

CADRE DE COHERENCE TECHNIQUE DU SYSTEME D'INFORMATION

ASSISTANCE PUBLIQUE HOPITAUX DE PARIS

NORMES ET STANDARDS D'ARCHITECTURE TECHNIQUE
2024 REVISION 1
DSN / SAU / CELLULE ARCHITECTURE TECHNIQUE

SUIVI DES VERSIONS

VERSION	DATE	AUTEUR	OBJET DE LA MODIFICATION
1.0	28/10/2004	P. BRILLANT	CREATION DU DOCUMENT
2.0	17/12/2004	P. BRILLANT	
3.0	21/12/2015	F.PERRIN	
3.3	04/01/2017	RESPONSABLES DES POLES DU DEPARTEMENT INFRASTRUCTURES ET SERVICES (ATI) F.PERRIN	AVANT DERNIERE VERSION
4.0	05/12/2019	EQUIPE ARCHITECTURE DIS VINCENT FETTER DAVID PORTE FABRICE TURBOULT EQUIPE SECURITE DIDIER PERRET CONTRIBUTIONS DES EQUIPES DSI (CSI) ET GH	RESTRUCTURATION MAJEURE <ul style="list-style-type: none"> • RENVOI DES DOCUMENTS REFERENCES EN ANNEXE • ORGANISATION EN REGLES • NOUVELLE REDACTION DE L'ENSEMBLE DES CHAPITRES • PRESENTATION DE MODELES D'ARCHITECTURE
2024_R1	11/2024	DSN/SAU/ARCHITECTURE NAWFAL LAIOUAR JULIEN NOISETTE DAVID PORTE EQUIPE SECURITE DIDIER PERRET CONTRIBUTIONS DES EQUIPES DSN/CSI, DSN/ID, DSN/CSA ET GH	CHANGEMENT DE VERSIONNING : <ANNEE>_<REVISIONN°> ACTUALISATION DES REGLES EXISTANTES ACTUALISATION DES RENVOIS DES DOCUMENTS HOMOGENEISATION DE L'ENSEMBLE DES 57 SCHEMAS Ajouts MAJEURS : <ul style="list-style-type: none"> • INTERDICTION DE DEPLOIEMENT DES BASES DE DONNEES ORACLE • INTERDICTION DE DEPLOIEMENT DES SOLUTION JAVA ORACLE • AJOUT DES REGLES DE TOPOLOGIES DE FLUX INTEREAPPLICATIFS • AJOUT DU METROCLUSTER VMWARE • AJOUT D'UN TABLEAU DE REFERENCE DES SOLUTIONS TECHNIQUES • AJOUT D'UN INDEX

SOMMAIRE

SUIVI DES VERSIONS	2
SOMMAIRE.....	3
INDEX DES FIGURES	6
PREAMBULE.....	8
OBJET DU DOCUMENT	9
A. LES PRINCIPAUX OBJECTIFS	9
B. LES BENEFICIAIRES DU CADRE DE COHERENCE TECHNIQUE	9
I. MAITRISE D'OUVRAGE ET MAITRISE D'ŒUVRE	9
II. LES APPLICATIONS ET LES SYSTEMES	10
C. APPLICATION DES REGLES.....	10
D. DESCRIPTION DES CLASSIFICATIONS DES REGLES	10
E. VALIDATION DE L'ARCHITECTURE TECHNIQUE.....	11
I. REDACTION ET VALIDATION DU CCT	11
II. CONCEPTION ET VALIDATION DE L'ARCHITECTURE TECHNIQUE	11
ARCHITECTURE D'EXECUTION	12
A. LES COMPOSANTS D'INFRASTRUCTURE.....	12
I. LE RESEAU	12
I.1. LES ZONES DE SECURITE HOMOGENE DU SI AP-HP	12
I.2. INTERCONNEXION DES SITES AP-HP	13
I.3. LES SERVICES HEBERGES SUR LE RESEAU MAN[ELICE]	15
I.4. LES DATACENTERS	15
I.5. ACCES INTERNET	16
I.6. PASSERELLE WEB D'INTERCONNEXION FILTREE	17
I.7. CONNEXIONS AVEC LES PARTENAIRES.....	19
I.8. LE RESEAU DATACENTER[BBS] (ZONE SERVEURS CENTRALE)	21
I.9. LES RESEAUX LAN ETHERNET DES ETABLISSEMENTS.....	29
I.10. WLAN.....	29
I.11. LA QUALITE DE SERVICE (QOS).....	30
I.12. CONNEXIONS	31
I.13. LIVRABLES	31
II. LES SERVEURS.....	32
II.1. LES SYSTEMES MAINFRAME.....	32
II.2. LES SERVEURS PHYSIQUES.....	32
II.3. LA VIRTUALISATION	34
II.4. LES SYSTEMES D'EXPLOITATION	44
III. LE STOCKAGE	45
III.1. CONCEPTS	45
III.2. LE STOCKAGE PRIMAIRE	46
III.3. LE STOCKAGE SECONDAIRE	47
IV. LES HEBERGEMENTS	48
IV.1. HEBERGEMENT PROPRE.....	48
IV.2. CLOUD PRIVE	49

IV.3. CLOUD PUBLIC.....	49
V. LE POSTE DE TRAVAIL	51
V.1. MATERIEL.....	51
V.2. SYSTEME	51
V.3. SECURITE	51
V.4. LOGICIELS	52
VI. LES SERVICES D'INFRASTRUCTURE.....	53
VI.1. LA REPARTITION DE CHARGE	53
VI.2. LA HAUTE DISPONIBILITE	55
VI.3. L'AUTHENTIFICATION.....	57
B. LES SERVICES APPLICATIFS	58
I. LES BASES DE DONNEES.....	58
I.1. LES BASES DE DONNEES RELATIONNELLES	58
I.2. LES BASES DE DONNEES NOSQL.....	58
I.3. LA REPLICATION DES DONNEES.....	59
II. LES ECHANGES INTER-APPLICATIFS	60
II.1. LES SOLUTIONS DE GESTION DES FLUX	60
II.2. MODELES DE FLUX INTER-APPLICATIF INTERNE.....	61
II.3. MODELES DE FLUX INTER-APPLICATIF EXTERNE.....	65
II.4. CHIFFREMENT DES ECHANGES	68
II.5. PROTOCOLES D'ECHANGE	69
II.6. AUTHENTIFICATION DES ECHANGES	69
II.7. FLUX D'ECHANGE INTERNE AU SI DE L'AP-HP.....	69
II.8. FLUX D'ECHANGE AVEC DES PARTENAIRES EXTERNES AU SI DE L'AP-HP	70
II.9. LES FORMATS D'ECHANGE	70
II.10. LES ECHANGES DE FICHIERS	70
III. LA PLANIFICATION DES TRAITEMENTS.....	71
IV. ORCHESTRATION	71
V. SERVEUR DE PUBLICATION	71
VI. AUTRES	71
VI.1. SERVEUR D'APPLICATIONS JAVA.....	71
C. LES COMPOSANTS APPLICATIFS	73
I. JAVA	73
ARCHITECTURE D'ADMINISTRATION	74
A. LA SECURITE DES SYSTEMES D'INFORMATION.....	74
I. PRINCIPES GENERAUX DE LA PGSI.....	74
II. ENVIRONNEMENT TECHNIQUE DE SECURITE DU SI DE L'AP-HP.....	74
II.1. POSTE DE TRAVAIL WINDOWS.....	74
II.2. MESSAGERIE ELECTRONIQUE.....	74
III. EXIGENCES TECHNIQUES DE SECURITE.....	74
III.1. POSTE DE TRAVAIL INFORMATIQUE	75
III.2. SERVEURS INFORMATIQUES.....	75
III.3. CONFIGURATION DU SYSTEME D'EXPLOITATION LINUX.....	75
III.4. ANNUAIRE ACTIVE DIRECTORY MICROSOFT	75
III.5. JOURNALISATION.....	76
III.6. TELEASSISTANCE INFORMATIQUE	76
III.7. CRYPTOGRAPHIE	76

