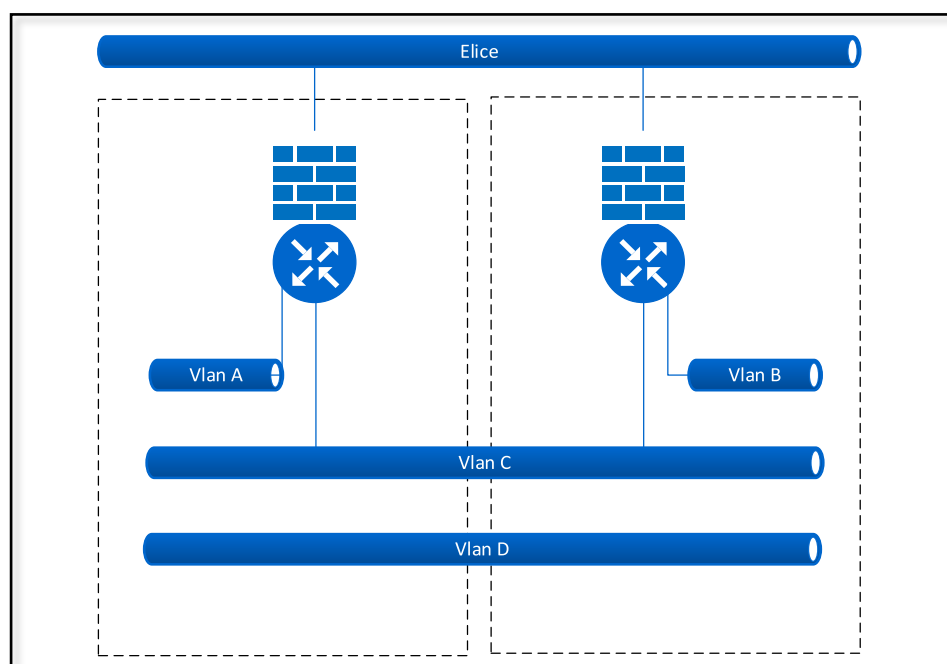


Figure 11 - Filtrage (II)

## Sécurisation périmétrique

La zone BBS héberge toutes les applications centralisées. Cette zone est composée de quatre firewalls physiques en clusters actif / passif croisés (premier cluster actif sur le premier datacenter et second cluster actif sur le second datacenter). Cette solution permet d'acheminer le flux au point de routage/filtrage le plus proche.

**O** Tous les flux entrant et sortant de la zone de sécurité BBS doivent être filtrés par les firewalls de la zone.

**I** Aucun flux entrant ou sortant de la zone de sécurité ne peut contourner le filtrage assuré par les firewalls de la zone.

## Les types de réseaux

Le réseau BBS se segmente en 4 réseaux différents définis en fonction des types de flux de données

- flux métier
- flux d'infrastructure
- flux de sauvegarde
- flux d'administration

Ce découpage permet de séparer les catégories de flux de données (en ne mélangeant pas les flux de données « métier » et les flux de données « techniques »), de garantir une disponibilité forte des infrastructures et d'assurer un niveau de sécurité élevé. Le filtrage entre les réseaux se fait par des équipements dédiés à la catégorie des flux traités.

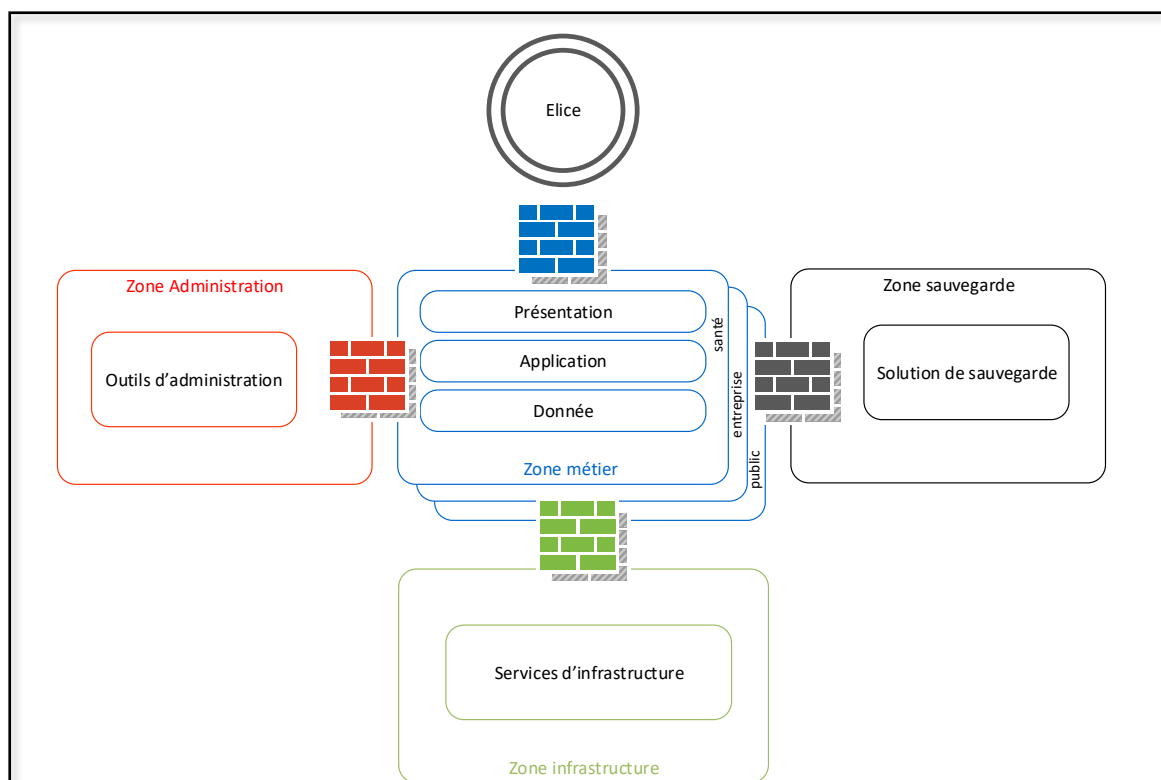


Figure 12 - Séparation des flux

Le réseau de service métier héberge l'ensemble des serveurs mis en œuvre pour les solutions métier.  
 Le réseau d'administration héberge les équipements servant à l'administration des solutions (outils d'administration et interfaces d'administration des serveurs à administrer).  
 Le réseau d'infrastructure héberge les équipements délivrant un service d'infrastructure technique aux solutions métiers (supervision, résolution de nom ...)  
 Le réseau de sauvegarde héberge les éléments constitutifs de la solution de sauvegarde (outils de sauvegarde et interfaces de sauvegarde des serveurs dont les données sont à protéger).  
 Les serveurs sont rattachés aux différents réseaux présentés ci-dessus par l'intermédiaire d'interfaces dans chaque zone réseau.

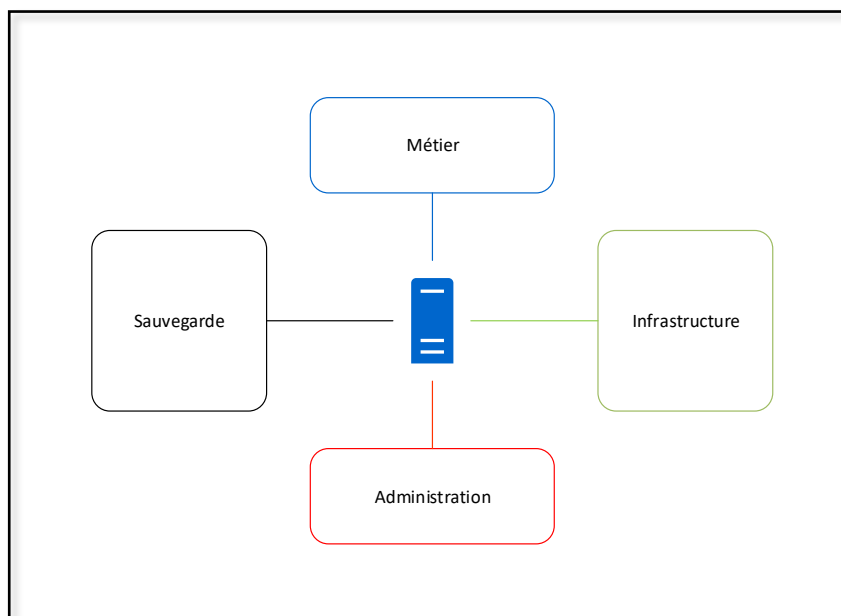


Figure 13 - Interfaces réseau d'un serveur

- Les échanges entre serveurs métier doivent être réalisés au travers des interfaces réseau métier de ceux-ci.

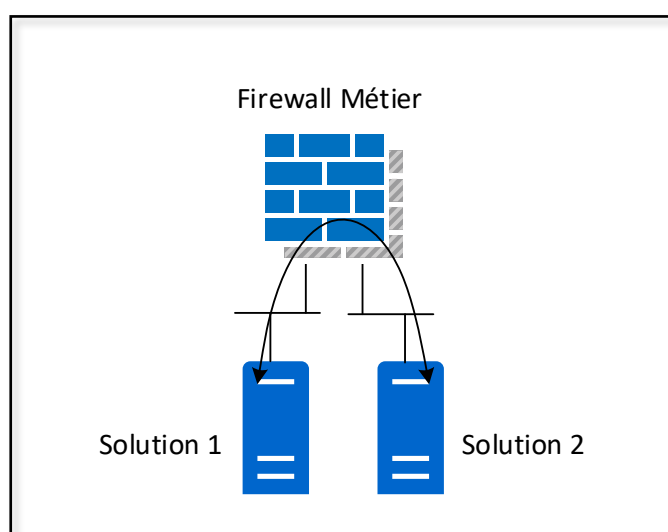
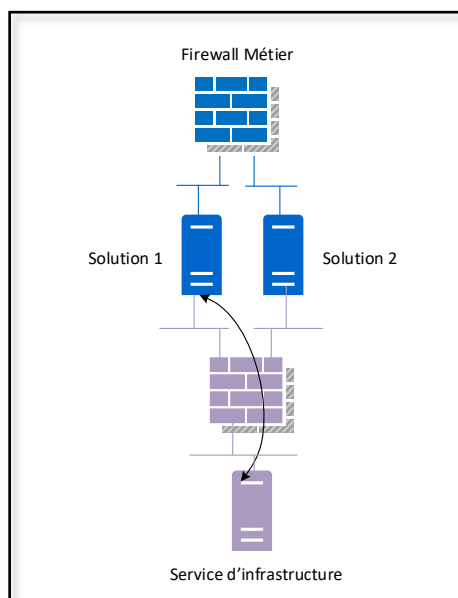


Figure 14 - Flux métier entre serveurs

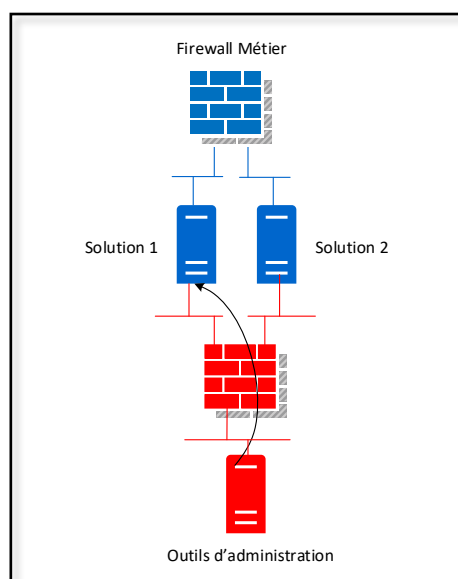
- Les échanges entre un serveur métier et un service d'infrastructure (exemple DNS, NTP, AD) doivent se faire au travers de l'interface d'infrastructure des serveurs.

Ces flux traversent un firewall dédié aux flux d'infrastructure : le firewall d'infrastructure.



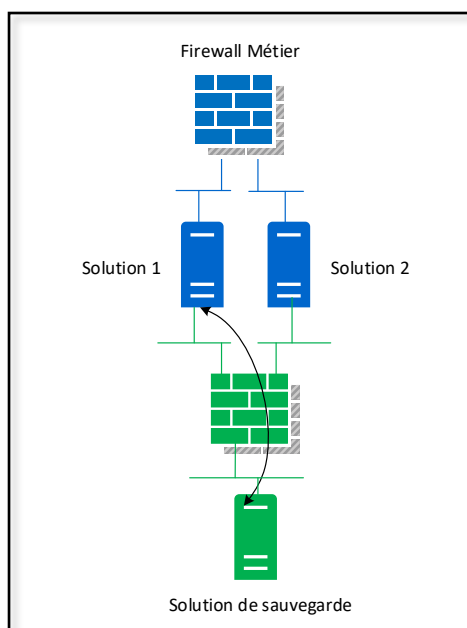
*Figure 15 - Flux d'infrastructure depuis un serveur métier*

- L'administration du serveur doit être réalisée au travers du réseau d'administration et spécifiquement par l'interface d'administration du serveur.



*Figure 16 - Flux d'administration vers un serveur métier*

- Les flux de sauvegarde doivent transiter au travers des interfaces de sauvegarde dédiées des serveurs



*Figure 17 - Flux de sauvegarde et de restauration d'un serveur*

Ce découpage constitue une cible à mettre en œuvre dans le SI de l'AP-HP dans la mesure où le SI n'a pas été historiquement construit de cette manière.

#### Le réseau de service métier

##### *a) Principe de cloisonnement par couche*

Les architectures applicatives de l'APHP doivent être composées de modules distincts permettant de prendre en charge indépendamment les rôles de serveur de présentation, de serveur applicatif et de serveur de données.

Les services d'une couche sont mis à disposition de la couche supérieure.

Le rôle de chacune des couches et leurs interfaces de communication étant bien définis, les fonctionnalités de chacune d'entre elles peuvent évoluer sans induire de changement dans les autres couches.

Le découpage en couches successives permet d'assurer une défense en profondeur et protéger les biens essentiels, les données.

Il est admis qu'il peut exister des couches mixtes en fonction des contraintes liées à l'ancienneté des architectures applicatives. Il est donc possible dans des cas exceptionnels de regrouper des serveurs de présentation avec des serveurs d'application dans une même couche. Cela n'est pour autant pas une pratique encouragée au sein de l'APHP.

Toutes les nouvelles applications doivent prendre en compte les principes d'architecture N-Tiers.

**O** Les applications N-tiers doivent être découpées en couches successives selon le modèle suivant : présentation, applications, données

**I** Les applications monolithiques (tous les composants installés sur une même infrastructure) ne respectant donc pas ce cloisonnement par couche sont interdites

**I** Une couche ne peut invoquer les services d'une couche plus basse que la couche immédiatement inférieure ou plus haute que la couche immédiatement supérieure (chaque couche ne communique qu'avec ses voisins immédiats).

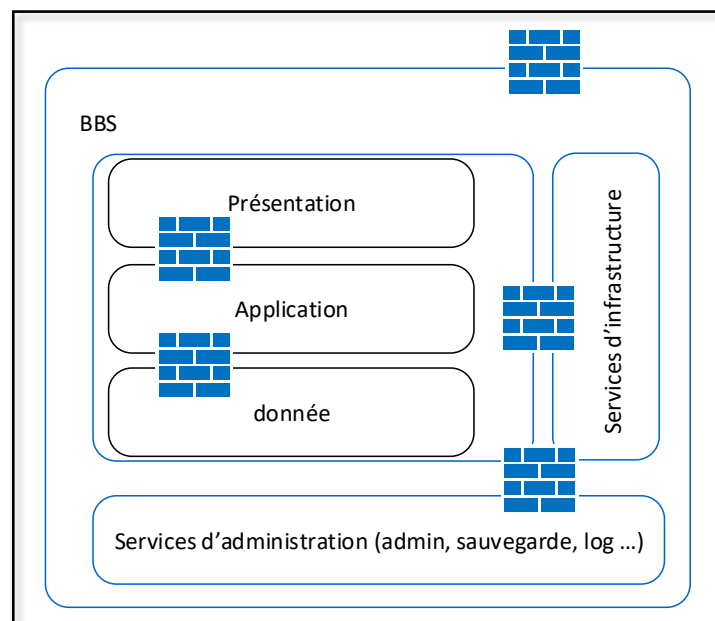


Figure 18 - Découpage en couches

**R** Si une application est composée d'un ensemble de composants portant des fonctions différentes, il est recommandé de séparer et de distribuer les composants sur des infrastructures différentes afin de permettre une meilleure évolutivité technique de chacune des fonctions (répartition de charge, résilience ...)