III.8. APPLICATIONS WEB	76
III.9. RESEAUX.....	76
III.10. TELEPHONES MULTIFONCTIONS.....	77
III.11. TELEPHONIE SUR IP	77
III.12. SECURITE PHYSIQUE ET DISPOSITIFS DE VIDEO PROTECTION.....	77
III.13. LUTTE CONTRE LES CODES MALFAISANTS	77
B. LA PROTECTION DES DONNEES	78
C. LA SUPERVISION	78
ANNEXES.....	79
A. ANNEXE 1 - DOCUMENTS DE REFERENCE	79
B. ANNEXE 2 - GLOSSAIRE.....	81
C. ANNEXE 3 - PROCESSUS DE CONCEPTION/VALIDATION DU DAT	84
D. ANNEXE 4 - SOLUTIONS TECHNIQUES PAR DOMAINES FONCTIONNELS.....	85
INDEX.....	86

INDEX DES FIGURES

Figure 1 - Les niveaux de règle	10
Figure 2 - Réseau de transport	13
Figure 3 - Le réseau MAN[ELICE]	13
Figure 4 - Services hébergés MAN[ELICE]	15
Figure 5 - Interconnexion Datacenters	15
Figure 6 - Les principaux sites d'hébergement	16
Figure 7 - Accès Internet	17
Figure 8 - WAF CLOUD	18
Figure 9 - Application Delivery Controller/ADC DMZ	19
Figure 10 - Liasions externes au SI	20
Figure 11 - Filtrage (I)	21
Figure 12 - Filtrage (II)	22
Figure 13 - Séparation des flux	23
Figure 14 - Flux métier entre serveurs	23
Figure 15 - Flux d'infrastructure depuis un serveur métier	24
Figure 16 - Flux d'administration vers un serveur métier	24
Figure 17 - Flux de sauvegarde et de restauration d'un serveur	25
Figure 18 - Découpage en couches	26
Figure 19 - Séparation des fonctions	26
Figure 20 - Flux entrant & reverse-proxy	28
Figure 21 - Flux sortant & firewall url-filtering	29
Figure 22 - Interfaces réseau d'un serveur	33
Figure 23 - Architecture du métrocluster VMWARE	36
Figure 24 - Règles d'éligibilité au métrocluster VMWARE	37
Figure 25 - Cluster Kubernetes	38
Figure 26 - Accès à un service conteneurisé	38
Figure 27 - Réseau de conteneurs (CNI)	39
Figure 28 - Création des images	42
Figure 29 - Catégories de stockage	45
Figure 30 - Multipathing SAN	46
Figure 31 - Utilisation du stockage secondaire	47
Figure 32 - Stratégie d'hébergement	48
Figure 33 - Cloud public Architecture Hub & Spoke	50
Figure 34 - Evolutivité horizontale	53
Figure 35 - Gestion des VIP (I)	53
Figure 36 - Gestion des VIP (II)	54
Figure 37 - Consommation d'un service redondé	54
Figure 38 - Principes RPO / RTO	55
Figure 39 - Haute-disponibilité (I)	56
Figure 40 - Haute disponibilité (II)	56
Figure 41 - Flux inter-applicatifs - Topologie SI→ SI interdite	61
Figure 42 - Flux inter-applicatifs - Topologie SI→ SI obligatoire	61
Figure 43 - Flux inter-applicatifs - Topologie SI↔GHU interdite	62
Figure 44 - Flux inter-applicatifs - Topologie SI↔GHU obligatoire	63
Figure 45 - Flux inter-applicatifs - Topologie SI↔CLOUD PRIVE interdite	63

Figure 46 - Flux inter-applicatifs - Topologie SI↔CLOUD PRIVE obligatoire.....	64
Figure 47 - Flux inter-applicatifs - Topologie GHU↔GHU interdite	64
Figure 48 - Flux inter-applicatifs - Topologie GHU↔GHU obligatoire	64
Figure 49 - Flux inter-applicatifs - Topologie SI↔CLOUD PRIVE interdite.....	65
Figure 50 - Flux inter-applicatifs - Topologie SI↔CLOUD PRIVE obligatoire.....	65
Figure 51 - Flux inter-applicatifs - Topologie GHU↔SAAS CLOUD interdit.....	66
Figure 52 - Flux inter-applicatifs - Topologie GHU↔SAAS CLOUD.....	67
Figure 53 - Flux inter-applicatifs - Topologie PUBLIC→SI interdit	67
Figure 54 - Flux inter-applicatifs - Topologie PUBLIC→GHU autorise	67
Figure 55 - Flux inter-applicatifs - Topologie PUBLIC→GHU interdit.....	68
Figure 56 - Flux inter-applicatifs - Topologie PUBLIC→GHU autorisé	68
Figure 57 - Puit de fichiers pour les flux.....	70

PREAMBULE

Le Cadre de Cohérence Technique (CCT) du Système d'Information (SI) de l'Assistance Publique – Hôpitaux de Paris (AP-HP) s'inscrit dans le prolongement du 'Cadre d'Urbanisation', document de référence pour l'architecture des systèmes d'information de la DSN. Le CCT tient compte également 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 Numériques (DSN) de l'AP-HP, via l'adresse dsn-sau-archi@aphp.fr.

* *
*

Les prescriptions du référentiel général d'interopérabilité 'RGI', du référentiel général d'amélioration de l'accessibilité 'RGAA' et du référentiel général de sécurité 'RGS' dans leur dernière version respective sont à respecter. Les prescriptions essentielles sont transposées dans ce Cadre de Cohérence Technique de l'AP-HP.

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,

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.

OBJET DU DOCUMENT

A. LES PRINCIPAUX OBJECTIFS

Le CCT 'Cadre de Cohérence Technique' du SI 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'interopérer entre eux et avec les partenaires extérieurs. Sur ce dernier point, le CCT s'appuie sur, complète et précise le RGI 'Référentiel Général d'Interopérabilité' ainsi que le 'Cadre d'interopérabilité AP-HP v2'
- ⇒ 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 communication, bases de données locales, gestion des habilitations, etc.).

B. LES BENEFICIAIRES DU CADRE DE COHERENCE TECHNIQUE

I. MAITRISE D'OUVRAGE ET MAITRISE 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 DSN 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 la DINUM (Direction Interministérielle du NUMérique).

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.

II. LES APPLICATIONS ET LES SYSTEMES

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, etc.) qu'à la seule condition d'avoir fait l'objet d'un rapport d'expertise technique favorable du pôle Centre de Solutions des Infrastructures (CSI) et du pôle Sécurité du Système d'Information (SSI) de la DSN de l'AP-HP.

Dans le cadre d'une mutualisation des expériences, la description d'application à contexte innovant est remontée à la DSN 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 DSN de l'AP-HP et peut aboutir à une évolution du CCT.

C. APPLICATION DES REGLES

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 système d'information de l'AP-HP.

D. DESCRIPTION DES CLASSIFICATIONS DES REGLES

Les règles décrites dans le Cadre de Cohérence Technique présentent trois niveaux de classification schématisés selon trois codes couleur différents (Voir les règles du RFC 2119) :

O	<u>OBLIGATOIRE [RFC 2119 : MUST]</u> La règle décrite constitue une exigence à respecter absolument. Aucun écart n'est toléré.
R	<u>RECOMMANDE [RFC 2119 : SHOULD]</u> 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.
I	<u>INTERDIT [RFC 2119 : MUST NOT]</u> La règle décrite constitue une interdiction de mise en œuvre à respecter absolument.