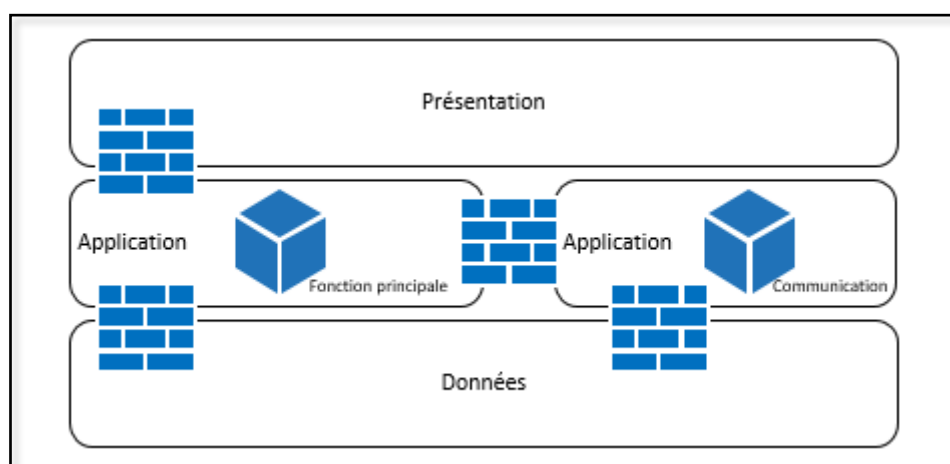


Figure 19 - Séparation des fonctions



### *b) Découpage selon la sensibilité des données*

L'AP-HP traite cinq niveaux de sensibilité de données :

- Données publiques
- Données confidentielles entreprise
- Données de santé
- Données de recherche
- Données HDS (Hébergement de Données de Santé)

Ainsi, les données et les applications doivent être regroupées en fonction de leurs sensibilités. Ce cloisonnement est effectué à la fois par le filtrage des firewalls et par croisement par VLANs. Dans certains cas, cette séparation peut être effectuée en utilisant du matériel physique dédié.

**O** Les applications et les données doivent être regroupées par niveau de sensibilité.

**R** Il est recommandé de mettre les applications et les données de niveau « données de santé » sur des infrastructures physiques différentes de celles hébergeant les applications et les données des autres niveaux de sensibilité.

**I** Des applications et des données de niveaux de sensibilité différents ne peuvent être hébergées dans un même VLAN.

### *c) Gestion des flux web utilisateurs*

Un flux entrant vers une ressource interne passe par un reverse-proxy :

**O** Les flux web entrants en provenance des utilisateurs internes ou externes doivent passer par les reverse proxy de la zone BBS avant d'être redistribués vers le serveur de présentation hébergeant le service web cible.

Le rôle d'un reverse-proxy dans BBS est de fournir des mécanismes de filtrage et, éventuellement, la connaissance des applications accessibles au travers du protocole HTTPS. Il assure par conséquent la redirection à effectuer pour assurer le lien entre une URL saisie et le serveur à contacter.

Un reverse-proxy est contacté par les navigateurs des postes clients à partir des informations fournies par le fichier « pac » chargé automatiquement au démarrage du navigateur (cf. la section relative au poste de travail).

**O** Chaque poste de travail de l'AP-HP doit utiliser le script d'autoconfiguration suivant pour les accès internet

- Pour les accès à internet : <http://proxy.aphp.fr/inter.pac>
- Pour les accès intranet : <http://proxy.aphp.fr/intra.pac>

Dans le cas où la configuration automatique n'est techniquement pas possible, il faut utiliser la configuration proxy manuelle suivante :

- Accès internet : proxym-inter.aphp.fr avec le port 8080
- Accès intranet seulement : proxym-intra.aphp.fr avec le port 8082.

Un reverse-proxy peut permettre l'authentification des utilisateurs de manière nominative. Il relaie ces informations d'identification aux serveurs de présentation des applications concernées. Ceci impose aux serveurs d'applications d'héberger des applications permettant la réception transparente pour l'utilisateur des informations de connexion. En effet les serveurs d'application doivent continuer à authentifier les utilisateurs (principe de défense en profondeur).

Une application métier ne peut être jointe directement par un utilisateur

**R** Pour les applications web accessibles en Intranet et celles accessibles depuis Internet, il est recommandé de faire passer le flux au préalable par un reverse-proxy de la zone BBS

C'est donc le reverse-proxy qui offre le lien entre une URL métier et un serveur de présentation. Afin de garantir la confidentialité des informations échangées entre d'une part l'utilisateur et le reverse-proxy et d'autre part entre le reverse-proxy et le serveur de présentation, les échanges doivent être réalisés de manière sécurisée.

**O** Les échanges entre un poste client et le reverse-proxy puis entre le reverse proxy et le serveur de présentation doivent être réalisés au sein d'une connexion sécurisée SSL.

Un reverse-proxy étant accédé par les utilisateurs, il est impératif qu'il puisse présenter un certificat serveur l'authentifiant. Ce certificat serveur doit naturellement être reconnu par les navigateurs des postes clients.

**R** Il est recommandé d'assurer les fonctions suivantes grâce à un reverse-proxy :

- rôle de cache pour les entêtes de données fixes (images, CSS, javascript)
- répartition de charge lorsque les serveurs de présentation sont plusieurs à rendre le même service
- redondance des accès en cas de panne si les serveurs de présentation sont multiples.

**R** Il est recommandé de faire transiter par un WAF les flux web en provenance des postes clients ou de la DMZ

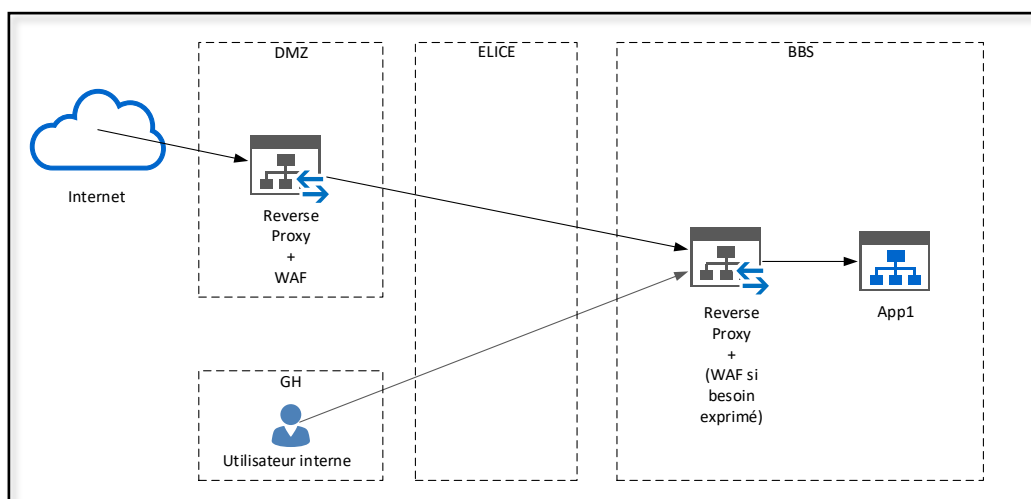


Figure 20 - Flux entrant et reverse-proxy

## LES RESEAUX LAN ETHERNET DES ETABLISSEMENTS

Les réseaux LAN des établissements de l'AP-HP sont constitués d'un cœur de réseau redondé qui réalise le routage entre les différents Vlan du réseau d'établissement.

Les réseaux LAN des sites disposent d'un double attachement au réseau ELICE avec redondance du routeur et firewall d'accès (haute disponibilité, en actif/standby).

Les fonctionnalités de détection et de réparation de liens (VRRP) sont mises en œuvre.

## WLAN

Les sites de l'AP-HP sont équipés de Wireless LAN en couverture totale ou partielle supportant les réseaux WIFI métiers et les réseaux WIFI dédiés au public et aux écoles.

Les réseaux WIFI public/écoles sont transportés sur ELICE au travers d'un réseau dédié étanche de type VPLS assuré par le WAN de l'AP-HP. Une infrastructure physique dédiée est déployée en central sur les Datacenters pour assurer la sécurité de ces WIFI publics (authentification, filtrage, proxy, ...). Ces réseaux WIFI publics partagent l'accès Internet de l'AP-HP.

- La sécurité wifi sur les sites AP-HP doit être a minima en 802.1x MSCHAP v2, avec chiffrement WPA2.

## LA QUALITE DE SERVICE (QoS)

La politique de QoS définie à l'AP-HP, consiste à marquer les flux en fonction de la criticité des applications mais aussi en prenant en compte les contraintes techniques de certains flux comme les flux voix ou les flux nécessitant une faible latence. La priorisation des flux s'appuie sur la norme DIFFSERV.

Un modèle à 5 classes de services (CoS) a été retenu afin de ne pas complexifier l'implémentation et la gestion de la QoS sur les réseaux de l'AP-HP :

- Une classe prioritaire pour les flux de gestion réseau afin d'assurer le bon fonctionnement du réseau même en cas de congestion ;
- Une classe ToIP : elle a pour but d'accueillir le trafic de téléphonie sur IP (ToIP). Ce trafic exige un faible délai, une faible gigue, un faible taux de perte de paquets et une faible bande passante pour sa transmission (en effet une communication de type voix sur IP [VoIP] ne nécessite jamais plus de ~100 kbps). Ce trafic sera d'une priorité absolue ;
- une classe Visio : cette classe a pour but d'accueillir le trafic de visioconférence. Ce trafic exige un faible délai, une faible gigue, un faible taux de perte de paquets mais est susceptible de consommer beaucoup de bande passante pour sa transmission ;
- Une classe Data Critique : cette classe a pour but d'accueillir les applications critiques de l'AP-HP ainsi que le trafic de signalisation de la ToIP. Cette classe est considérée comme moins sensible au délai, à la gigue, peut accepter plus de pertes de paquets mais est par contre susceptible de consommer beaucoup de bande passante ;
- Une classe best effort : cette classe est la classe par défaut pour les applications restantes. Elle n'a aucune contrainte.

L'implémentation de la QoS sur les LAN est réalisée au fur et à mesure des besoins et lorsque c'est le cas, elle est implémentée de bout-en-bout. Tous les équipements réseau intermédiaires traitent la QoS sans en modifier le champ DSCP.

Sur les LAN, un re-marquage systématique du champ DSCP est effectué au niveau des équipements réseau d'extrémité pour interdire aux machines connectées (postes de travail, serveurs ou toute autre machine IP) de rendre plus prioritaire leur trafic réseau.

Toute application nécessitant une gestion différente de la QoS (ex : marquage par l'application) doit faire l'objet d'une étude et validation par l'équipe réseau de la DSI de l'AP-HP.

De ce fait, pour toute nouvelle application nécessitant des traitements prioritaires, une matrice des flux est exigée, pour permettre le marquage du trafic réseau en adéquation aux contraintes liées à celle-ci.

Tous les équipements réseaux sont paramétrés pour prendre en compte les différents niveaux de priorité prédéfinis.

Les cœurs de réseau et les équipements du réseau d'interconnexion ne réalisent pas de marquage (sauf dans le cas où des serveurs hébergeant des applications sensibles, seraient connectés directement au cœur de réseau).

## CONNEXIONS

---

**I** Les sessions TCP permanentes sont interdites

**O** L'ouverture d'une session TCP doit gérer un timeout de connexion

- Tout nouveau projet doit élaborer une matrice des flux décrivant l'intégralité des flux à autoriser entre les différents composants utilisés par la solution (poste client, serveurs internes, services externes ...).  
Cette matrice des flux doit respecter le modèle fourni par l'AP-HP  
Cette matrice doit accompagner le dossier d'architecture technique.  
Cette matrice constitue un élément indispensable à la mise en œuvre de toute solution informatique.

## **b. Les serveurs**

### LES SYSTEMES MAINFRAME

---

**I** Les nouveaux systèmes Mainframes d'IBM ne sont plus autorisés au sein du SI de l'AP-HP.

### LES SERVEURS PHYSIQUES

---

#### Règles générales

---

La mise en place d'une infrastructure serveur physique (système d'exploitation installé sur une machine physique) est régie au sein de l'AP-HP par les règles suivantes :

**O** Un logiciel tiers n'ayant pas une méthode de licence conciliante avec la virtualisation est impérativement installé sur une infrastructure physique quel que soit son niveau d'environnement (développement, qualification, production...).  
Exemple : base de données Oracle

**R** Le choix de la mise en place d'une infrastructure physique est limité aux conditions strictes suivantes :

➤ Condition relative au niveau d'environnement cible :

Seuls les environnements 'production', 'pré-production' sont éligibles aux infrastructures physiques (sauf exception comme pour un logiciel tiers voir cadre ci-dessus [Obligatoire]).

➤ Condition relative au type d'applicatif embarqué :

La liste non exhaustive suivante définit les applicatifs éligibles aux infrastructures physiques :

- Les bases de données
- Les systèmes distribués (ex : Mesos, Kubernetes, ...)
- Les clusters
- Les solutions SAP (ECC, BI) pour la « central instance »

#### Format

---

**O** Deux formats de serveurs physiques sont autorisés :

- Le format rack
- Le format châssis/lame, frame/compute

- O** Toutes les lames/computes au sein d'un même châssis/frame appartiennent exclusivement à l'un des deux niveaux d'environnement suivants :
  - production (production, formation)
  - non-production (développement, qualification, ...)

**I** Le mélange de lames/computes d'environnements de production et de non-production au sein d'un même châssis/frame est interdit.

**I** Le format dit « tour » est interdit

## Architecture

---

Deux types d'architectures serveurs cohabitent au sein du SI :

- L'architecture « x86 »
- L'architecture « Itanium »

- O** Toute nouvelle infrastructure serveur mise en place est de type :
  - Architecture « x86 » 64 bits.

**I** L'architecture « Itanium » n'est plus autorisée au sein du SI de l'AP-HP.

**Note** : Le seul cas consenti pour la mise en place d'une nouvelle architecture « Itanium » concerne la consolidation d'infrastructures « Itanium » (de plusieurs serveurs existants déjà vers un seul serveur).

## Infrastructures convergées et hyperconvergées

---

- O** Les infrastructures convergées doivent être en conformité avec les marchés en vigueur concernant l'acquisition et la mise en oeuvre de telles infrastructures.

A date, il s'agit des infrastructures suivantes :

- Oracle Exadata
- HPE Synergy

Les infrastructures hyperconvergées doivent être en conformité avec les marchés en vigueur concernant l'acquisition et la mise en oeuvre de telles infrastructures.

A date, il s'agit des infrastructures suivantes :

- HPE Simplivity

## Interfaces réseaux

Un serveur doit pouvoir accéder aux différents segments réseaux décrits au paragraphe « les types de réseaux ».

- O Tout nouveau serveur doit accéder à tous les segments réseaux à travers une interface dédiée : chaque interface réseau est liée exclusivement à un et à un seul des segments réseaux identifiés

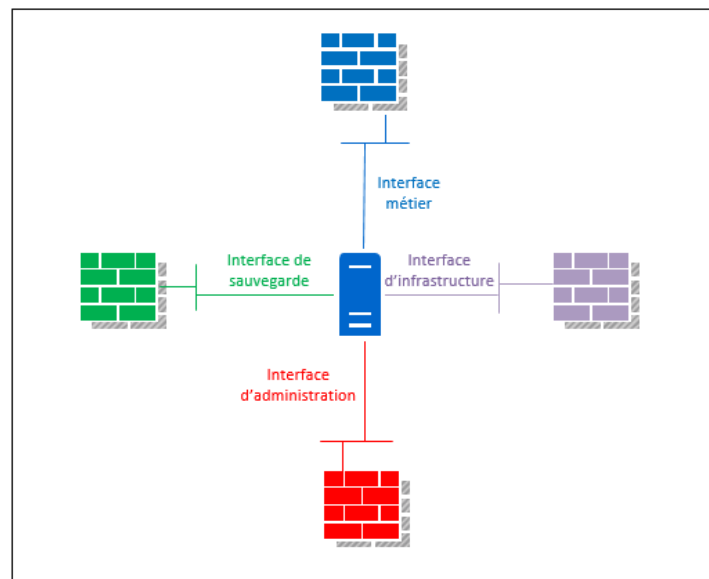


Figure 21 - Interfaces réseau d'un serveur

- R Il est recommandé de mettre en œuvre une haute-disponibilité pour les interfaces réseau suivantes pour les environnements de production :
  - interface réseau d'infrastructure
  - interface réseau de sauvegarde

## LA VIRTUALISATION

### La virtualisation système

#### a) Règles générales

La virtualisation système est une méthode qui permet d'exécuter sur un serveur dit hôte un ou plusieurs systèmes d'exploitation (OS), dans des environnements cloisonnés.