Figure 1 - Les niveaux de règle

E. VALIDATION DE L'ARCHITECTURE TECHNIQUE

I. REDACTION ET VALIDATION DU CCT

Le CCT est un document de synthèse auquel contribuent les différentes équipes de la DSN & DSIL 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.

II. 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/validation du DAT.

Cette phase de conception réunit un ensemble d'acteurs (architectes, experts techniques, experts sécurité, exploitants, chef de projet, intégrateurs, etc.) 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 DSN de l'AP-HP. Cette validation

- ⇒ S'accompagne de la production de trois documents
 - Une fiche de relecture qui consigne l'ensemble des remarques émises par la Cellule Architecture Technique lors 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 DSN de l'AP-HP
- ⇒ Conditionne la mise à disposition des infrastructures de pré-production et de production de la solution informatique

Il est également important de noter que toute application et tout module d'interface doivent être déclarés et décrits dans la cartographie applicative du SI de l'AP-HP. De ce fait, le fournisseur et/ou le chef de projet doivent transmettre toutes les informations utiles au près de la Cellule Urbanisation de la DSN.

ARCHITECTURE D'EXECUTION

Ce 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, etc.

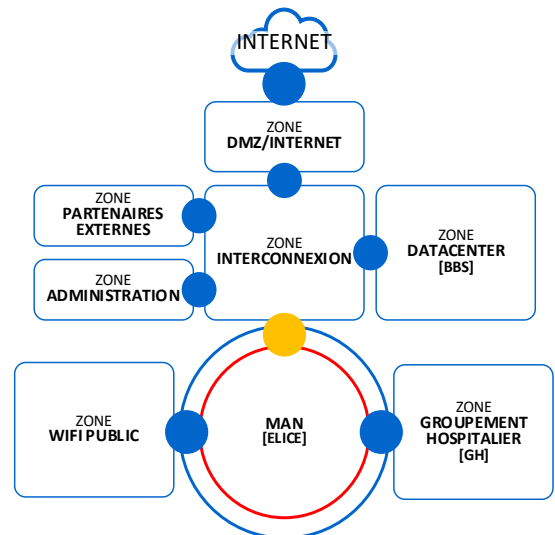
A. LES COMPOSANTS D'INFRASTRUCTURE

I. LE RESEAU

I.1. 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 DATACENTER[BBS], DMZ, etc.) instanciée sur des matériels physiques dédiés. Ces zones de sécurité sont au nombre de sept actuellement :

- ⇒ La **DMZ/INTERNET** 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 **DATACENTER[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 **MAN[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 (DATACENTER[BBS], les GHs, la DMZ, les partenaires, etc.).
- ⇒ La zone **INTERCONNEXION** est une zone d'échange entre les plateforme DATACENTER[BBS], DMZ/INTERNET, MAN[ELICE], Partenaires externes et zone d'admin.
- ⇒ 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 PRIVE, CLOUD PUBLIC**.



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

Il est **interdit de déployer des solutions applicatives** dans la zone **DMZ/INTERNET**. Cette zone porte exclusivement des solutions de sécurité. Les solutions déjà présentes sont amenées à être déplacées dans la zone **DATACENTER[BBS]**.

I.2. INTERCONNEXION DES SITES AP-HP

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

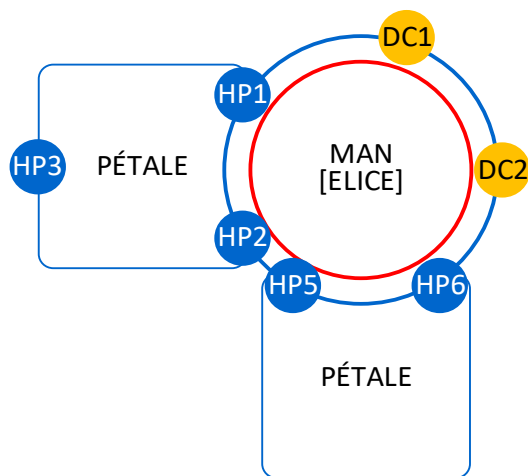


Figure 2 - Réseau de transport

Ce réseau est composé d'une 'double boucle fibre' opérateur dédiée. Il est de 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 MAN[ELICE], sont doublés afin d'assurer la redondance en cas de défaillance d'un équipement.

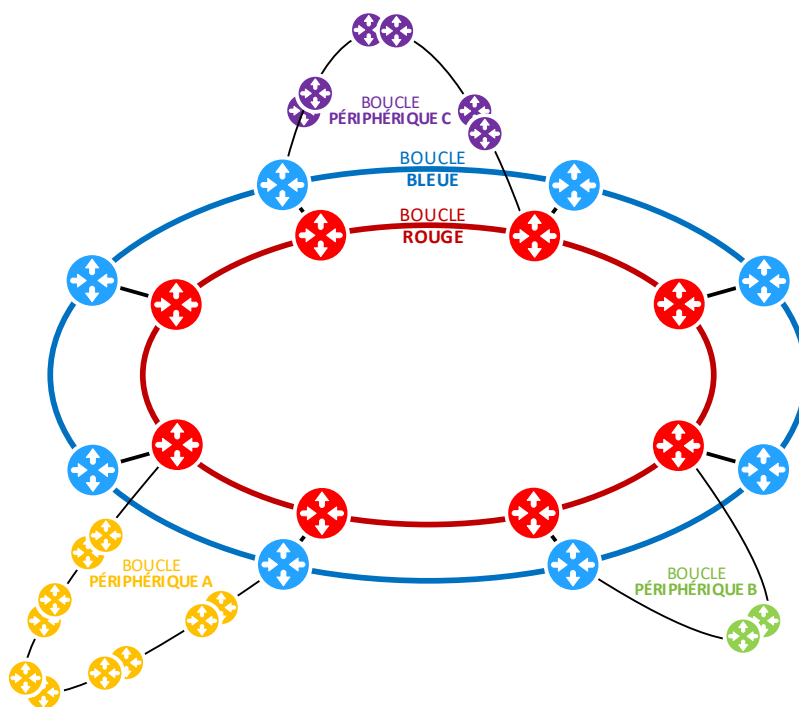


Figure 3 - Le réseau MAN[ELICE]

SITES		DEBIT D'ACCES
ABC	ANTOINE BECLERE	1 GBIT/S
ACH	ALBERT CHENEVIER	1 GBIT/S
APR	AMBROISE PARE	5 GBIT/S
AVC	AVICENNE ^[1]	1 GBIT/S ^[1]
BCH	BICHAT (ANCIEN DATACENTER)	10 GBIT/S
BCT	BICETRE	5 GBIT/S
BCT	BICETRE (DATACENTER N°3)	10 GBIT/S
BJN	BEAUJON	1 GBIT/S
BRC	BROCA	1 GBIT/S
BRK	BERCK	100 MBIT/S
BRS	BROUSSAIS	5 GBIT/S
BRT	BRETONNEAU	1 GBIT/S
CCH	COCHIN	5 GBIT/S
CCL	CORENTIN CELTON	1 GBIT/S
CFX	CHARLES FOIX	1 GBIT/S
CLI	CLICHY (DATACENTER N°1)	10 GBIT/S
EGP	GEORGES POMPIDOU	5 GBIT/S
EPS	AGEPS NANTERRE	1 GBIT/S
ERX	EMILE ROUX	1 GBIT/S
GCL	GEORGES CLEMENCEAU	200 MBIT/S
HAD	HAD VESALE	1 GBIT/S
HMN	HENRI MONDOR	5 GBIT/S
HND	HENDAYE	100 MBIT/S

SITES		DEBIT D'ACCES
HTD	HOTEL DIEU	1 GBIT/S
DUP	DUPUYTREN	1 GBIT/S
JVR	JEAN VERDIER	1 GBIT/S
LCP	LA CHAPELLE (DATACENTER N°2)	10 GBIT/S
LMR	LOUIS MOURIER	1 GBIT/S
LRB	LARIBOISIERE	5 GBIT/S
NCK	NECKER	5 GBIT/S
PBR	PAUL BROUSSE	1 GBIT/S
PSL	PITIE	5 GBIT/S
RDB	ROBERT DEBRE	1 GBIT/S
RMB	RENE MURET	1 GBIT/S
RPC	RAYMOND POINCARE	1 GBIT/S
RTH	ROTHSCHILD ^[2]	1 GBIT/S ^[2]
NSA	DIDEROT	5 GBIT/S
SAT	SAINT ANTOINE	5 GBIT/S
SCB	MAC DONALD	100 MBIT/S
SLS	SAINT LOUIS	5 GBIT/S
SMS	SCA	1 GBIT/S
SPR	SAINTE PERINE	1 GBIT/S
SSL	SAN SALVADOUR	100 MBIT/S
TNN	TENON	1 GBIT/S
TRS	TROUSSEAU	1 GBIT/S
VGR	VAUGIRARD	100 MBIT/S

Note : ^{[1], [2]} Prévision d'upgrade de la liaison fibre à 5Gbit/s courant 2025

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

Les débits d'accès des sites établissement sur ce réseau varient de 100 Mb/s à 5 Gb/s. Les deux sites datacenter disposent d'accès redondé à 10 Gb/s. Un troisième site (salle serveurs) hébergeant les éléments de synchronisation ou d'arbitrage pour les solutions en haute disponibilité dispose d'un accès 5 Gb/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, DATACENTER[BBS], GH, etc.

I.3. LES SERVICES HEBERGÉS SUR LE RESEAU MAN[ELICE]

Le réseau MAN[ELICE] héberge des services communs aux différents hôpitaux et à la zone serveurs DATACENTER[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.

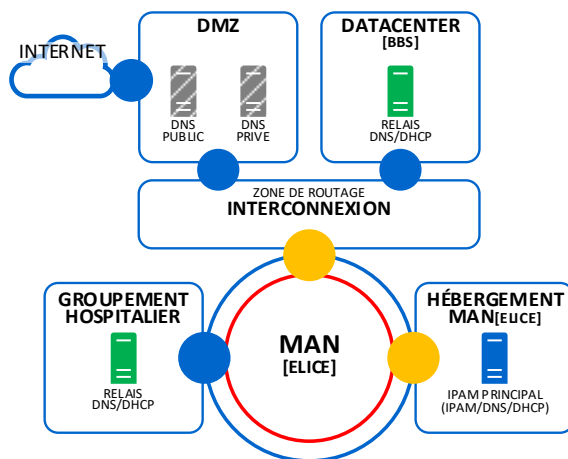


Figure 4 - Services hébergés MAN[ELICE]

I.4. LES DATACENTERS

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

- ⇒ Datacenter 1 (CLICHY/CLI)
- ⇒ Datacenter 2 (LACHAPELLE/LCH)

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 délivrant les services suivants :

- ⇒ 2 Fiber Channel (FC) 100 Gb/s [4x25Gb/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.

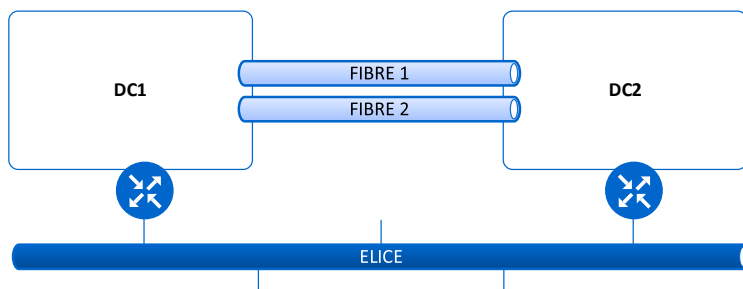


Figure 5 - Interconnexion Datacenters

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 les environnements de qualification. Ce troisième site (en prévision 2025) disposera d'un accès à 10Gb/s redondé et d'une infrastructure réseau hautement disponible. Ce site sera accessible au travers du réseau MAN[ELICE] uniquement via un niveau 2 VPLS actif/passif vers les deux autres Datacenters.

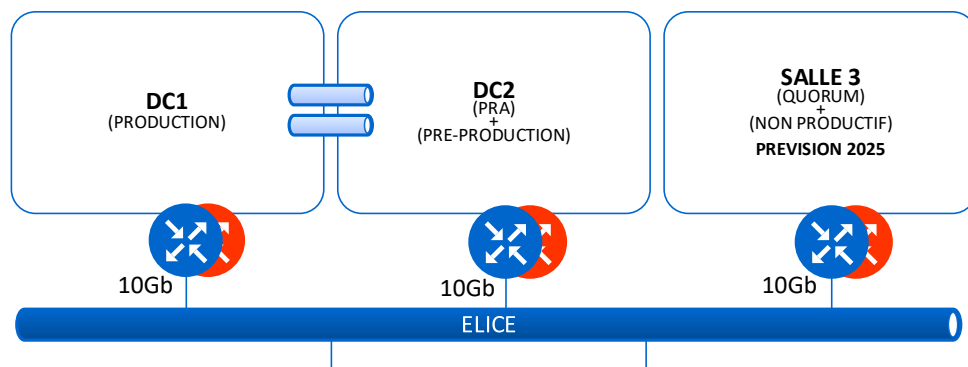


Figure 6 - Les principaux sites d'hébergement

I.5. ACCES INTERNET

L'AP-HP dispose d'un accès Internet à 10 Gb/s redondé sur les deux datacenters en mode actif/passif. Il est utilisé :

- ⇒ par l'ensemble des personnels de l'AP-HP pour accéder à 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

Les flux d'accès internet sont séparés en 2 catégories au niveau du SI :

- ⇒ Les flux WEB portés par les protocoles HTTP/HTTPS
- ⇒ Les flux HORS WEB représentant tous les autres protocoles

Les **flux HORS WEB** sont protégés par 2 FIREWALLS et 2 ROUTEURS (FAI) qui sont doublement connectés sur les cœurs de réseau de la zone Intranet.

Les **flux WEB** transitent par un **firewall dédié** disposant de la fonctionnalité '**URL FILTERING**'. Cette protection est utilisée afin d'accéder de façon implicite et de façon routée aux ressources web Internet.

L'ensemble des ces flux sortant passent également par un antiddos déployé entre les FIREWALLS précédemment cités et les routeurs Opérateur. Cet équipement permet de filtrer et protéger les flux en provenance d'Internet à destination de l'AP-HP, mais aussi des flux en provenance de l'AP-HP vers internet. L'antiddos dispose d'une licence autorisant le filtrage pour un débit à hauteur de 8 Gb/s.

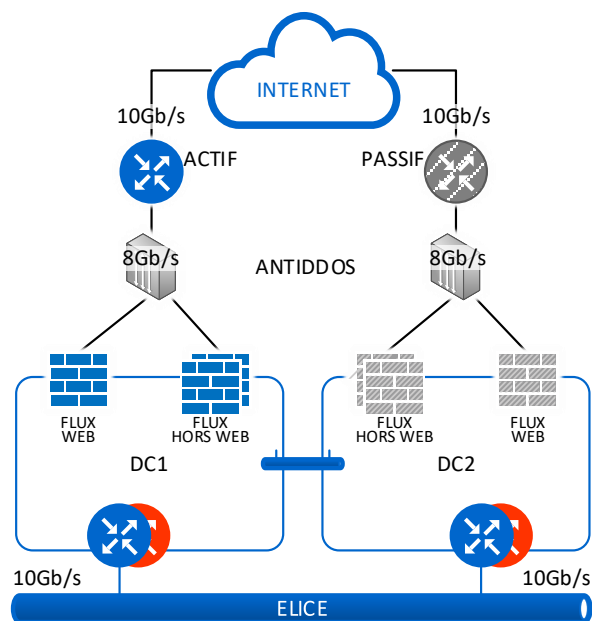


Figure 7 - Accès Internet

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

○ L'ensemble des **FLUX WEB sortants** échangés depuis les éléments du SI (postes de travail, Citrix, serveurs, etc.) vers une ressource internet en HTTP/HTTPS **doit être filtré** par le **FIREWALL** portant la fonctionnalité **URL-FILTERING**.