- O Toute virtualisation système dans le SI de l'AP-HP repose sur la solution vSphere de VMWARE



**O** Toute appliance sous environnement virtuel doit être compatible avec la solution de virtualisation VMWare

**R** Toute nouvelle solution sera déployée sous un environnement virtuel (machine virtuelle sur un serveur ESX)

**I** Il est interdit de déployer un environnement virtuel dont les ressources dépassent les caractéristiques suivantes :

- virtuel CPU > 16
- mémoire RAM > 32Go

Il faut privilégier une infrastructure physique pour ce genre de configuration

Un logiciel tiers n'ayant pas une méthode de licence conciliante avec la virtualisation ne doit pas être installé sur machine virtuelle, quel que soit son niveau d'environnement (développement, qualification, production...).

Exemple : base de données Oracle

Il est interdit d'implémenter une machine virtuelle reposant sur les configurations suivantes :

- Pass-through VMDirectPath permettant de présenter et de dédier à la VM un composant matériel de l'hyperviseur
- Affinité CPU permettant d'assigner à la VM un processeur physique spécifique
- Réserve de ressources (CPU/RAM)
- Présentation de stockage en mode bloc de type Raw Device Mapping

Une infrastructure « x86 » hébergeant un socle de virtualisation est mise à disposition pour permettre un déploiement de bases de données Oracle dans un environnement de consolidation. L'éligibilité des applications utilisant cette infrastructure se fait projet par projet.

#### *b) Infrastructures*

**O** Les serveurs sur lesquels est installée la solution de virtualisation sont :

- Soit des serveurs physiques
- Soit des systèmes convergés
- Soit des systèmes hyperconvergés

**O** Une ferme de serveurs ESX dans laquelle des VM sont hébergées et peuvent se déplacer par le mécanisme de vMotion doit être constituée de serveurs ESX identiques

**O** Les VM de production doivent être hébergées sur des serveurs ESX dédiés à l'activité de production

**I** Il est interdit d'installer et de mélanger des VM de production et des VM de non-production sur une même infrastructure virtuelle (ESX seul ou ferme d'ESX)

#### c) Architecture

**O** Un seul type d'architecture pour les serveurs virtuels et l'environnement hôte est autorisé :

- Architecture « x86 » 64 bits.

#### d) Interfaces réseaux

Les règles sont identiques à celles énoncées pour les serveurs physiques.

**O** La haute disponibilité des interfaces réseaux est portée par le serveur hôte ESX

Chaque vSwitch doit être composé d'au moins deux interfaces réseaux physiques ou virtuelles (cas du virtualConnect) pour la configuration du teaming

La haute-disponibilité des interfaces réseaux est assurée par les hyperviseurs (load balancing, network failure, notify switches, failback)

#### e) Stockage

**R** Pour les VM dont le système d'exploitation est Windows, il est recommandé de définir autant de fichiers VMDK que de disques présentés au système d'exploitation

#### f) Fermes ESX

Des fermes de serveurs ESX sont constituées afin

- De répartir l'ensemble des VM en fonction notamment des ressources (grâce au mécanisme de répartition VMWARE DRS)
- De palier le dysfonctionnement d'un ESX au sein d'une ferme en répartissant les VM concernées sur les autres ESX actifs de la ferme

Les fonctionnalités DRS et de haute-disponibilité (redémarrage automatique des machines virtuelles après un incident) sont proposées en standard pour tous les environnements (production et non production) sauf exception explicitement mentionnée dans les livrables de conception.

**O** La répartition des VM sur une ferme de serveurs ESX doit permettre de continuer à absorber la charge globale si un ESX rencontre un incident et ne peut plus héberger de VM

**R** En fonctionnement nominal d'une ferme de serveurs ESX d'un cluster à deux nœuds et d'un cluster étendu, il est recommandé de charger chaque ESX à 50% de sa capacité

## La virtualisation applicative – la conteneurisation

La virtualisation applicative (conteneurisation) est une méthode de virtualisation de système d'exploitation (OS) permettant de lancer une application et ses dépendances à travers un ensemble de processus isolés du reste du système. Comme toute solution de virtualisation, elle nécessite la mise en place d'une infrastructure spécifique liée à la gestion des applications virtualisées (conteneurs).



Docker est le moteur de conteneurisation du SI de l'AP-HP

Kubernetes (K8S) est la solution d'orchestration de conteneurs du SI de l'AP-HP

### a) Infrastructures serveurs K8S

L'infrastructure cluster Kubernetes est découpée en trois zones distinctes afin de respecter le principe de cloisonnement :

- Une zone d'orchestration constituée de plusieurs serveurs (nœuds) typés « Master »
- Une zone dite « Front-End » constituée de nœuds typés « Worker » dédiés à l'hébergement des conteneurs de services de présentation
- Une zone dite « Back-End » constituée de nœuds typés « Worker » dédiés à l'hébergement des conteneurs de services applicatifs

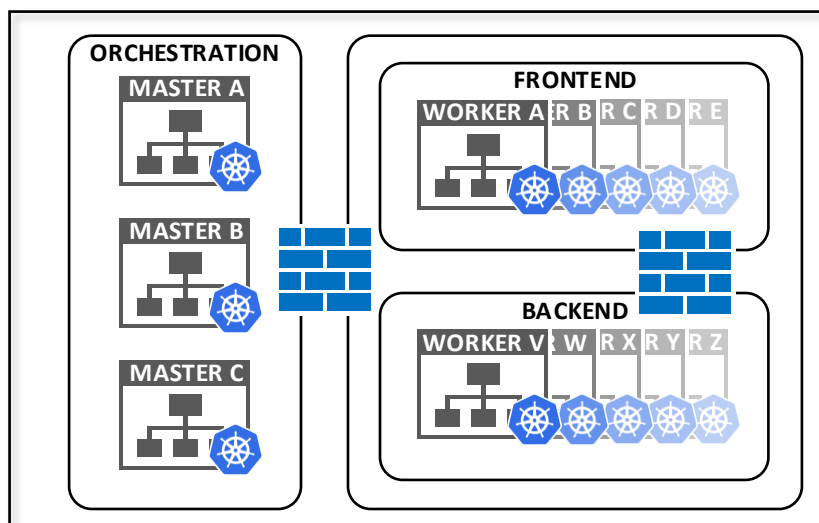


Figure 22 - Cluster Kubernetes

### b) Accès aux services conteneurisés

Le réseau de conteneurs étant un réseau virtuel privé, son accès depuis l'extérieur du cluster Kubernetes est strictement bloqué par défaut. Pour rendre les services frontaux des applicatifs conteneurisés joignables, des contrôleurs dits « Ingress » sont positionnés sur tous les nœuds « Worker » de présentation.

**O** L'accès aux services de présentation des applications conteneurisées doit obligatoirement utiliser une VIP ayant pour cible les « Ingress » des nœuds « worker » du cluster Kubernetes.  
Cette VIP doit être portée par une infrastructure matérielle ou logicielle offrant les fonctionnalités de reverse-proxy, de load-balancing et de web application firewall.

**O** Tout conteneur exposant un service devant être accédé depuis l'extérieur du cluster Kubernetes doit utiliser une règle « Ingress »

**I** Il est interdit d'utiliser la méthode « nodeport » de Kubernetes pour exposer un service.

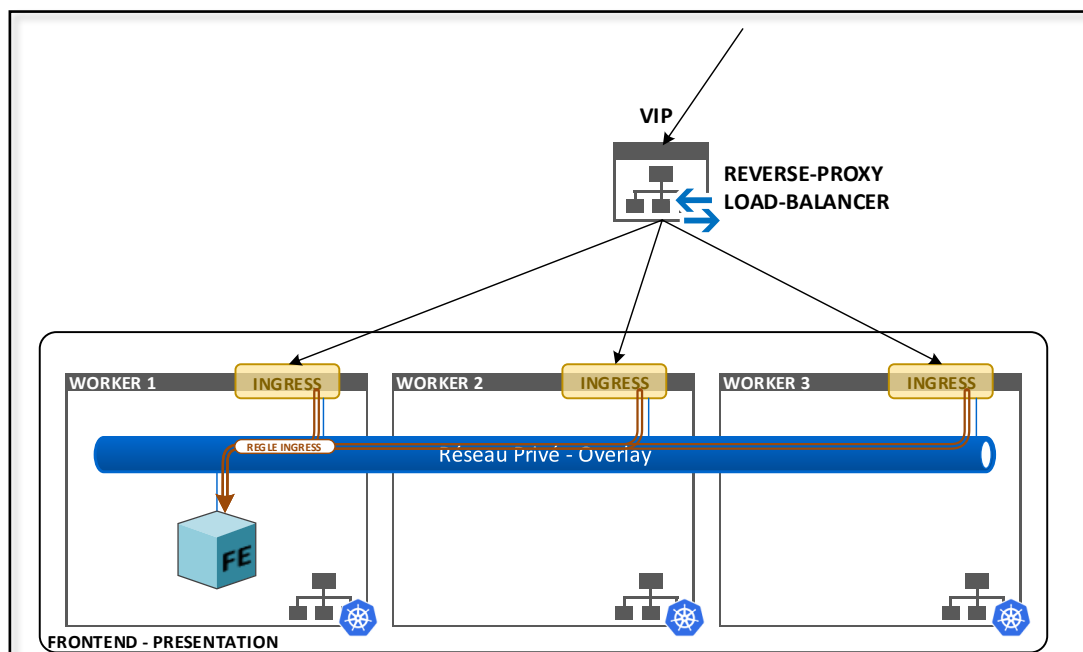


Figure 23 - Accès à un service conteneurisé

### c) Le réseau de conteneurs

Le réseau de conteneurs du cluster Kubernetes est un réseau privé (overlay) agnostique vis-à-vis du réseau d'entreprise. Le filtrage des flux entre conteneurs n'est donc pas réalisé par les éléments de filtrage du réseau d'entreprise, mais par le composant logiciel portant la solution d'overlay : Container Network Interface (CNI) de Kubernetes.

**O** La solution logicielle choisie pour tenir le rôle de CNI doit supporter toutes les fonctionnalités de politique de filtrage implémentées dans Kubernetes.

**I** La solution CNI ne doit pas utiliser le protocole BGP

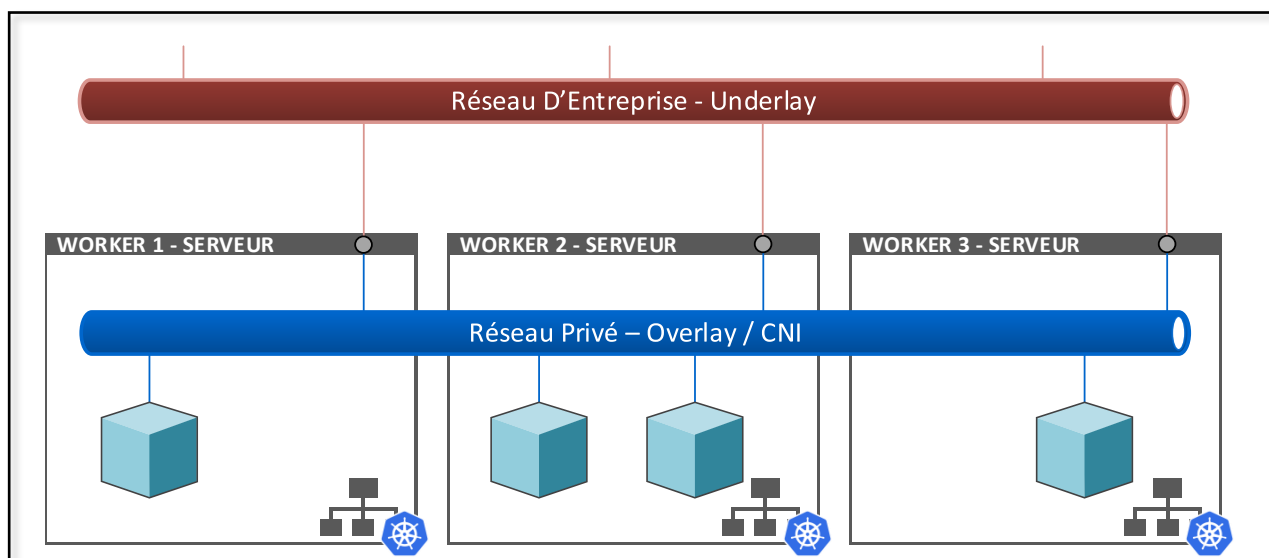


Figure 24 - Réseau de conteneurs (CNI)

#### d) Le cloisonnement

Le cluster Kubernetes a pour vocation de porter un nombre important de solutions applicatives. Afin de maîtriser les ressources et la sécurité de ces solutions, Kubernetes introduit la notion de « namespace » que l'on pourrait résumer à du cluster virtuel.

**O** Toute solution applicative déployée au sein d'un cluster Kubernetes doit être déployée dans un namespace dédié

**O** Toute création d'un namespace s'accompagne d'une limitation des ressources « compute » (CPU) et « mémoire » (RAM).

**O** Toute manipulation d'objets Kubernetes au sein d'un namespace doit être réalisée par un compte de service exclusivement dédié à ce namespace

**O** La politique réseau appliquée par défaut à tout nouveau namespace bloque tous flux

- en provenance d'autres namespaces
- à destination d'autres namespaces

Par défaut, les « namespaces » sont étanches les uns vis-à-vis des autres.

**I** Il est interdit de manipuler les d'objets d'un namespace avec des comptes de service globaux

#### e) Le pod

Le pod est le plus petit objet manipulé par Kubernetes. Un pod est un groupement d'un ou plusieurs conteneurs partageant le réseau. Les conteneurs d'un pod sont toujours localisés ensemble et ordonnés ensemble dans un même contexte d'exécution.

### Composition technique d'un pod

- O** Chaque conteneur d'un pod doit être accompagné d'une limitation de ses ressources « compute » et « mémoire »
- O** Les données persistantes manipulées par un conteneur sont localisées physiquement hors de l'enveloppe image du conteneur
- R** Un pod ne contient qu'un seul conteneur
- I** Il est interdit aux conteneurs d'un pod de manipuler des données persistantes se trouvant localement dans leur image

### Identification d'un pod

- O** Les informations suivantes doivent pouvoir être identifiées dans un pod :
    - Le nom de l'application
    - La version de l'application
    - Un nom unique d'instance applicative
    - Le composant dans l'architecture de la solution
    - Le nom de la solution dont il fait partie
    - Le nom de l'outil utilisé pour son déploiement
- L'utilisation des labels et des annotations est obligatoire pour renseigner toutes ces informations

### Filtrage entre les pods

La politique réseau appliquée par défaut à tout nouveau pod bloque tout flux en provenance d'autres pods et à destination d'autres pods.

- O** Tout flux identifié entre des pods doit faire l'objet d'une politique réseau Kubernetes ingress (flux en entrée) et/ou egress (flux en sortie)
- O** Tout pod déployé au sein du cluster Kubernetes doit être placé dans un namespace dédié à son application

#### f) Les images

Une image de conteneur est un système de fichiers inerte, immuable, comprenant une application accompagnée de toutes ses dépendances. Elle est composée de couches juxtaposées définies lors de chacune des étapes de sa création.

Afin de maîtriser le contenu et la création de l'ensemble de ses images, l'APHP a défini son propre processus de création des images. De ce processus, quatre types d'image sont à générer :

- les images de base : copie validée d'une image d'un éditeur de confiance dans le dépôt privé APHP.
- les images d'entreprise : durcissement et adaptation spécifique APHP de l'image de base.
- les images d'environnement : ajout d'une couche logiciel à l'image d'entreprise.
- les images applicatives : ajout d'une couche applicative spécifique à la solution métier à l'image d'environnement.

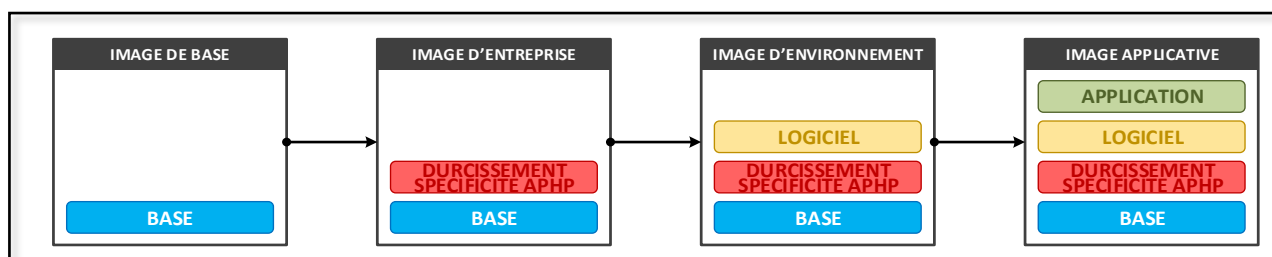


Figure 25 - Création des images

**O** L'image de base est l'image fournie par l'éditeur Red Hat (image non modifiée de l'éditeur)

**O** Les images d'entreprise et d'environnement sont créées dans un workflow interne non spécifique à une solution applicative

**O** Toutes les images applicatives utilisées au sein du SI APHP sont créées :

- dans un workflow interne spécifique à la solution à déployer
- à partir des images d'environnement

**O** La création d'une image doit être reproductible :

- Tous les composants ajoutés à une image font l'objet d'une gestion de version explicite
- Tous les composants ajoutés à une image proviennent d'un dépôt privé local à l'AP-HP

**I** Il est interdit d'utiliser une image téléchargée sur internet

**I** Il est interdit d'ajouter des composants à une image directement téléchargée d'internet



## Choix des systèmes d'exploitation

---

**O** Pour toute nouvelle solution/application du type progiciel, seuls trois systèmes d'exploitation sont supportés :

- Linux
- Windows Serveur
- Unix

**O** Les systèmes d'exploitation doivent être installés dans leur dernière version et leur dernier niveau de mise à jour

**O** La seule distribution Linux autorisée est RedHat Entreprise

La seule distribution Unix autorisée est HP-UX

**R** Dans le cas où une application est compatible avec les trois systèmes d'exploitation autorisés, le système d'exploitation Linux est privilégié

**R** Pour toute nouvelle solution/application construite sous forme de développement spécifique (ne s'appuyant donc pas sur une solution éditeur), le système d'exploitation privilégié est Linux

**I** Il est interdit d'utiliser des systèmes d'exploitation dont la date de fin de support est dépassée, pour la mise en place de toute nouvelle solution

## Mise à jour

---

**O** Tous les systèmes d'exploitation s'interfacent avec leur service de mise à jour centralisé (interne à l'AP-HP) respectif :

- Pour les systèmes RedHat Entreprise Linux : RedHat Satellite
- Pour les systèmes Microsoft Windows : SCCM/WSUS

La mise à jour des systèmes d'exploitation respecte

- la politique du cycle de vie de l'AP-HP des systèmes d'exploitation
- la politique de sécurité de l'AP-HP des systèmes d'exploitation

I Un système d'exploitation ne doit pas être capable de se mettre à jour depuis un dépôt se trouvant en dehors du SI de l'AP-HP (Internet)

### c. Le stockage

#### CONCEPTS

Il faut distinguer :

- Les données utilisées directement par les applications et les utilisateurs à travers leurs travaux de bureautique. Ces données sont stockées sur du stockage dit primaire et doivent faire l'objet d'une stratégie de protection.
- Des données générées par la sauvegarde des données se trouvant sur le stockage primaire. Ces données sont stockées sur du stockage dit secondaire.

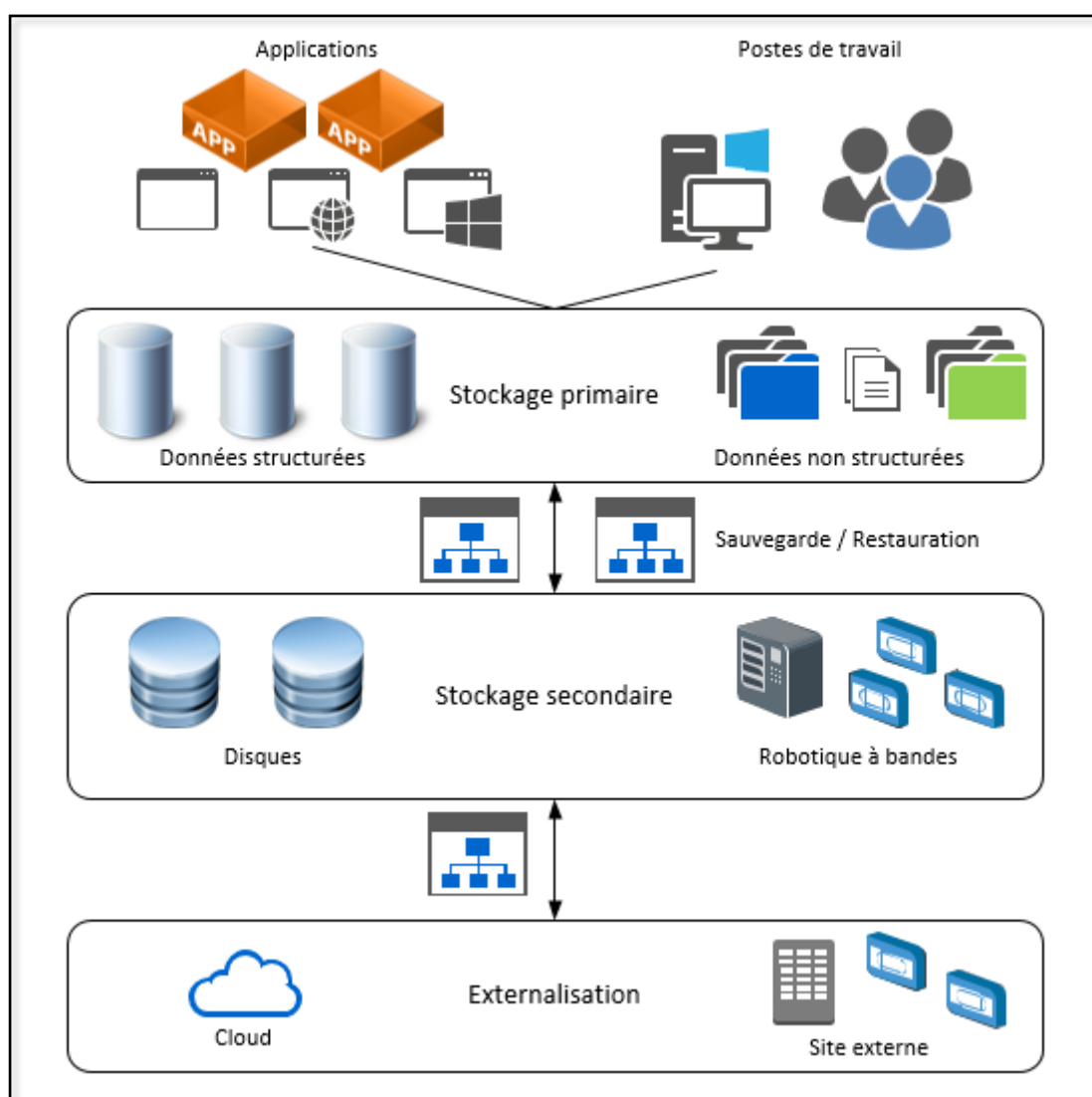


Figure 26 - Catégories de stockage

### Le stockage des systèmes

---

**R** Il est recommandé d'installer

- les hyperviseurs de virtualisation (vSphere de VMWARE)
- les orchestrateurs de conteneur (Kubernetes)
- le système d'exploitation d'un serveur physique

sur les disques locaux de l'infrastructure physique serveur

**O** Le système d'exploitation d'une machine virtuelle doit être installé sur un réseau de stockage SAN

### Le stockage des données

---

#### a) Règles générales

**O** Les données d'un serveur physique et d'un serveur virtuel doivent être hébergées sur un réseau de stockage SAN (Storage Area Network)

**I** Aucune donnée primaire ne peut être disposée sur des infrastructures dédiées au stockage des données issues des sauvegardes (les données secondaires)

#### b) Réseau de stockage SAN

**O** Dans le cas de LUN répliquée par un mécanisme de baie de stockage primaire entre deux datacenters, le multipathing des ordres de lecture / d'écriture doit se limiter à la baie de stockage du datacenter d'où provient l'ordre.

**I** Dans le cas de LUN répliquée par un mécanisme de baie de stockage primaire entre deux datacenters, il est interdit de faire du multipathing des ordres de lecture / d'écriture réparti sur les deux datacenters

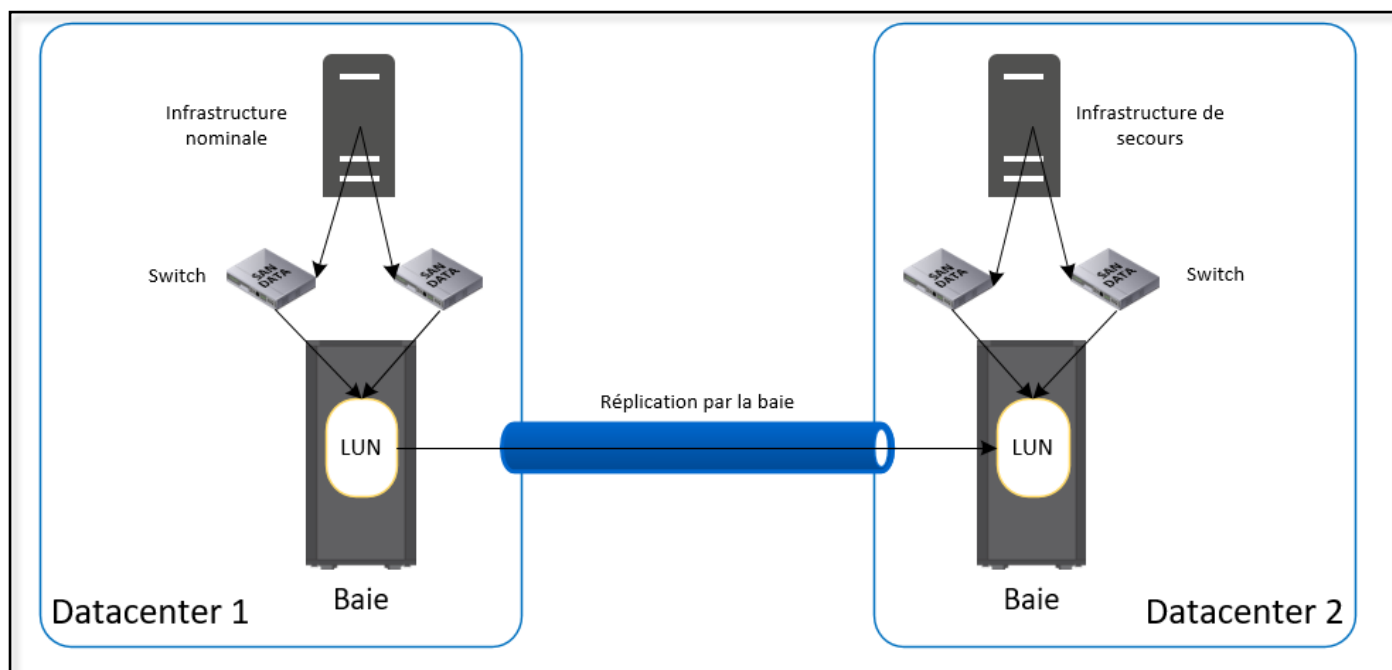


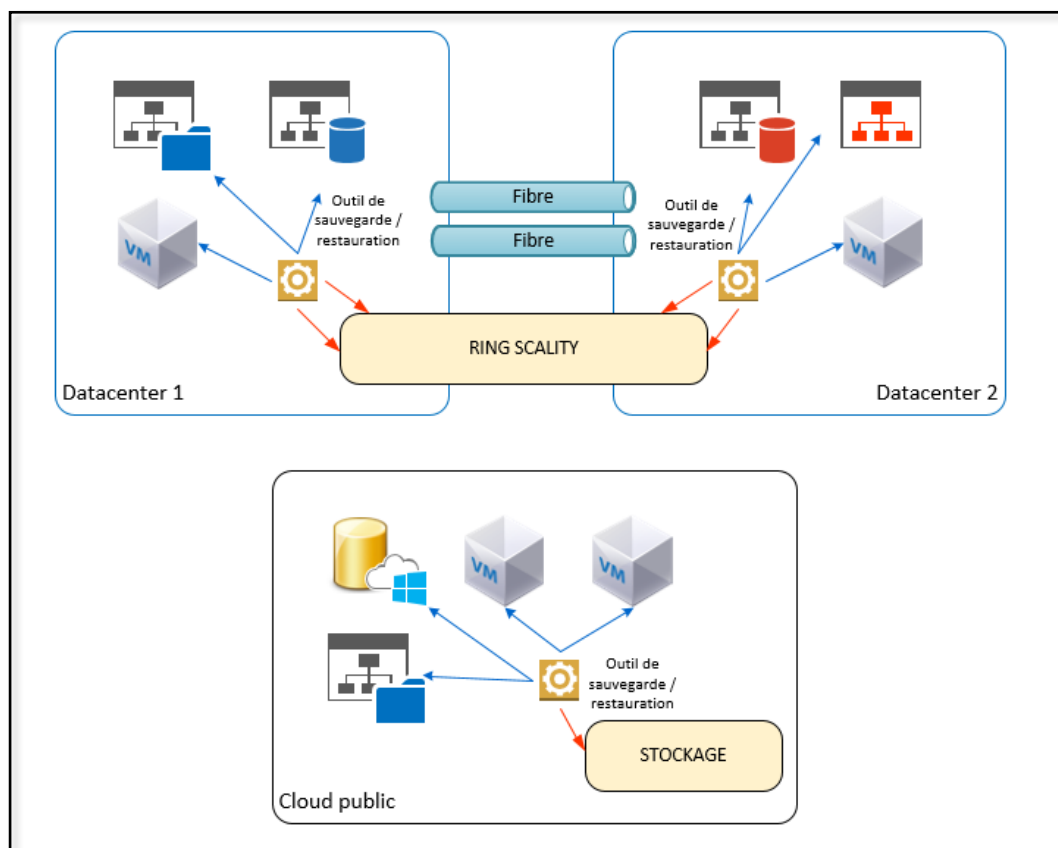
Figure 27 – Multipathing SAN

## Gestion du stockage

**R** Afin d'optimiser l'espace alloué et d'éviter une sur-allocation inutile, il est recommandé de faire du thin-provisioning au moment de la création des ressources

- O** Le type de stockage doit être adapté au contenu déposé et à son utilisation
- Les applications ayant besoin de haute performance en terme d'IOPS doivent privilégier des infrastructures de stockage à base de disques SSD et SAS
  - Les applications n'ayant pas besoin de haute performance en terme d'IOPS doivent privilégier des infrastructures de stockage à base de disques SATA

- O** Les données de sauvegarde des données des applications hébergées dans les datacenters de l'AP-HP doivent être déposées sur les infrastructures de stockage secondaire dédiées à cet effet : le RING SCALITY
- O** Les données de sauvegarde des données des applications hébergées dans un cloud public doivent être déposées sur ce même cloud public
- I** Les données de sauvegarde des données des applications hébergées dans un cloud public ne doivent pas être déposées sur le stockage secondaire RING SCALITY hébergé dans les datacenters de l'AP-HP (pour des raisons de coût des flux descendant du cloud public)



*Figure 28 - Utilisation du stockage secondaire*

- I** Les données de sauvegarde écrites sur des bandes magnétiques ne doivent plus utiliser des bandes LTO d'ancienne génération (toutes celles avant la LTO-7)

#### d. Les hébergements

##### HEBERGEMENT PROPRE

##### Stratégie d'hébergement

- R** Il est recommandé de ne pas distribuer une solution applicative de production sur plusieurs datacenters, en mode de fonctionnement nominal :
- La production en mode nominal se trouve sur un seul datacenter (le datacenter hébergeant les systèmes de production)
  - La production en mode secours (utilisée en cas de dysfonctionnement de la production nominale) se trouve sur le deuxième datacenter hébergeant les systèmes de secours