○ L'ensemble des **FLUX dits HORS-WEB sortants**, quant à eux, **doit être filtré** par la 2ème infrastructure de **FIREWALL**, i.e. celle ne portant pas la fonctionnalité URL-FILTERING.

! Les **infrastructures** hébergées dans la **zone DATACENTER[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 DATACENTER[BBS] **est interdit et bloqué**.

I.6. PASSERELLE WEB D'INTERCONNEXION FILTREE

L'interconnexion entre Internet et un service HTTP/HTTPS de l'AP-HP est effectuée à travers 2 zones distinctes qui se succèdent :

- ⇒ Une 1^{ère} zone, hors AP-HP, hébergée dans le CLOUD fournissant un 1^{er} niveau de service de sécurité de filtrage de flux.

- ⇒ Une 2^{ème} zone, physiquement dans le SI AP-HP, dédiée à l'hébergement d'équipements fournissant un 2^{ème} niveau de service de sécurité de filtrages de flux.

6.1. 1^{ERE} ZONE D'INTERCONNEXION

Cette zone est hébergée dans le CLOUD. Elle intègre des équipements de filtrage qui effectuent une **1^{ère} dépollution** des **FLUX WEB**, protocoles HTTP/HTTPS, entrant à destination de services internes au SI de l'AP-HP ou de services AP-HP hébergés en SAAS/CLOUD hors du SI de l'AP-HP.

- O** Tout **FLUX WEB** en provenance d'Internet, utilisant le **protocole HTTP/HTTPS**, à destination d'un service hébergé soit dans le SI de l'AP-HP, soit en SAAS/CLOUD externe au SI de l'AP-HP, **doit obligatoirement passer** par les **éléments de filtrage WAF** hébergés dans le **CLOUD**.

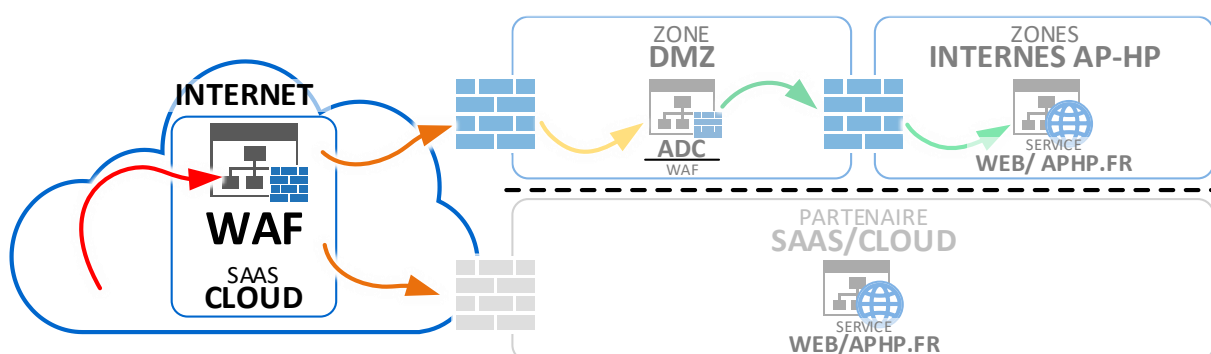


Figure 8 - WAF CLOUD

6.2. 2^{EME} ZONE D'INTERCONNEXION

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 DATACENTER[BBS] n'est autorisé.

- I** Aucun flux initié depuis la DMZ et allant vers la zone sécurisée DATACENTER[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 '**IPS**' (Intrusion **P**revention **S**ystem).

L'AP-HP dispose d'une infrastructure '**ADC**' (Application **D**elivery **C**ontroller), solution de type load balancer avancée, fournissant des fonctionnalités de Firewall Applicatif Web (WAF) qui permettent de sécuriser les accès aux services WEB hébergés dans le SI de l'AP-HP et exposés sur Internet. (**Voir les fonctionnalités de l'ADC** : Gestion des flux web utilisateurs vers une application interne p.27 et La répartition de charge p.53)

La solution '**ADC**' du système d'information de l'AP-HP est assurée par le solution **RADWARE ALTEON**.

- Tous les flux web en provenance d'Internet et entrant dans le SI doivent transiter par le composant technique ADC (Application Delivery Controller) de la DMZ, permettant d'activer l'analyse des flux via la fonctionnalité de pare-feu applicatif (WAF).

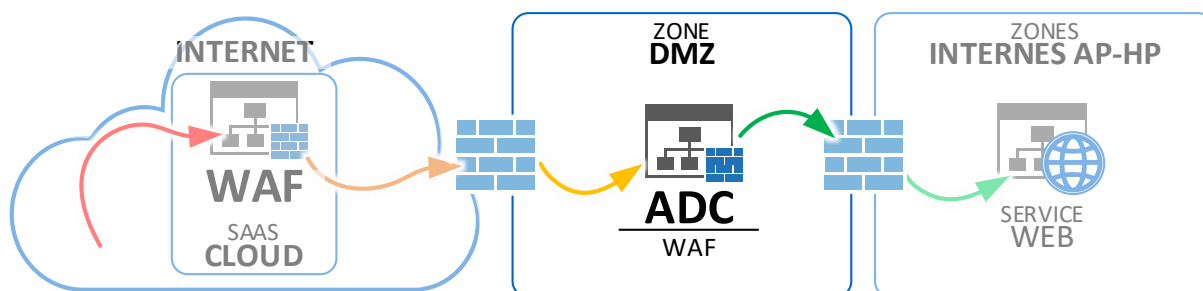


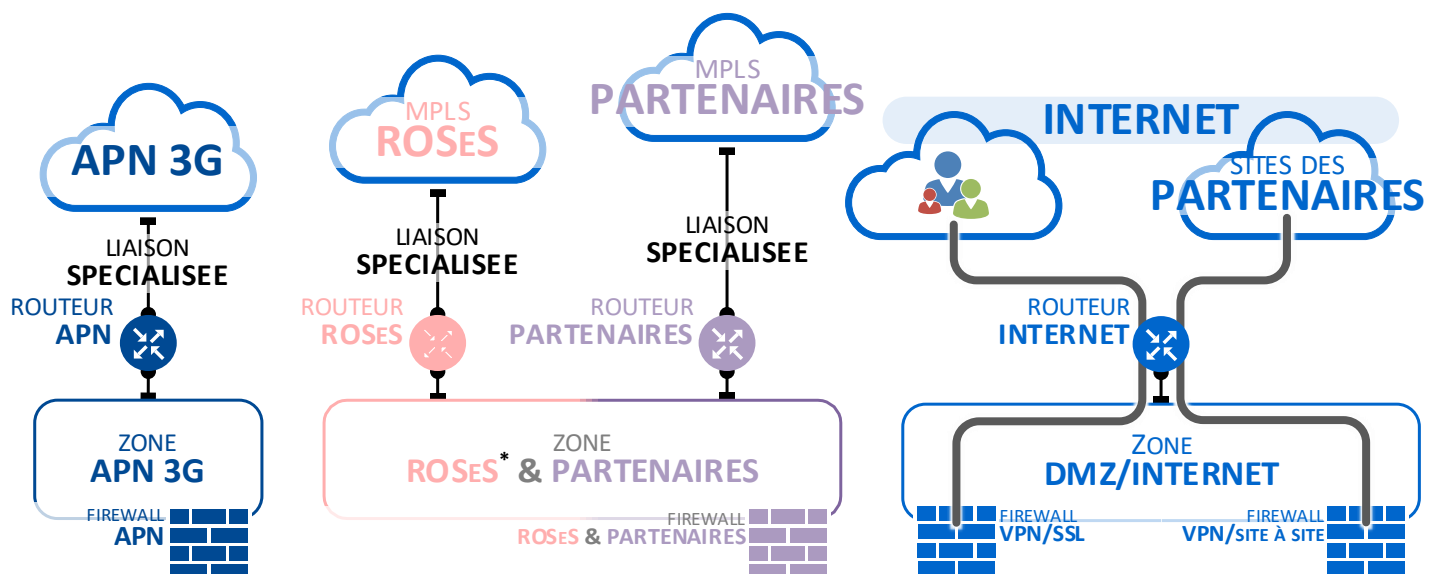
Figure 9 – Application Delivery Controller/ADC DMZ