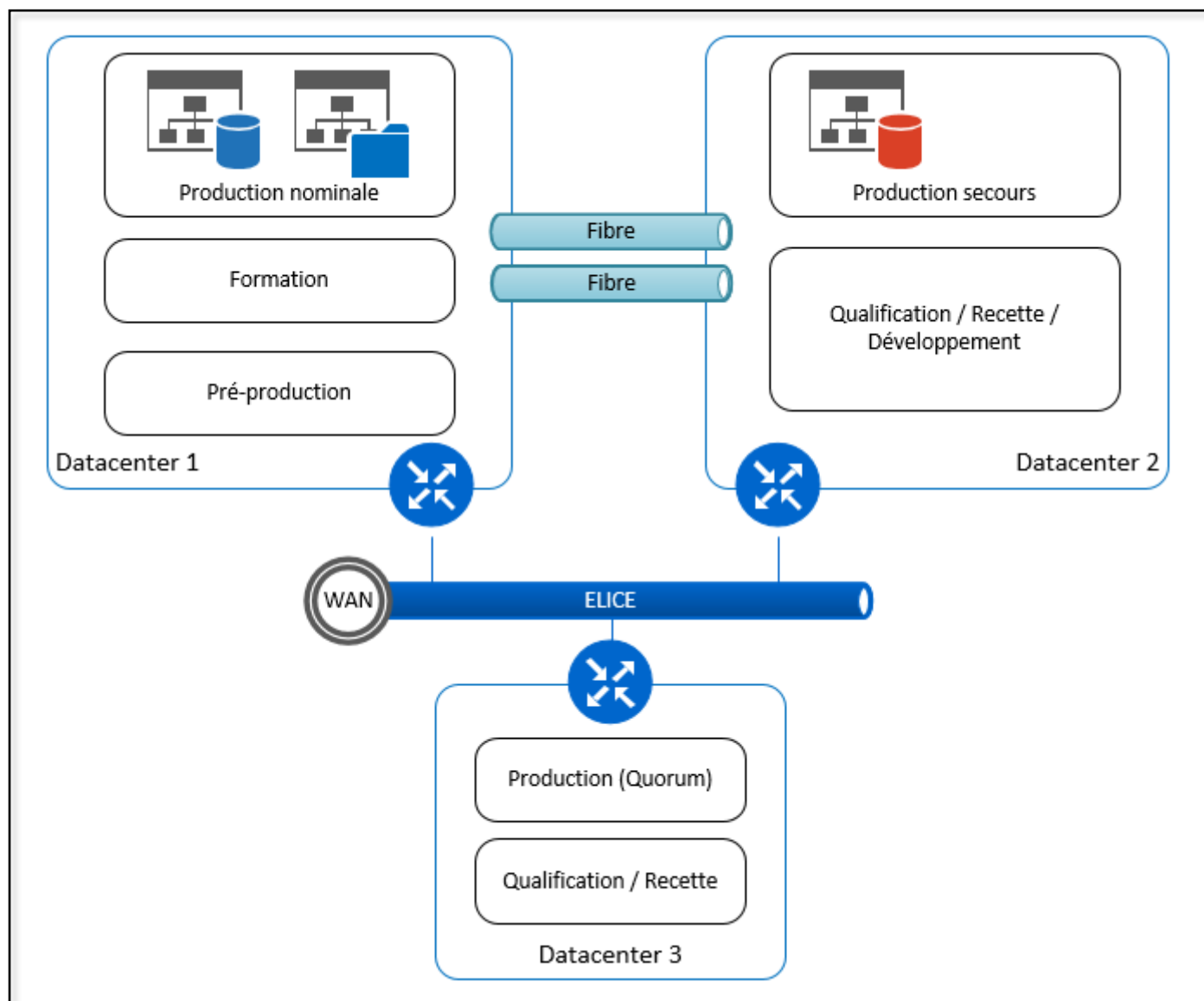


Figure 29 - Stratégie d'hébergement

- O** Les infrastructures portant les systèmes de surveillance des solutions en haute-disponibilité (les quorums) doivent être hébergées dans un datacenter différent
  - du datacenter de production nominale
  - du datacenter de production de secours

Les infrastructures portant les environnements de qualification d'intégration, de recette et de développement doivent être hébergées dans le même datacenter que celui hébergeant les infrastructures portant les environnements de production de secours

Les infrastructures portant les environnements de formation et de pré-production doivent être hébergées dans le même datacenter que celui hébergeant les infrastructures portant les environnements de production nominale

- I** Les infrastructures portant les environnements de production de secours ne doivent pas être hébergées dans le même datacenter que celui hébergeant les infrastructures portant les environnements de production nominale.

## CLOUD PUBLIC

---

### Règles générales

---

- O** Seul un Cloud Public étant officiellement reconnu comme étant un Hébergeur de Données de Santé (certification HDS) peut être utilisé pour héberger une solution informatique de l'AP-HP

- O** Toutes les règles à respecter dans le cadre d'un hébergement propre et définies dans le CCT restent valables dans la mise en place de solutions dans un Cloud Public quel qu'il soit

### Architecture

---

- O** L'architecture à mettre en œuvre est de type « Hub & Spoke »
  - Une zone dite « Hub » rassemblant l'ensemble des services d'infrastructure (DNS, NTP, Filtrage, Anti-virus, WAF, Poller de supervision ...) nécessaires aux solutions applicatives déployées dans le cloud public
  - Autant de zones dites « Spoke », chacune rassemblant l'ensemble des composants d'une solution applicative

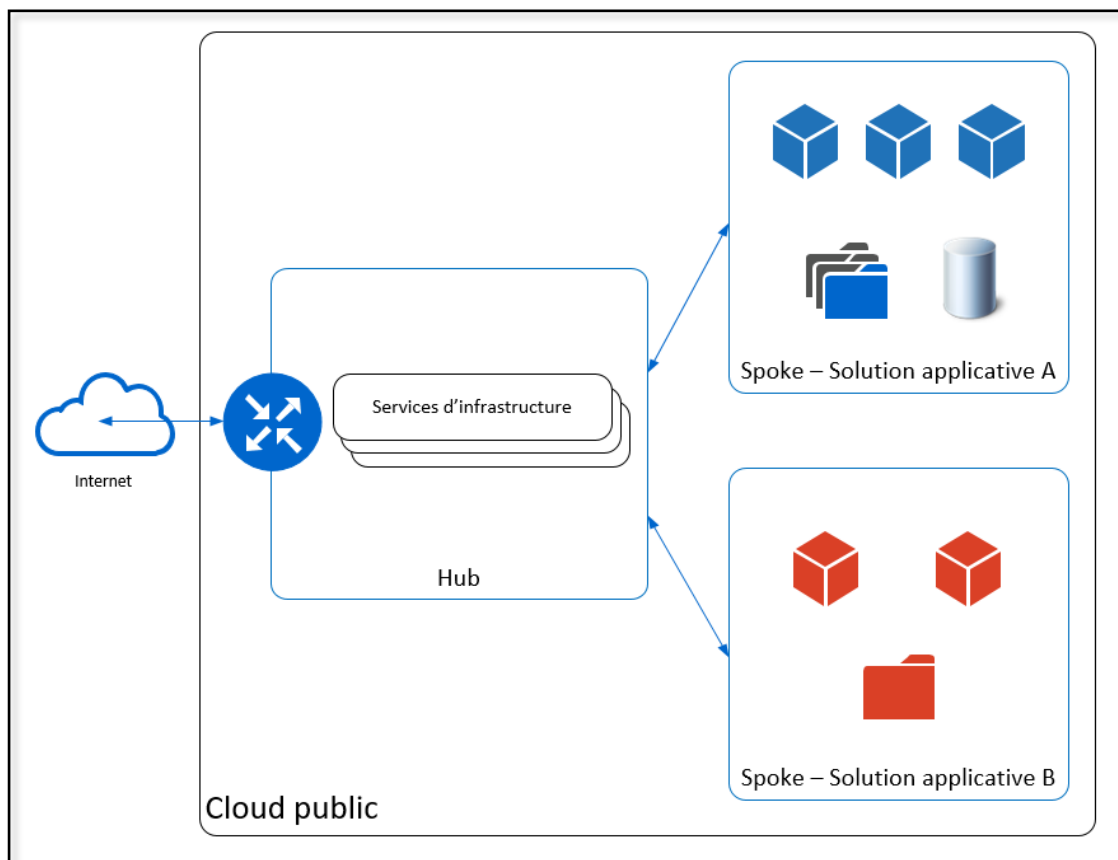
Chaque nouvelle application déployée dans le Cloud fait l'objet de la définition d'un nouveau Spoke

Cette architecture doit se décliner selon les environnements :

- Une architecture « Hub & Spoke » de production
- Une architecture « Hub & Spoke » de pré-production

➤ Une architecture « Hub & Spoke » de qualification

Et ainsi de suite



*Figure 30 - Cloud public Architecture Hub & Spoke*

**R** Il est recommandé de ne pas faire dépendre les applications déployées sur un Cloud Public de services d'infrastructures situés dans les hébergements propres du SI de l'AP-HP. Il est donc recommandé de déployer l'ensemble de ces services d'infrastructure dans le Cloud Public utilisé pour minimiser le nombre de flux de communication entre ce Cloud Public et le SI de l'AP-HP



### **e. Le poste de travail**

Les Postes de Travail de l'AP-HP sont achetés dans le cadre de marchés publics de fournitures de biens et services. Ils sont normalisés et banalisés. Chaque poste peut accéder à une ou plusieurs applications.

## **MATERIEL**

---

### **Postes fixes**

---

- R** Il est recommandé de déployer les modèles suivants, correspondant aux marchés en vigueur, selon les situations identifiées :
- Modèle 2 pour les déploiements
  - Modèle 4 pour le gain de place
  - Modèles 5 et 6 pour les postes typés « experts » (exemple : console PACS)

### **Postes mobiles**

---

- R** Il est recommandé de privilégier le déploiement d'ordinateur portable plutôt que de tablette pour les situations nécessitant de la mobilité
- Il est recommandé de déployer les modèles suivants, correspondant aux marchés en vigueur, selon les situations identifiées :
- Portable modèles 1 et 3 avec lecteur de carte intégré
  - Portable modèle 5 pour les VIP
  - Tablette modèle 2 pour les VIP

## **SYSTEME**

---

- O** Le système d'exploitation de tout nouveau poste de travail de type portable est Microsoft Windows 10
- Tout nouveau poste de travail doit être intégré à l'outil de gestion de parc Microsoft SCCM

- Tous les postes de travail doivent être protégés par la solution anti-virus de l'AP-HP : Symantec SEP
- Tout nouveau poste de travail doit être intégré à l'outil de gestion des mises à jour Microsoft SCCM

- Les navigateurs web autorisés sont :
  - Internet Explorer
  - Firefox ESR
- Tout client lourd applicatif doit être installé dans une ferme Citrix accessible depuis les postes de travail devant l'utiliser
- Les déploiements des applications clientes doivent se faire par l'intermédiaire de packages mis à disposition et déployés à l'aide de la solution SCCM
- Un poste est déployé avec le socle logiciel minimal suivant :
  - Lecteur PDF (Acrobat Reader)
  - Outil de compression / décompression d'archives (7zip)
  - Flash player
  - Outil de capture d'écran
  - Polices institutionnelles
  - Firefox ESR
  - VLC
  - Internet Explorer 11
  - LAPS UI
  - Skype
  - Framework .Net
  - Citrix Receiver

## f. Les services d'infrastructure

### LA REPARTITION DE CHARGE

- O Les applications conçues / à mettre en œuvre dans le SI de l'AP-HP et pour lesquelles un fort volume de connexions simultanées (correspondant à l'activité des utilisateurs) est attendu doivent permettre une évolutivité horizontale de leurs composants en acceptant une répartition de cette charge sur plusieurs instances identiques de ces composants et sans impact sur l'utilisation de l'application par les utilisateurs (pas de perte de contexte)

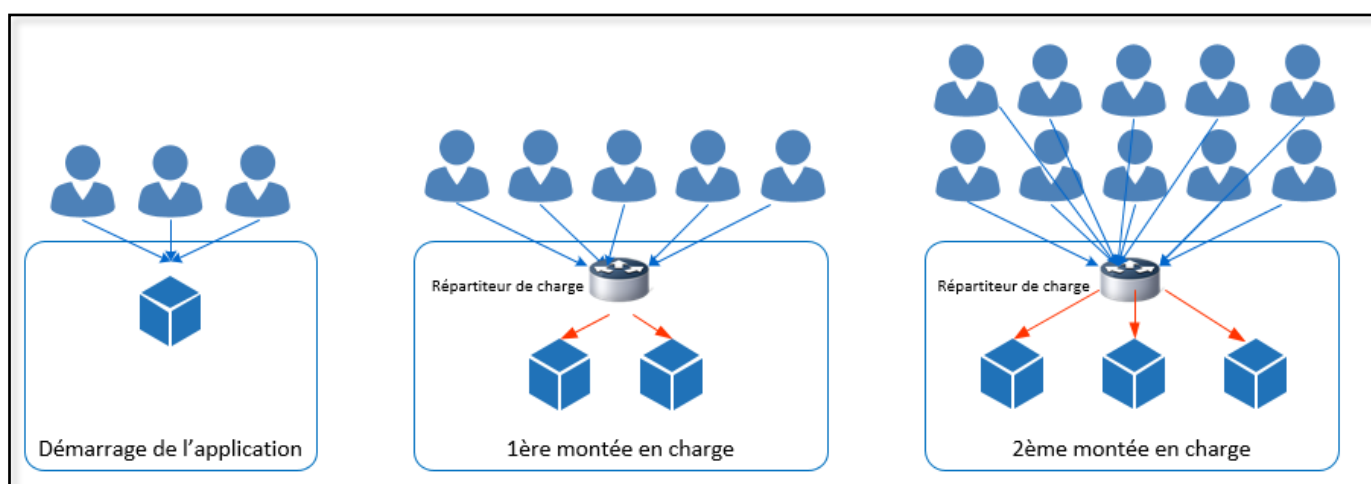


Figure 31 - Evolutivité horizontale

- O Un service proposant un fonctionnement avec de la répartition de charge doit être accédé grâce à une adresse IP virtuelle (VIP)

- I Deux services différents proposant un fonctionnement avec de la répartition de charge ne peuvent pas partager la même VIP (même s'ils se trouvent sur un même composant)

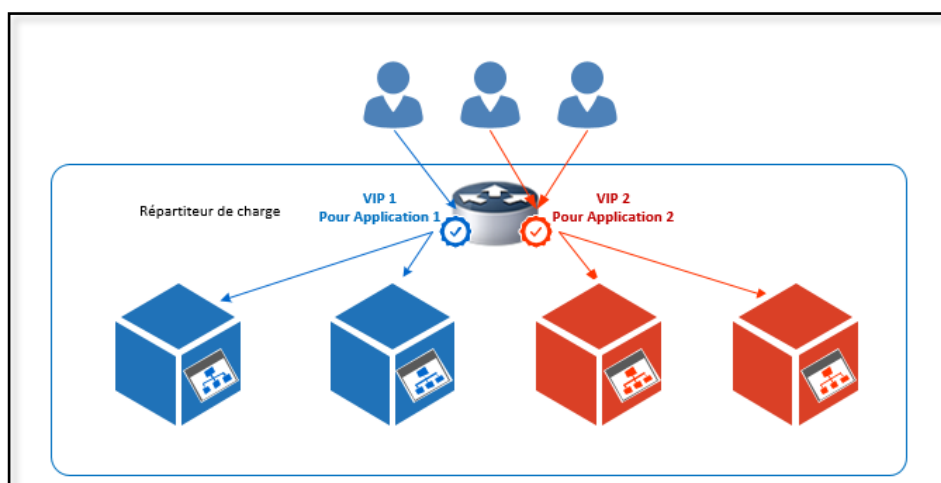


Figure 32 - Gestion des VIP (I)

**O** Une VIP est affectée à un et un seul service

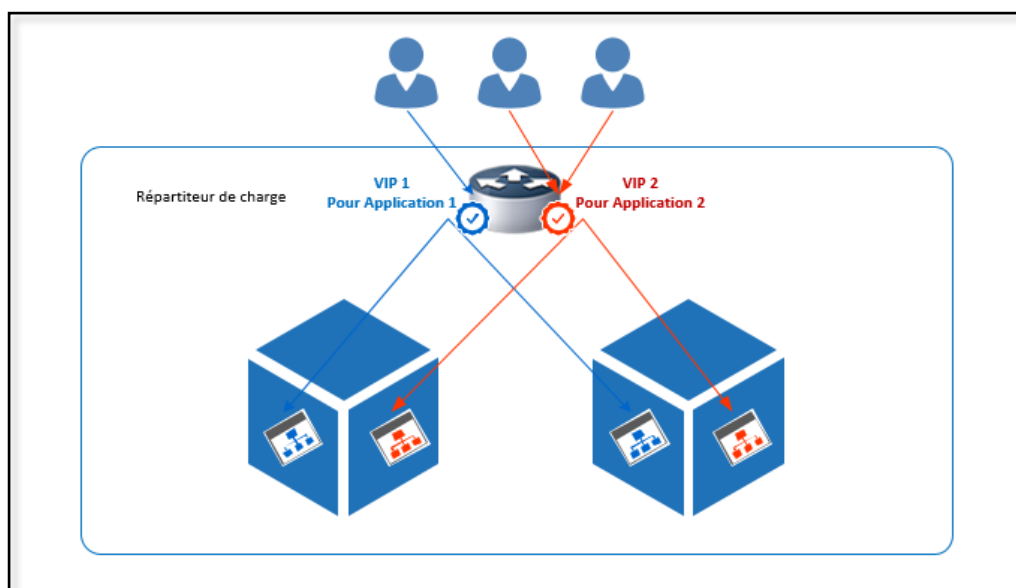


Figure 33 - Gestion des VIP (II)

**O** La répartition de charge des flux métiers doit être faite par la solution adoptée par le SI de l'AP-HP : Radware Alteon

**R** La solution de répartition de charge NGINX est tolérée dans des cas d'usage non couverts par la solution Radware Alteon

**I** Une solution applicative ne doit pas s'occuper de la répartition de charge vers un service externe dont elle a besoin. Elle doit se reposer sur un répartiteur de charge dont c'est le rôle

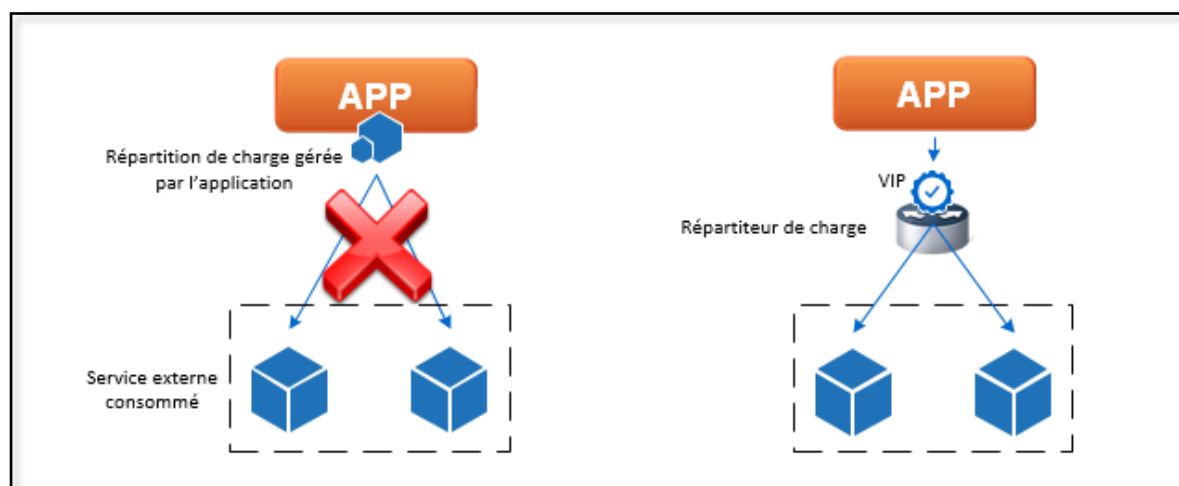


Figure 34 - Consommation d'un service redondé

## Concepts

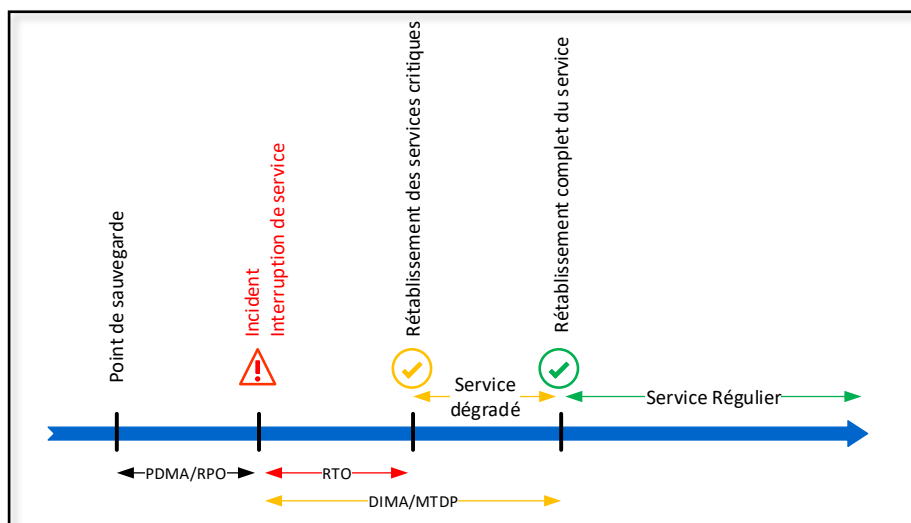


Figure 35 - Principes RPO / RTO

Les solutions de haute-disponibilité à mettre en œuvre doivent s'appuyer sur trois indicateurs :

- Le RPO (Recovery Point Objective) : en cas d'incident survenu sur une application, il s'agit de temps qu'il faudra remonter avant l'incident pour identifier l'instant où les données de l'application sont considérées comme devant être retrouvées au redémarrage de l'application après la résolution de l'incident.
- Le RTO (Recovery Time Objective) : en cas d'incident sur une application, il s'agit du temps d'indisponibilité, depuis l'instant où est survenu l'incident, de l'application avant le redémarrage de celle-ci en mode dégradé.
- La DIMA (Durée d'Interruption Maximale Acceptée) : en cas d'incident sur une application, il s'agit du temps d'indisponibilité, depuis l'instant où est survenu l'incident, de l'application avant le redémarrage de celle-ci en mode nominal.

**O** Pour chaque nouvelle application, ces trois indicateurs sont à définir avec l'équipe projet à partir des besoins exprimés par la maîtrise d'ouvrage / l'assistance à maîtrise d'ouvrage et / ou par les utilisateurs de l'application

### O Les applications pour lesquelles

- Le RTO est supérieur ou égal à 24h
- Le RPO correspond à la réalisation d'une dernière sauvegarde

doivent faire l'objet d'une restauration de la dernière sauvegarde en cas d'incident. Aucune solution de haute-disponibilité n'est nécessaire.

### R Pour les applications trois tiers traditionnelles (présentation / application / base de données) nécessitant un niveau élevé de haute-disponibilité (RPO & RTO inférieurs à 4h), il est recommandé de mettre en place une solution de haute-disponibilité :

- Composants en actif / actif sur le premier datacenter avec
  - de la répartition de charge sur les composants de présentation et d'application
  - un cluster de base de données de type maître /esclave
- Architecture identique mais dormante sur le deuxième datacenter
- Réplication des données entre les deux datacenters

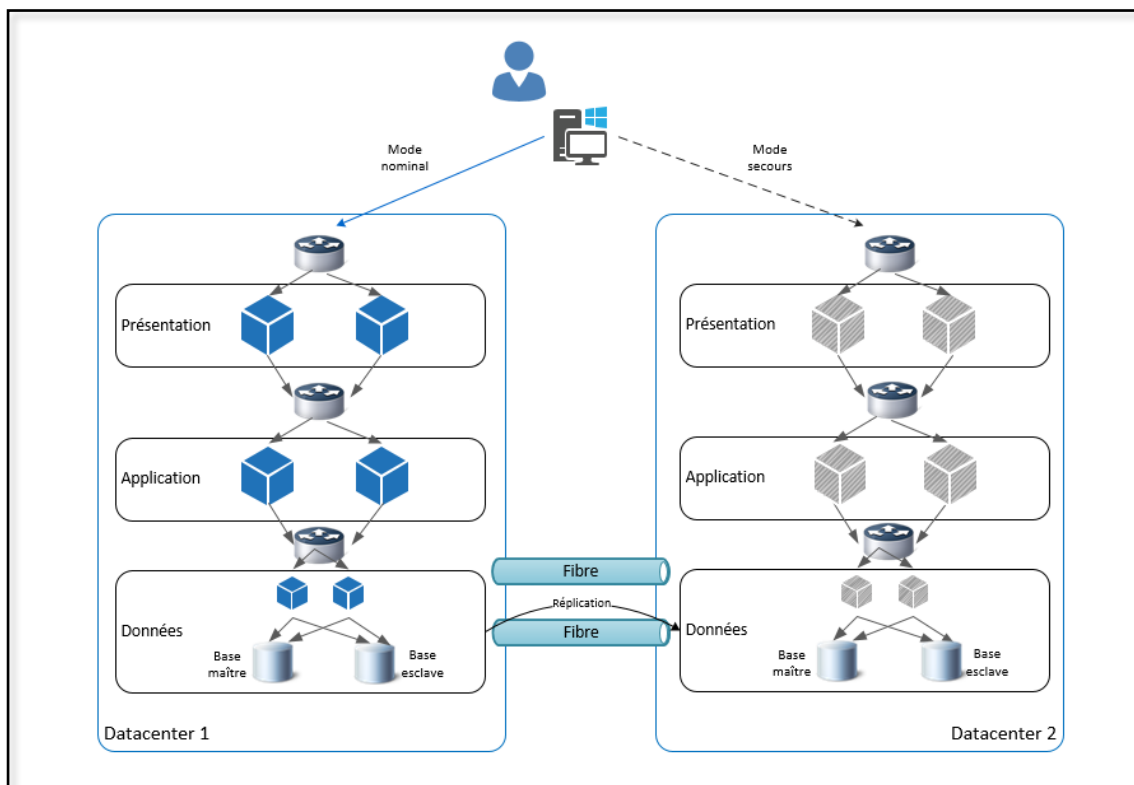


Figure 36 - Haute-disponibilité

**I** En cas d'incident sur une application trois tiers traditionnelle (présentation / application / base de données) et disposant d'une haute-disponibilité, la bascule vers le datacenter de secours ne doit pas se faire sur une partie des composants afin d'éviter des flux inter-datacenters pour le fonctionnement interne à la solution

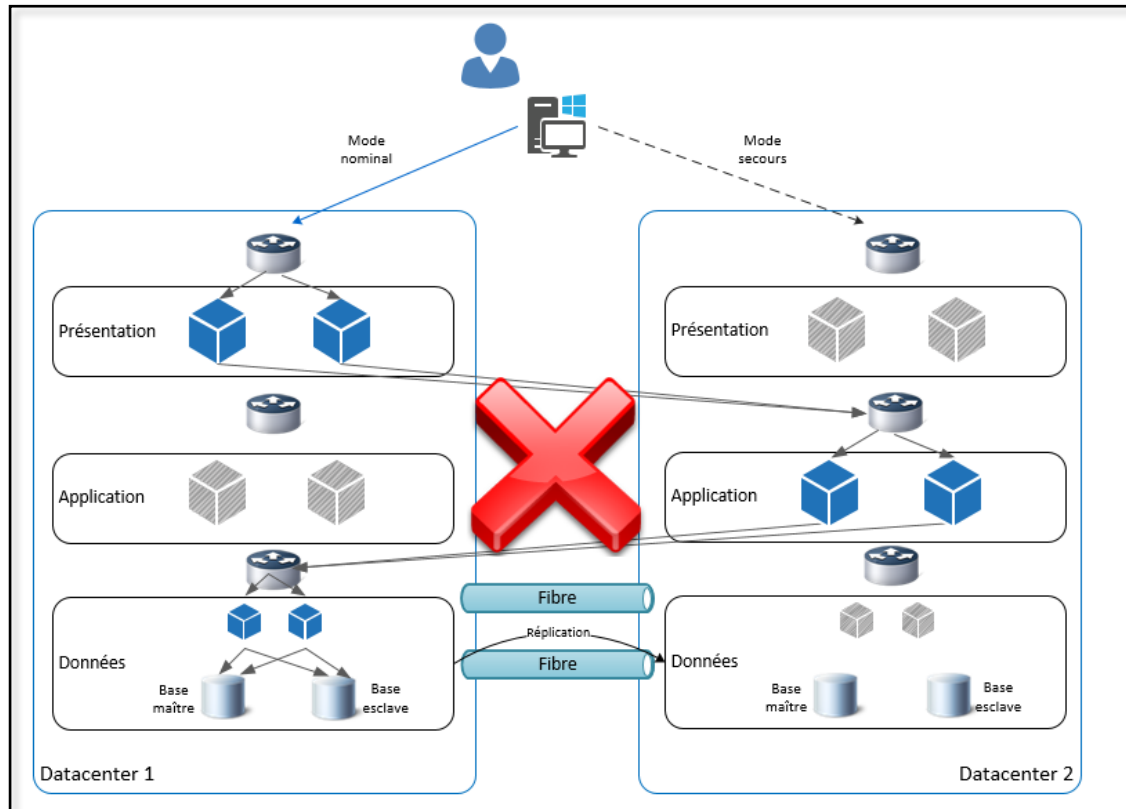


Figure 37 - Haute disponibilité (II)

**O** En cas d'incident sur une application trois tiers traditionnelle (présentation / application / base de données) et disposant d'une haute-disponibilité, la bascule vers le datacenter de secours doit se faire pour l'intégralité des composants de la solution

**O** Lors de la mise en place d'un cluster d'un ensemble de composants :

- Soit sur le même datacenter de production nominale
- Soit distribué sur deux datacenters

le service de surveillance du cluster (le quorum) doit être installé sur un autre datacenter, celui dédié à l'hébergement de ce type de service

**R** Les solutions de clustering recommandées sont :

- Safeguard pour les environnements HP-UX
- Pacemaker / Corosync pour les environnements Linux
- Real Application Cluster (RAC) pour une base de données Oracle
- PGPOOL pour une base de données PostgreSQL
- Safekit pour les solutions IAM

## L' AUTHENTIFICATION

---

### Authentification des utilisateurs AP-HP

---

**O** L'authentification des utilisateurs AP-HP lors d'une connexion à une application doit se baser sur la solution Active Directory

La délégation de l'authentification à Active Directory doit se faire

- Soit par un bind LDAPS
- Soit par l'utilisation d'un web service mis à disposition par l'APHP
  - Accessible en SOAP : <https://adswas.bbs.aphp.fr/was/AdConnect.asmx>
  - Accessible en REST API : <https://adswas.bbs.aphp.fr/was/AdConnect.svc>

**O** Une application non hébergée dans les datacenters de l'AP-HP doit authentifier les utilisateurs AP-HP en utilisant la solution de Web SSO mise en œuvre dans le SI de l'AP-HP (solution basée sur SAML)

**I** La saisie du login et du mot de passe d'un utilisateur AP-HP, correspondant à ses identifiants internes, dans une application non hébergées dans les datacenters est interdite

**O** Toute nouvelle application mise en œuvre dans le SI de l'AP-HP doit être compatible avec la solution de Single Sign On (SSO) mise en œuvre à l'AP-HP : la solution Bull Evidian

### Double facteur

---

**O** Toute application relevant du périmètre HDS doit proposer une authentification à double facteur



## 2. Les services applicatifs

### a. Les bases de données

#### LES BASES DE DONNEES RELATIONNELLES

---

Un système de gestion de base de données (SGBD) est un logiciel système destiné à stocker et à partager des informations stockées de manière structurée. Il doit garantir la qualité, la pérennité et la confidentialité des informations, tout en cachant la complexité des opérations.

Une base de données relationnelle (SGBDR) est une base de données où l'information est organisée dans des tableaux à deux dimensions appelés relations ou tables.

**O** Les bases de données sont déployées sur les systèmes d'exploitation suivants :

- Red Hat Entreprise Linux
- Microsoft Windows Serveur
- HP UX

**R** Les bases de données recommandées dans le SI APHP sont par ordre de priorité les bases dites open source, puis les bases dites propriétaires.

- SGDB open source
  - PostgreSQL
  - MySQL ou mariaDB
- SGDB propriétaire
  - Oracle Database Serveur
  - Microsoft SQL Serveur

**O** Pour les bases de données dites open source, les packages d'installation autorisés proviennent obligatoirement, et par ordre de priorité, soit du fournisseur de l'OS, soit de l'éditeur de la base de données

#### LES BASES DE DONNEES NOSQL

---

Les bases de données NoSQL (non relationnelle) sont conçues pour résoudre les problèmes de traitement de données en volume, multi-sources et multi-formats, dans des environnements dits de « Big Data ». On classe ce type de bases de données en quatre catégories : les bases orientées document, les bases clé/valeur, les bases en colonnes et les bases orientées graphes.