I.7. 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
VPN/SSL	<p>LE VPN SSL EST UTILISE NOTAMMENT POUR DES ECHANGES QUI NE NECESSITENT PAS DE CONNEXIONS INITIALISEES DEPUIS LE RESEAU AP-HP</p> <p>L'ACCES AU VPN SSL EST SOUMIS A L'AUTHENTIFICATION. LES COMPTES D'ACCES DOIVENT ETRE NOMINATIFS. LES COMPTES GENERIQUES NE SONT PLUS SUPPORTES HORMIS DEROGATION POUR DES CAS PARTICULIERS APRES VALIDATION DE L'EQUIPE SECURITE OPERATIONNELLE DE LA DSN DE L'AP-HP</p>
VPN/SITE - SITE	<p>IL PERMET DE REpondre AU BESOIN D'ECHANGES INITIES DEPUIS L'AP-HP VERS LE PARTENAIRE ET INVERSEMENT.</p> <p>L'ENSEMBLE DES CONNEXIONS VPN SONT ETABLIES AVEC UN FIREWALL VPN DEDIE AU « VPN SITE TO SITE ET MPLS PARTENAIRES »</p>
MPLS/PARTENAIRE	<p>IL REpond AU BESOIN D'ECHANGE AVEC QUALITE DE SERVICE (QOS)</p> <p>TOUTES LES CONNEXIONS DISTANTES SONT CENTRALISEES EN UN POINT UNIQUE ET REDONDE DE L'AP-HP.</p> <p>UN VPN PARTENAIRE EST CONSTRUIT SUR UNE ARCHITECTURE DE TYPE HUB & SPOKE. LA PARTIE HUB (POINT D'ACCES CENTRAL A 10Mb/s EN ACTIF/PASSIF) EST REALISEE 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'ACCES MPLS PARTENAIRES BENEFICIE DE QOS (TRANSPORT DE FLUX DE DONNEES ET DE VOIX).</p> <p>L'ENSEMBLE DES CONNEXIONS VPN SONT ETABLIES AVEC UN FIREWALL VPN DEDIE AU « VPN SITE TO SITE ET MPLS PARTENAIRES »</p>

TYPE DE CONNEXION	CAS D'USAGE
MPLS/AP-HP	<p>LES SITES CLIENTS RACCORDES AU RESEAU MPLS DE L'AP-HP SONT PRINCIPALEMENT MIS A DISPOSITION DES HOPITAUX. ILS SONT AU NOMBRE DE 15 A CE JOUR ET SONT RACCORDES AU RESEAU MPLS AP-HP. TOUS CES SITES DISTANTS SONT RACCORDES EN UN POINT UNIQUE ET REDONDE DE L'AP-HP.</p> <p>CE MPLS AP-HP EST CONSTRUIT SUR UNE ARCHITECTURE DE TYPE HUB & SPOKE. LA PARTIE HUB (POINT D'ACCES CENTRAL A 90MB/S EN ACTIF/PASSIF) EST REALISEE AU NIVEAU DES DEUX DATACENTERS. LES SITES DISTANTS SONT LES SPOKES. ILS 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'ACCES MPLS AP-HP BENEFICIE DE QOS (TRANSPORT DE FLUX DE DONNEES ET DE VOIX).</p>
MPLS/3G	<p>LE VPN MPLS 3G PERMET AUX DETENTEURS DE CLES 3G SFR DE L'AP-HP DE SE CONNECTER AU RESEAU AP-HP SANS PASSER PAR L'ACCES INTERNET.</p> <p>CE RESEAU EST RACCORDE SUR LES FIREWALLS DE LA DMZ DU SI DE L'AP-HP.</p> <p>L'ENSEMBLE DES CONNEXIONS VPN SONT ETABLIES AVEC UN FIREWALL DEDIE AU MPLS 3G. IL EST TOTALEMENT SEPRE DES AUTRES COMPOSANTS RESEAUX OU DE PROTECTION AU SEIN DE L'AP-HP.</p>
MPLS/ADMIN	<p>CET ACCES PERMET DE SE CONNECTER AUX EQUIPEMENTS RESEAUX DES DATACENTERS SANS PASSER PAR LES EQUIPEMENTS DE ROUTAGE QUEL QUE SOIT L'ETAT DU RESEAU.</p>
ROSES	<p>ROSES (RESEAU OPTIQUE SECURISE POUR LA ESANTE) FEDERE TOUS LES TYPES D'ETABLISSEMENTS DE SANTE EN ÎLE-DE-FRANCE, DU CABINET PRIVE AU CENTRE HOSPITALIER, AUTOUR D'UN RESEAU DE TELECOMMUNICATION SECURISE ET A HAUT DEBIT. LE RESEAU DE L'AP-HP DISPOSE D'UNE INTERCONNEXION AVEC LE RESEAU ROSES, A 1Gb/s ET REDONDEE AU NIVEAU DES DEUX DATACENTERS.</p> <p>L'ENSEMBLE DES CONNEXIONS VPN SONT ETABLIES AVEC UN FIREWALL DEDIE A ROSES. IL EST TOTALEMENT SEPRE DES AUTRES COMPOSANTS RESEAUX OU DE PROTECTION AU SEIN DE L'AP-HP.</p>



* ROSES : RÉSEAU OPTIQUE SÉCURISÉ POUR LA ESANTÉ

Figure 10 - Liasions externes au SI

O Tous les VPNs venant de l'extérieur du SI (VPN Site à Site, MPLS Partenaires, MPLS 3G, ROSES) passent obligatoirement par leur élément de filtrage dédié.

I.8. LE RESEAU DATACENTER[BBS] (ZONE SERVEURS CENTRALE)

Le réseau DATACENTER[BBS] hébergeant les serveurs centraux du SI est étendu sur les deux DATACENTERS de l'AP-HP. Ce réseau dispose d'un double raccordement à la zone MAN[ELICE] (réseau d'interconnexion d'établissements) via la zone d'INTERCONNEXION. L'infrastructure de ce réseau de production est redondante.

La zone DATACENTER[BBS] n'inclut pas la zone INTERNET/DMZ qui est une zone de sécurité spécifique et indépendante.

8.1. ADRESSAGE ET ROUTAGE RESEAU

Le réseau DATACENTER[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 ailleurs au sein du SI de l'AP-HP.

O

Un VLAN doit être dimensionné selon des plages d'adresses IP soit en /24, soit en /23.

O

Un VLAN est de Classe C.

R

Les plages d'adresses IP en /24 (256 adresses) sont recommandées

R

Il est recommandé de dimensionner les sous-réseaux d'interconnexion sur des plages IP restreintes (/27, /28, /29).

8.2. FILTRAGE

Tous les segments réseaux de la zone DATACENTER[BBS] sont distribués par des switches 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.

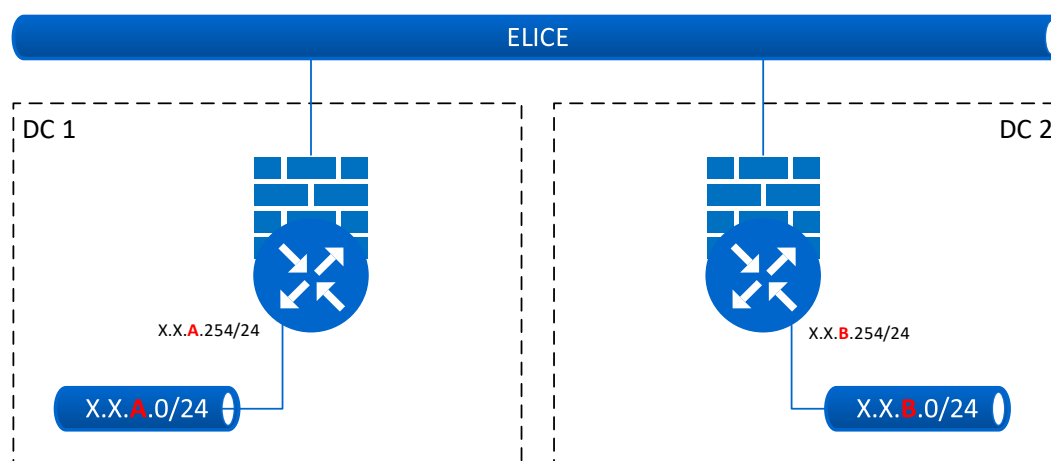


Figure 11 - Filtrage (I)

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

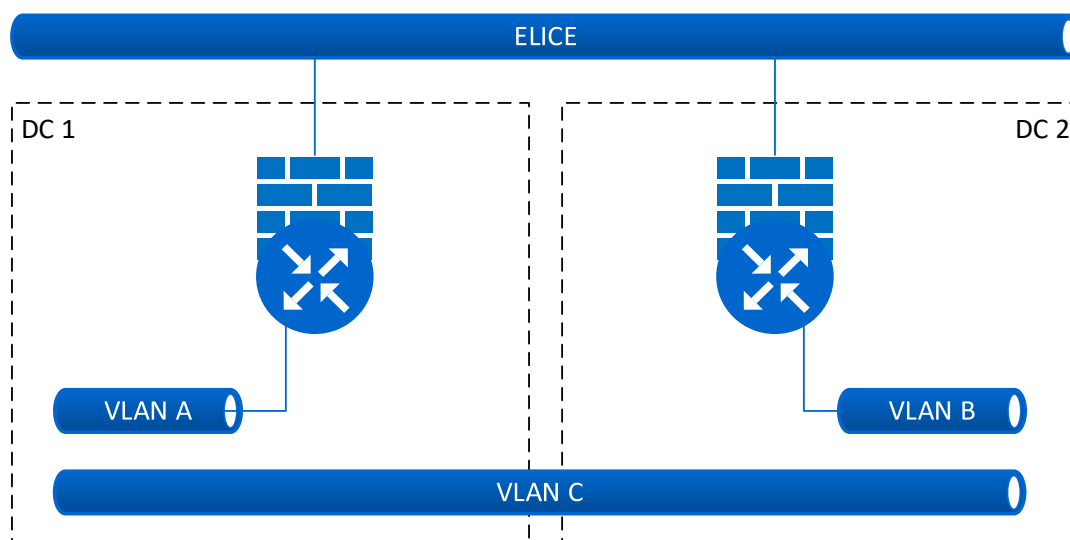


Figure 12 - Filtrage (II)

8.3. SECURISATION PERIMETRIQUE

La **zone DATACENTER[BBS]** héberge toutes les applications centralisées. Cette zone est découpée en 2 sous-zones d'environnement :

- ⇒ Une sous-zone PRODUCTION. Elle héberge toutes les applications dites de PRODUCTION, i.e. les environnements de 'PRODUCTION' et de 'FORMATION'
- ⇒ Une sous-zone HORS-PRODUCTION. Elle héberge toutes les applications dites de NON-PRODUCTION, i.e. les environnements de 'DEVELOPPEMENT', 'QUALIFICATION', 'RECETTE', 'PRE-PRODUCTION'.

Chacune de ces 2 sous-zones 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 entrants et sortants dans les sous-zones de sécurité DATACENTER[BBS] PRODUCTION ou HORS-PRODUCTION doivent être filtrés par les firewalls respectifs de la sous-zone.

O L'ensemble des applications doivent accoster derrière la sous-zone respectivement dédiée au niveau d'environnement de déploiement de l'application :

- ⇒ Les déploiements d'applications en environnement soit de 'PRODUCTION' ou de 'FORMATION' doivent accoster derrière la sous-zone PRODUCTION.
- ⇒ Les déploiements d'applications en environnements de 'DEVELOPPEMENT', de 'QUALIFICATION', de 'RECETTE' ou de 'PRE-PRODUCTION' doivent accoster derrière la sous-zone HORS-PRODUCTION.

I Aucun flux entrant ou sortant dans les sous-zones de sécurité DATACENTER[BBS] PRODUCTION ou HORS-PRODUCTION ne peut contourner le filtrage assuré par les firewalls respectifs de la sous-zone.

8.4. LES TYPES DE RESEAUX

Le réseau DATACENTER[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

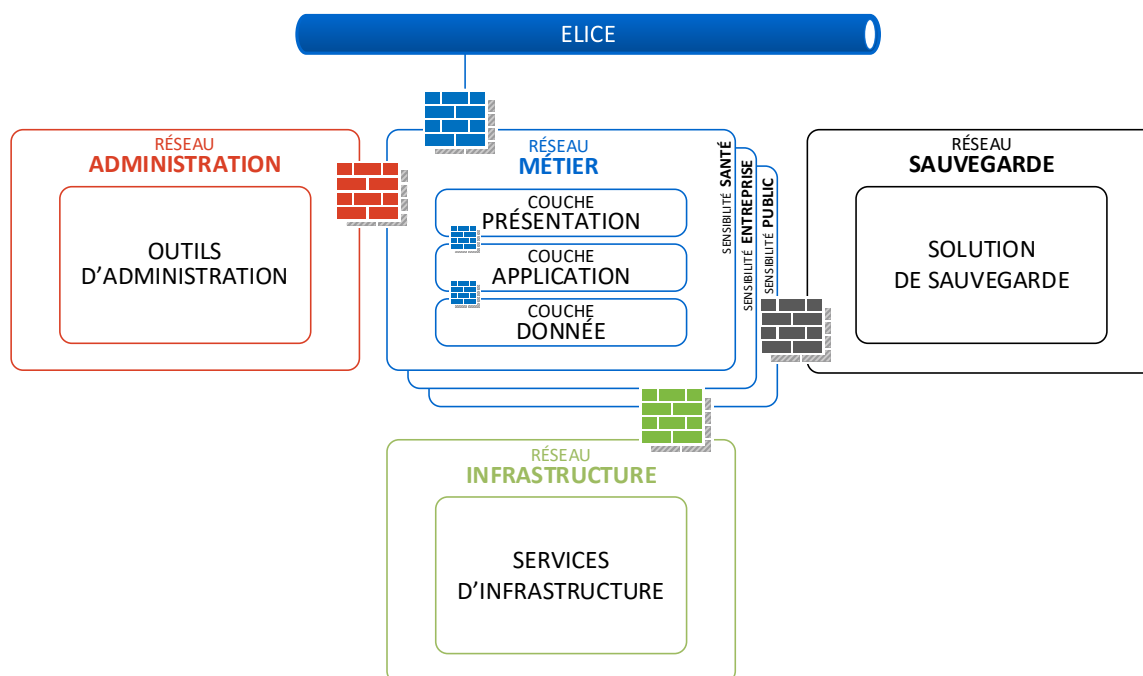


Figure 13 - Séparation des flux

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.