**O** Pour les bases NoSQL, les packages d'installation autorisés proviennent obligatoirement, et par ordre de priorité, soit du fournisseur de l'OS, soit de l'éditeur de la base

## Les bases de données orientées document

---

Les bases de données orientées document stockent les données dans des structures identiques à celles de documents. Elles peuvent parfois être sans schéma.

Usage : Elles sont souvent utilisées dans les systèmes de gestion de contenus, ainsi que pour collecter et traiter des données à partir d'applications à fort trafic, pour les monitorer.

**R** La base de données NoSQL recommandée est MongoDB

## Les bases de données clé / valeur

---

Les bases de données clé/valeur sont de forme très simple. Elles associent des clés uniques à des valeurs dans des données, avec pour objectif de renforcer fortement les performances des applications reposant sur des jeux de données relativement simple.

Usage : les bases clé/valeur sont très légères et sont souvent utilisées dans les cas à fort changement de données pour une utilisation en temps réelle.

**R** Les bases de données NoSQL à clé / valeur recommandées sont :

- Redis
- ETCD

## Les bases en colonnes

---

Les bases de données en colonnes conservent les données dans des tables qui disposent d'un très grand nombre de colonnes. Elles offrent des hauts niveaux de performance et de dimensionnement lorsqu'il faut traiter (et parcourir) d'importants jeux de données.

Usage : leurs usages varient de la recherche sur Internet aux applications WEB à grande échelle, ainsi qu'aux applications analytiques capables de traiter des péta-octets de données.

**R** Base recommandée :

- HBase (Hadoop DB)
- Cassandra

## Les bases orientées graphes

---

Les bases 'orientées graphes' stockent des éléments de données dans des structures en graphes et permettent de créer des associations entre eux.

L'AP-HP ne recommande pas, pour le moment, de bases en particulier.

**R** Si une base de données relationnelle d'une application nécessite une réplication de son contenu, il est recommandé de choisir la base parmi les solutions suivantes :

- PostgreSQL
- Oracle
- Microsoft SQL Server
- MySQL ou mariaDB

Si une réplication des données d'une base de données vers une autre base de données s'avère nécessaire, les solutions suivantes sont recommandées

- Pour PostgreSQL : réplication des journaux de transaction WAL
- Pour Oracle
  - Soit Dataguard (si la base répliquée ne doit pas être ouverte)
  - Soit Active Dataguard (si la base répliquée doit être ouverte)
- Pour Microsoft SQL Server : Always On
- MySQL ou mariaDB : réplication des binary logs

## **b. Les échanges inter-applicatifs**

Les échanges inter-applicatifs sont des flux incontournables dans le partage d'informations entre les applications d'un SI. L'AP-HP utilise un très grand nombre d'applications en raison des multiples métiers existant au sein de l'institution. Ces échanges sont donc très nombreux et critiques de par la nature des données traitées.

Pour assurer la simplification, l'harmonisation, la maîtrise, la sécurité de ses échanges inter-applicatif l'AP-HP a mis en place des solutions de management des flux.

### LES SOLUTIONS DE GESTION DES FLUX

---

#### EAI / ETL

---

La solution d'intégration EAI/ETL est une solution entièrement développée par l'AP-HP. La solution implémente plusieurs types de service dont le traitement par lots, le traitement au fil de l'eau. Ces traitements peuvent subir des transformations, du filtrage et du routage. Les flux inter-applicatifs sont réalisés par demi-interface : un flux complet comprend obligatoirement au moins une demi-interface d'entrée et au moins une demi-interface de sortie.

#### API Management

---

L'API Management est une solution permettant de gérer les flux reposant sur du REST API. Il s'agit d'une solution en cours de construction dans le SI de l'AP-HP.

#### Règles générales

---

**I** Aucun échange métier (synchrone ou asynchrone) inter-applicatifs n'est autorisé entre deux applications directement, afin d'éviter le phénomène de couplage fort.

**O** Tout nouvel échange inter-applicatifs doit transiter par l'une des solutions de management des flux du SI de l'AP-HP :

- EAI / ETL
- API Management

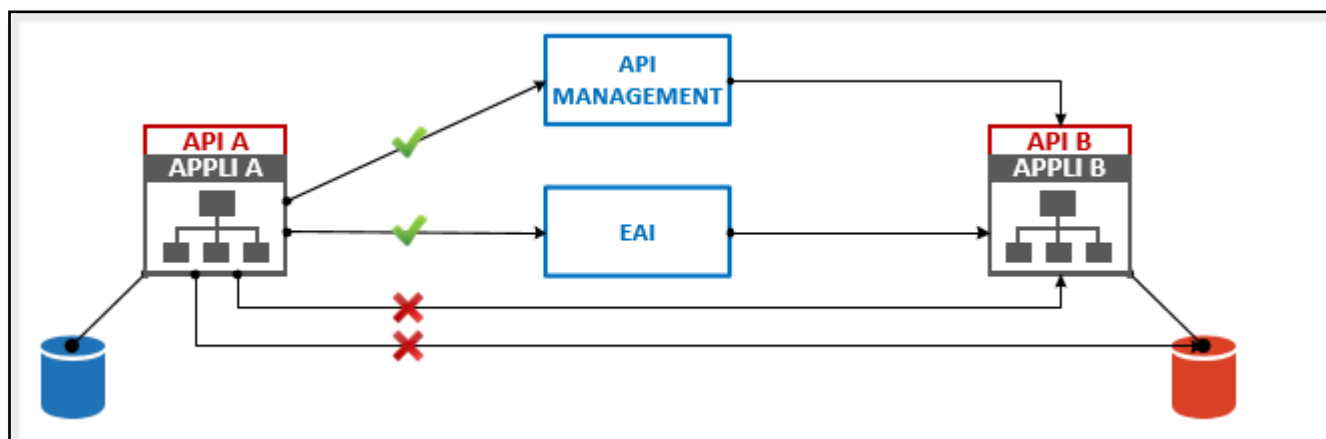
Toute solution, souhaitant partager (en émission ou en acquisition) de la donnée appartenant déjà à un flux existant au sein du SI doit utiliser la solution d'échange gérant ce flux.

L'utilisation d'une brique intermédiaire comme l'EAI ou l'API Management n'affranchit nullement les applications échangeant des informations de mécanismes de reprise sur incident. En cas d'incident ayant abouti à l'échec de l'échange

- Une application émettrice doit pouvoir émettre de nouveau si la communication avec la brique intermédiaire échoue
- Une application réceptrice doit pouvoir rejouer l'intégration si la brique intermédiaire a bien transmis les données mais qu'elles n'ont pas été intégrées correctement par l'application

**R** Il est recommandé d'utiliser le service d'API Management pour les échanges basés sur du REST API

Pour tout autre type d'échange, il est recommandé d'utiliser l'EAI



*Figure 38 – Flux inter-applicatifs*

## Chiffrement des échanges

**O** Tous les échanges inter-applicatifs sortant du ou entrant dans le SI de l'AP-HP sont chiffrés.

Tous les échanges inter-applicatifs dans l'environnement HDS sont chiffrés

**R** Pour des échanges entre des applications de même niveau de confidentialité, le chiffrement du flux n'est pas une obligation. Il reste cependant à la discrétion du département en charge de la sécurité du SI de l'AP-HP.

## Protocoles d'échange

**I** Les protocoles, même chiffrés, n'assurant ni fiabilité, ni intégrité sont à proscrire lors de la mise en œuvre d'un échange inter-applicatif

**O** Tout nouveau flux d'échange doit utiliser une solution de transfert qui assure :

- La fiabilité du transfert
- L'intégrité des données transférées

## Authentification des échanges

---

**R** Il est recommandé d'authentifier un appel de type Web Service ou REST API par l'intermédiaire d'un jeton.

Pour l'authentification par jeton, il est recommandé de mettre en place un jeton JSON Web Token (JWT)

## Flux d'échange interne au SI de l'AP-HP

---

**I** L'utilisation du protocole JDBC depuis une application ou un EAI directement (sans passer par son serveur d'application) vers la base de données d'une autre application est interdite. L'application doit à cet effet fournir un accès ses données au travers une interface dédiée (par exemple de type REST API) respectant ainsi les règles d'intégrité et de sécurité.

La mise en œuvre de DBLink entre deux bases de données appartenant à des applications différentes est interdite.

**R** Le protocole FTP, chiffré ou non, n'est plus recommandé dans les échanges inter-applicatifs. Il ne peut être utilisé que dans des cas où l'analyse de risque ne demande pas de sécurisation particulière sur le flux.

Liste des protocoles d'échange recommandés :

- HTTP/HTTPS (SOAP – REST)
- SAP RFC – pour la communication avec SAP
- MLLP pour les données de type HL7

La mise en œuvre de DBLink entre deux bases de données n'étant plus autorisée, il est recommandé d'utiliser les couches applicatives des applications (qui possèdent l'intelligence métier de leur périmètre) et des API pour échanger des données.

## Flux d'échange avec des partenaires externes au SI de l'AP-HP

---

**I** Le protocole FTP, chiffré ou non, est interdit pour les échanges entre une application externe au SI de l'AP-HP et une application interne au SI de l'AP-HP

**R** Le protocole d'échange recommandé est :  
➤ HTTPS

**R** Les formats recommandés pour les échanges inter-applicatifs sont :

- XML
- JSON
- SAP IDOC pour les flux avec SAP

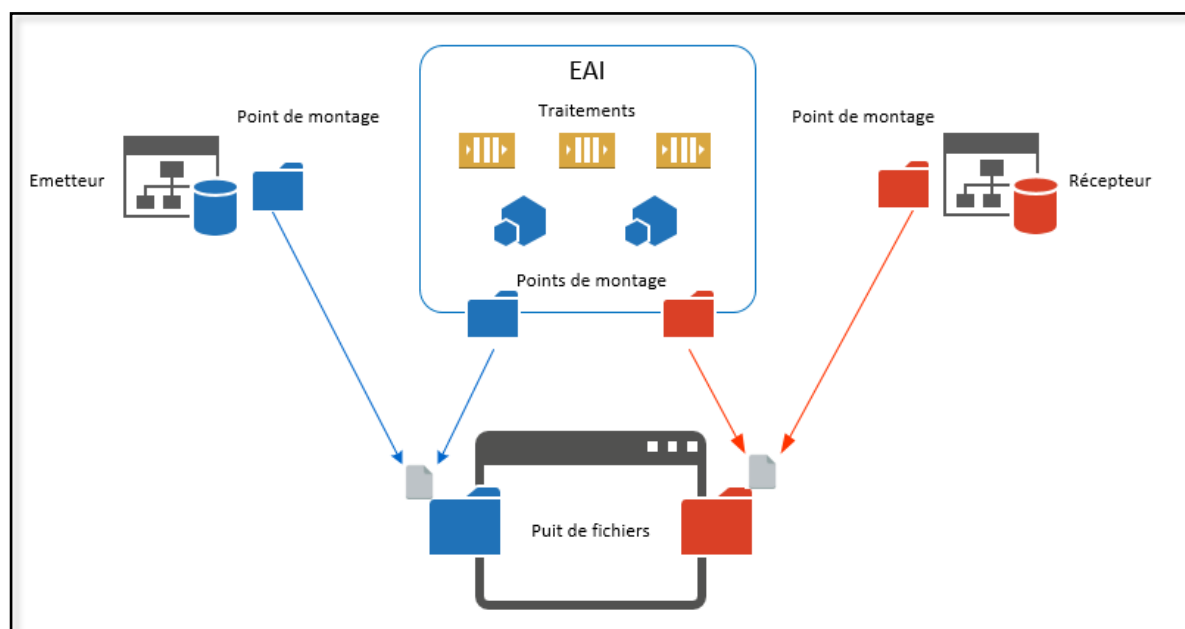
Pour un échange de données de santé, les formats recommandés sont :

- XML/HL7
- XML/FHIR

## Les échanges de fichiers

**R** Afin de minimiser les espaces de stockage et la duplication des fichiers transférés, il est recommandé de mettre en œuvre des puits de fichiers proposant des espaces de stockage (répertoires) uniques et présentés aux différents composants concernés par le flux (émetteur / EAI / récepteur) sous forme de points de montage

- NFS (version 3 a minima)
- SMB (version 2 a minima)



*Figure 39 - Puit de fichiers pour les flux*

**I** Il est interdit de mettre en œuvre de tels points de montage NSF ou CIFS au travers du WAN AP-HP (cas d'un échange entre un émetteur hébergé dans un établissement hospitalier et un récepteur hébergé dans un datacenter)

### **c. La planification des traitements**

**I** Il est interdit de déclencher des traitements d'arrière-plan et récurrents par l'intermédiaire de l'ordonnanceur intégré au système d'exploitation (cron table, tâche planifiée Windows)

**O** Les traitements d'arrière-plan récurrents doivent être planifiés par l'ordonnanceur du SI de l'AP-HP : VTOM

### **d. Orchestration**

**R** Il est recommandé d'orchestrer les tâches techniques, éligibles à ce genre d'automatisation et quel que soit leur périmètre d'origine (système physique, système virtuel, réseau ...), par l'intermédiaire de la solution d'orchestration du SI de l'AP-HP : HPE Operations Orchestration

### **e. Serveur de publication**

Afin de faciliter la gestion, la compatibilité et l'accessibilité des progiciels utilisés au sein du SI. L'AP-HP a mis en place une solution de publication d'applications et sessions sous Citrix XenApp. Avec cette solution, les applications ne sont plus installées au sens traditionnel du terme sur les postes clients, mais sur les serveurs Citrix.

**O** Toute nouvelle solution/application construite sous forme de développement spécifique doit être accessible exclusivement par client léger (Navigateur Web).

Tout progiciel nécessitant la mise en place de client lourd sur le poste de travail de l'utilisateur se voit imposer l'installation de ce client sous Citrix XenApp. Le progiciel doit donc être compatible avec le mécanisme de publication Citrix ainsi qu'avec la version de la solution Citrix utilisée à l'AP-HP

Les solutions publiées et nécessitant une authentification forte de l'utilisateur doivent utiliser la solution Netscaler de Citrix.

**R** Dans le cas où une application est accessible aussi bien par client lourd que par client léger (Navigateur Web), il est recommandé de favoriser la solution client léger



# Architecture d'administration

---

## 1. La sécurité des systèmes d'information

### *a. Principes généraux de la PGSSI*

L'AP-HP a défini en 2010 et actualisé en 2016 une Politique Générale de Sécurité du Système d'Information (PGSSI). L'objectif de cette politique est la préservation et la sécurisation de l'intégralité du système d'information de l'AP-HP.

Les règles énoncées dans la PGSSI de l'AP-HP qui ont un impact direct sur les normes et standards techniques à respecter dans le cadre de la mise en œuvre d'un nouveau composant matériel ou logiciel sont mentionnées dans les paragraphes ci-après.

L'AP-HP met en œuvre le principe de défense en profondeur des systèmes d'information tel que préconisé par l'ANSSI (La défense en profondeur appliquée aux systèmes d'information).

L'AP-HP suit les bonnes pratiques de sécurité préconisées par l'ASIP Santé.

### *b. Environnement technique de sécurité du SI de l'AP-HP*

#### POSTE DE TRAVAIL WINDOWS

---

L'ensemble des postes de travail et serveurs informatiques sous WINDOWS est protégé par un antivirus. Cet antivirus intègre des fonctions de détection et d'éradication des codes informatiques malveillants en temps réel et en mode planifié, un pare-feu hôte et un module de prévention d'intrusion. La configuration de l'antivirus suit les recommandations des éditeurs de logiciels afin d'optimiser les performances (détection, charge, temps de réponse).

Les correctifs de sécurité WINDOWS sont gérés par la Solution WSUS de Microsoft pour les serveurs et SCCM pour les postes de travail. La mise à jour des serveurs fait l'objet d'un plan de maintenance minimisant les impacts sur le service rendu par les systèmes mis à jour.

#### MESSAGERIE ELECTRONIQUE

---

La messagerie met en œuvre un antivirus sur les MTA afin de bloquer la transmission de codes informatiques malveillants. Les fichiers « exécutables » sont bloqués

Un service ANTISPAM et antivirus est utilisé pour les messages électroniques en provenance et à destination de l'Internet. Les protocoles SPF, DKIM et DMARC sont utilisés pour assurer l'intégrité des messages acheminés par le réseau Internet.

Les vulnérabilités techniques sont identifiées par l'outil SECURITY CENTER de TENABLE en lien avec une centralisation des journaux techniques.

L'accès au réseau Internet est réalisé au travers d'un PROXY filtrant équipé d'un antivirus.

### c. Exigences techniques de sécurité

O

Les prestations qui nécessitent l'usage de mot de passe suivent, sans restriction, les recommandations de la CNIL « Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe »

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033928007&categorieLien=id> éditée au journal officiel

Les prestations mettant en œuvre des logiciels sont compatibles sans restriction avec l'usage des versions supportées par leur éditeur respectif (communauté dans le cas de logiciel « libre ») à la date de notification du marché jusqu'à sa date de fin d'exécution.

#### POSTE DE TRAVAIL INFORMATIQUE

---

O

Les prestations qui nécessitent l'usage de poste de travail informatique suivent, sans restriction, les recommandations de la note technique intitulée « Recommandations de configuration matérielle de postes clients et serveurs x86 » <https://www.ssi.gouv.fr/administration/guide/recommandations-de-configuration-materielle-de-postes-clients-et-serveurs-x86/> éditée par l'ANSSI.

R

Les prestations, qui nécessitent l'usage de poste de travail informatique sous système d'exploitation WINDOWS de Microsoft, suivent les recommandations de la note technique intitulée « Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows » <https://www.ssi.gouv.fr/guide/recommandations-pour-la-mise-en-oeuvre-dune-politique-de-restrictions-logicielles-sous-windows/> éditée par l'ANSSI.

Les prestations, qui nécessitent l'usage du logiciel JAVA pour les postes de travail informatique sous système d'exploitation WINDOWS de Microsoft, suivent les recommandations de la note technique intitulée « Recommandations de sécurité relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows » <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-aux-environnements-dexecution-java-sur-les-postes-de-travail-microsoft-windows/> éditée par l'ANSSI

#### NAVIGATEURS

---

R

Les prestations qui nécessitent l'usage d'un navigateur suivent les recommandations des notes techniques intitulées « Recommandations pour le déploiement sécurisé du navigateur MOZILLA FIREFOX sous WINDOWS », <https://www.ssi.gouv.fr/guide/recommandations-pour-le-dploiement-securise-du-navigateur-mozilla-firefox-sous-windows/> « Recommandations pour le déploiement sécurisé du navigateur Google Chrome sous Windows » <https://www.ssi.gouv.fr/guide/recommandations-pour-le-dploiement-securise-du-navigateur-google-chrome-sous-windows/> et « Recommandations pour le déploiement sécurisé du navigateur Microsoft Internet Explorer » <https://www.ssi.gouv.fr/guide/recommandations-pour-le-dploiement-securise-du-navigateur-microsoft-internet-explorer/>, éditées par l'ANSSI.

## SERVEURS INFORMATIQUES

---

O

Les prestations qui nécessitent l'usage de serveur informatique suivent sans restriction les recommandations des notes techniques intitulées « Recommandations de configuration matérielle de postes clients et serveurs x86 » <https://www.ssi.gouv.fr/administration/guide/recommandations-de-configuration-materielle-de-postes-clients-et-serveurs-x86/> et « Problématiques de sécurité associées à la virtualisation des systèmes d'information » <https://www.ssi.gouv.fr/guide/problematiques-de-securite-associees-a-la-virtualisation-des-systemes-dinformation/> éditées par l'ANSSI.

## CONFIGURATION DU SYSTEME D'EXPLOITATION LINUX

---

O

Les prestations qui nécessitent l'usage du système d'exploitation LINUX suivent sans restriction les recommandations dites de **niveau minimal** de la note technique intitulée « Recommandations de configuration d'un système GNU/Linux » <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/> éditée par l'ANSSI

Pour les systèmes accédés par des **tiers**, notamment depuis **Internet**, les prestations qui nécessitent l'usage du système d'exploitation LINUX suivent sans restriction les recommandations de **niveau intermédiaire** de la note technique référencée ci-dessus intitulée « Recommandations de configuration d'un système GNU/Linux » <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/> éditée par l'ANSSI

## ANNUAIRE ACTIVE DIRECTORY MICROSOFT

---

O

Les prestations qui nécessitent l'usage de l'annuaire ACTIVE DIRECTORY de Microsoft suivent, sans restriction, les recommandations de la note technique intitulée « Recommandations de sécurité relatives à Active Directory » <https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-a-active-directory/> éditée par l'ANSSI.

## JOURNALISATION

---

O

Les prestations suivent, sans restriction, les recommandations de la note technique intitulée « Recommandations de sécurité pour la mise en œuvre d'un système de journalisation » <https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/> éditée par l'ANSSI.

## TELEASSISTANCE INFORMATIQUE

---

O

Les prestations qui nécessitent l'usage de la téléassistance suivent sans restriction les recommandations de la note technique intitulée « Recommandations de sécurité relatives à la téléassistance » <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-la-tele-assistance/> éditée par l'ANSSI.

## CRYPTOGRAPHIE

---

O

Les prestations qui nécessitent l'usage de la cryptographie suivent, sans restriction, les recommandations de la note intitulée « Annexe B1 - Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » <https://www.ssi.gouv.fr/entreprise/guide/cryptographie-les-regles-du-rgs/> du Référentiel Général de Sécurité (RGS version 2.0) disponible publiquement sur le site Internet de l'ANSSI.

## APPLICATIONS WEB

---

O

Les prestations en lien avec les applications WEB suivent, sans restriction, les recommandations de la note technique intitulée « Recommandations pour la sécurisation des sites web » <https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/> éditée par l'ANSSI.

## RESEAUX

---

O

Les prestations qui nécessitent l'usage du réseau informatique sont compatibles, sans restriction, avec le principe de défense en profondeur. Elles devraient permettre la mise en œuvre de zones de sécurité séparées par des pare-feu ou des passerelles et l'établissement de matrices de trafic.

I

L'usage des versions non sécurisées des protocoles est interdit (REXEC, RLOGIN, TELNET, http, FTP).

O

Les prestations qui nécessitent l'usage du protocole TLS suivent, sans restriction, les recommandations de la note technique intitulée « Recommandations de sécurité relatives à TLS » <https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-tls/> éditée par l'ANSSI

Les prestations qui nécessitent l'usage des protocoles IPsec SSH suivent, sans restriction, les recommandations des notes techniques intitulées « Recommandations de sécurité relatives à IPsec pour la protection des flux réseau » <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-ipsec-pour-la-protection-des-flux-reseau/> et « Recommandations pour un usage sécurisé d'(Open)SSH » <https://www.ssi.gouv.fr/administration/guide/recommandations-pour-un-usage-securise-dopenssh/> éditées par l'ANSSI.

Les prestations qui nécessitent l'usage de réseau WIFI suivent, sans restriction, les recommandations de la note technique intitulée « Recommandations de sécurité relatives aux réseaux WiFi » <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-aux-reseaux-wifi/> éditée par l'ANSSI

## TELEPHONES MULTIFONCTIONS

---

O

Les prestations qui nécessitent l'usage de téléphone multifonction (SMART PHONE) suivent sans restriction les recommandations de la note technique intitulée « Recommandations de sécurité relatives aux ordiphones » <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-aux-ordiphones/> éditée par l'ANSSI

## TELEPHONIE SUR IP

---

R

Les prestations qui nécessitent l'usage de la téléphonie sur IP suivent, sans restriction, les recommandations de la note technique intitulée « Recommandations de sécurisation d'une architecture de téléphonie sur IP » <https://www.ssi.gouv.fr/guide/recommandations-de-securisation-dune-architecture-de-telephonie-sur-ip/> éditée par l'ANSSI

O

Les prestations qui nécessitent l'usage de la téléphonie sur IP suivent, sans restriction les recommandations R8, R9, R10, R11, R12, R19, R41 et R42, de la note technique référencée ci-dessus intitulée « Recommandations de sécurisation d'une architecture de téléphonie sur IP » <https://www.ssi.gouv.fr/guide/recommandations-de-securisation-dune-architecture-de-telephonie-sur-ip/> éditée par l'ANSSI

O

Les prestations qui nécessitent l'usage de dispositifs de sécurité physique suivent, sans restriction, les recommandations du guide « SECURITE DES TECHNOLOGIES SANS-CONTACT POUR LE CONTROLE DES ACCES PHYSIQUES » <https://www.ssi.gouv.fr/guide/la-securite-des-technologies-sans-contact-pour-le-contrôle-des-accès-physiques/> édité par l'ANSSI

Les prestations qui nécessitent l'usage de dispositifs de sécurité physique sont compatibles sans restriction avec les cartes CPS de l'ASIP Santé <https://integrateurs-cps.asipsante.fr/pages/La-carte-CPS3>

Les prestations qui nécessitent l'usage de dispositifs de vidéo protection suivent, sans restriction, les recommandations de la note technique intitulée « Recommandations de sécurité pour la mise en œuvre de dispositifs de vidéo protection » <https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-de-dispositifs-de-videoprotection/> éditée par l'ANSSI

## LUTTE CONTRE LES CODES MALFAISANTS

---

O

Les prestations qui nécessitent l'usage d'équipement utilisant le système d'exploitation WINDOWS sont compatibles avec la présence d'un antivirus

R

Les prestations qui nécessitent l'usage d'équipement utilisant le système d'exploitation WINDOWS sont avec l'antivirus utilisé par l'AP-HP

## 2. La protection des données

**O** Les composants (serveurs physiques, serveurs virtuels, bases de données, NAS, postes de travail, snapshot de baie de stockage, serveurs de fichiers ...) devant faire l'objet d'une protection de leurs données sont sauvegardés par l'outil unique de sauvegarde et de restauration du SI de l'AP-HP : Commvault

**O** Les infrastructures hébergées dans un cloud public sont protégées par l'outil la solution de sauvegarde et de restauration Commvault à partir d'une ou plusieurs instances directement installées dans ce même cloud public

**I** Il est interdit d'utiliser la solution de sauvegarde pour réaliser de l'archivage de données

## 3. La supervision

**O** La supervision technique et applicative des composants déployés dans le SI de l'AP-HP est réalisée par l'outil unique de supervision du SI de l'AP-HP : Centreon

**R** Pour toute nouvelle solution, il est recommandé qu'elle soit en mesure de communiquer avec la solution de supervision de l'AP-HP, a minima à l'aide du protocole SNMP

# Annexes

## ANNEXE 1 – DOCUMENTS DE REFERENCE

<b>Référentiel Général d'interopérabilité (RGI)</b>	Cadre de recommandations référençant des normes et des standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration ( <a href="http://references.modernisation.gouv.fr/interoperabilite">http://references.modernisation.gouv.fr/interoperabilite</a> )
<b>Référentiel Général d'Accessibilité pour les Administrations (RGAA)</b>	Document décrivant des bonnes pratiques à mettre en œuvre pour assurer l'accessibilité des applications à tous les publics ( <a href="https://references.modernisation.gouv.fr/rgaa-3-0">https://references.modernisation.gouv.fr/rgaa-3-0</a> )
<b>Référentiel Général de Sécurité (RGS)</b>	Document définissant des règles et bonnes pratiques en matière de sécurité des systèmes d'information ( <a href="http://references.modernisation.gouv.fr/securite">http://references.modernisation.gouv.fr/securite</a> )
<b>Recommandations de la CNIL sur le thème de la santé</b>	<a href="http://www.cnil.fr/les-themes/sante/">http://www.cnil.fr/les-themes/sante/</a>
<b>Référentiels GMSIH et ANAP</b>	Les référentiels et dossiers publiés par le Groupement pour la Modernisation des Systèmes d'Information Hospitaliers (GMSIH) et ceux publiés par l'ANAP (Agence Nationale d'Appui à la performance des Etablissements de santé et médico-sociaux), accessibles sur le site de l'ANAP à l'adresse suivante, <a href="http://www.anap.fr/nc/publications-outils/">http://www.anap.fr/nc/publications-outils/</a> (le GMSIH a été intégré à l'ANAP en octobre 2009).



<b>AP- HP</b>	Assistance Publique – Hôpitaux de PARIS
<b>API</b>	Application Programming Interface
<b>BGP</b>	Border Gateway Protocol
<b>CCT</b>	Cadre de Cohérence Technique
<b>CNI</b>	Container Network Interface
<b>CPU</b>	Central Processing Unit : Unité centrale de traitement
<b>COS</b>	Class of Service
<b>DDOS</b>	Distributed Denial Of Service
<b>DIMA</b>	Durée d'Interruption Maximale Acceptable
<b>DIS</b>	Département Infrastructures et Services
<b>DISIC</b>	Direction des Systèmes d'Information et de Communication de l'État (voir SGMAP)
<b>DNS</b>	Domain Name System
<b>DRS</b>	Distributed Ressource Scheduler
<b>DSCP</b>	Differentiated Services Code Point
<b>DSFP</b>	Direction Spécialisée des Finances Publiques
<b>DSI</b>	Direction des Systèmes d'Information
<b>DWDM</b>	Dense Wavelength Division Multiplexing
<b>EAI</b>	Enterprise Application Integration (intégration d'applications d'entreprise)
<b>ETALAB</b>	Mission en charge de l'ouverture des données publiques de l'État (voir SGMAP)
<b>ETL</b>	Extract Transform Load. Outil d'extraction de données d'une base de données, permettant de les modifier et de les y replacer.
<b>FC</b>	Fiber Channel
<b>FTP</b>	File Transfer Protocol
<b>GED</b>	Gestion électronique de documents
<b>GH</b>	Groupement Hospitalier
<b>HDS</b>	Hébergeur de Données de Santé
<b>HTTP</b>	HyperText Transfer Protocol
<b>HTTPS</b>	HTTP sécurisé par SSL
<b>IAAS</b>	Infrastructure As A Service
<b>IOPS</b>	Input / Output Operations per Second
<b>IP</b>	Internet Protocol

<b>IPS</b>	Intrusion Prevention System
<b>ISO</b>	International Standardization Organization
<b>JDBC</b>	Java Database Connectivity
<b>JWT</b>	JSON Web Token
<b>K8S</b>	Kubernetes
<b>LAN</b>	Local Area Network, en français réseau local.
<b>LTO</b>	Linear Tape-Open
<b>MOA</b>	Maître d'ouvrage
<b>MOE</b>	Maîtrise d'œuvre
<b>MPLS</b>	Multi Protocol Label Switching
<b>MTA</b>	Mail Transfer Agent
<b>NAS</b>	Network Attached Storage
<b>NFS</b>	Network File System
<b>NIS</b>	Network Information Service
<b>NTP</b>	Network Time Protocol
<b>OS</b>	« Operating System » : Système d'exploitation
<b>PGSSI</b>	Politique Générale de la Sécurité du Système d'Information
<b>QOS</b>	Quality Of Service
<b>RAC</b>	Real Application Cluster
<b>RGAA</b>	Référentiel Général d'Accessibilité pour les Administrations
<b>RGI</b>	Référentiel Général d'Interopérabilité
<b>RGS</b>	Référentiel Général de Sécurité
<b>RPO</b>	Recovery Point Objective
<b>RTO</b>	Recovery Time Objective
<b>SAAS</b>	Software As A Service
<b>SAE</b>	Système d'Archivage Electronique
<b>SAN</b>	Storage Area Network
<b>SCCM</b>	System Center Configuration Manager
<b>SCSI</b>	Small Computer System Interface
<b>SEDA</b>	Standard d'Echange de Données pour l'Archivage
<b>SGBDR</b>	Système de Gestion de Base de Données Relationnelles
<b>SGMAP</b>	Secrétariat Général pour la Modernisation de l'Action Publique (administration regroupant la DISIC, ETALAB et la Direction interministérielle pour la modernisation de l'action publique)

<b>SI</b>	Système d'Information
<b>SIAP</b>	Système d'Information de l'Assistance Publique – Hôpitaux de Paris
<b>SIF</b>	Système d'Information Financier
<b>SNMP</b>	Simple Network Management Protocol
<b>SQL</b>	Structured Query Langage
<b>SSL</b>	Secure Socket Layer
<b>SSO</b>	Single Sign On
<b>TCP</b>	Transmission Control Protocol
<b>TOIP</b>	Telephony Over IP
<b>VM</b>	Virtual Machine
<b>VMDK</b>	Virtual Machine Disk
<b>VPN</b>	Virtual Private Network
<b>VOIP</b>	Voice Over IP
<b>VRRP</b>	Virtual Router Redundancy Protocol
<b>WAF</b>	Web Application Firewall
<b>WAL</b>	Write-Ahead Logging
<b>WSUS</b>	Windows Server Update Services

## ANNEXE 3 – PROCESSUS DE CONCEPTION ET DE VALIDATION DE L'ARCHITECTURE TECHNIQUE