Les serveurs sont rattachés aux différents réseaux présentés ci-dessus par l'intermédiaire d'interfaces dans chaque zone réseau.

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

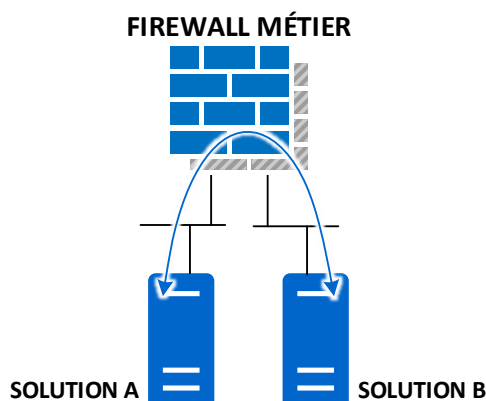


Figure 14 - Flux métier entre serveurs

- Les échanges entre un serveur métier et un service d'infrastructure DNS, NTP, AD, etc. 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.

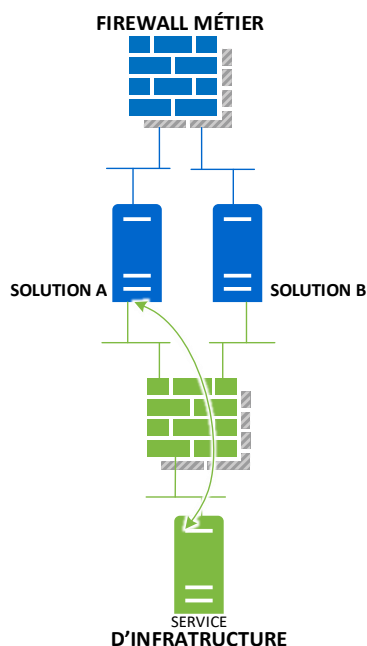


Figure 15 - Flux d'infrastructure depuis un serveur métier

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

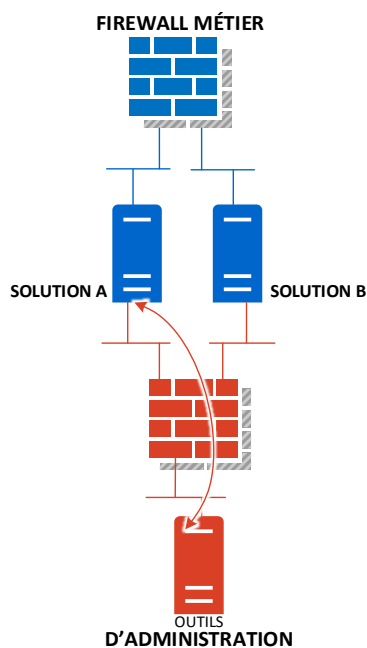


Figure 16 - Flux d'administration vers un serveur métier

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

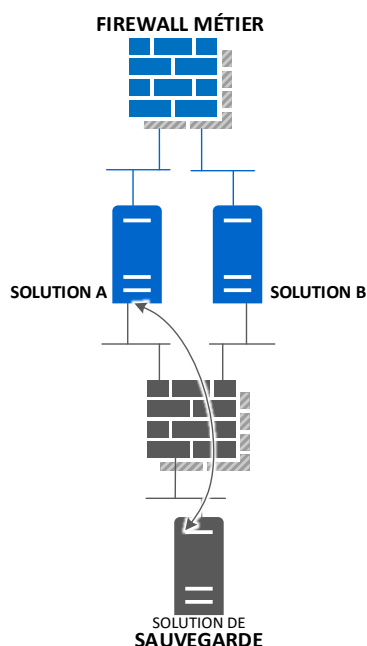


Figure 17 - Flux de sauvegarde et de restauration d'un serveur

REMARQUE : 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.

8.5. LE RESEAU DE SERVICE METIER

a) PRINCIPE DE CLOISONNEMENT PAR COUCHE

Les architectures applicatives de l'AP-HP 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, protégeant les biens essentiels et 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'AP-HP.

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 autre couche, à l'exception de ceux des couches immédiatement inférieure ou supérieure. Chaque couche ne communique qu'avec ses voisins immédiats.

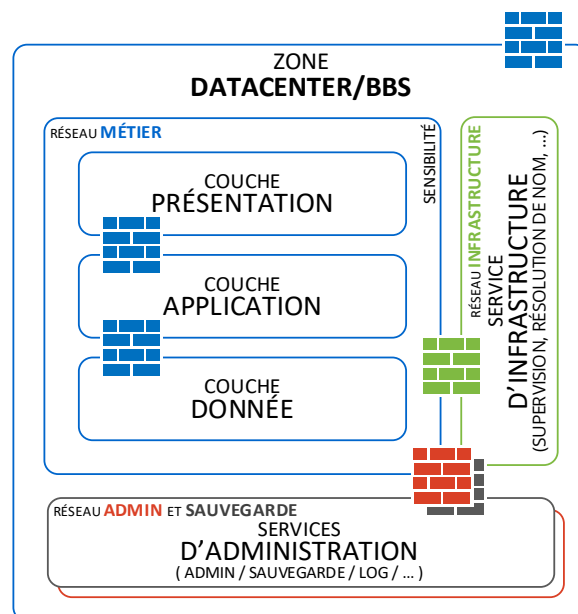


Figure 18 - Découpage en couches

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, etc.).

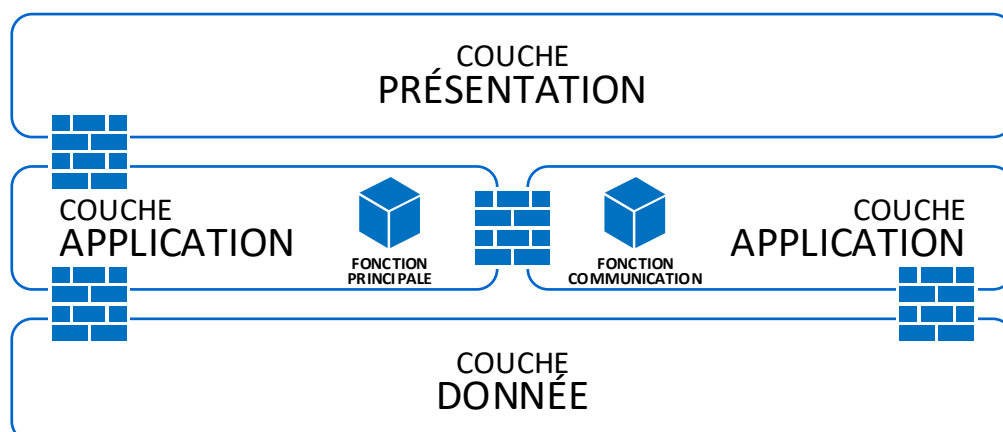


Figure 19 - Séparation des fonctions

b) DECOUPAGE SELON LA SENSIBILITE DES DONNEES

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

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

Ainsi, les données et les applications doivent être regroupées en fonction de leurs sensibilités, on parle alors de zone de sensibilité. Ce cloisonnement est effectué à la fois par le filtrage des firewalls et par croisement par VLANs, VLANs dédiés à leur zone de sensibilité. 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 placer 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 VERS UNE APPLICATION INTERNE

Les services WEB portés par les ressources internes du SI AP-HP n'ont pas d'accès direct. Ces services WEB doivent être accédés par les utilisateurs internes ou externes à partir d'une URL de service exposée par un élément intermédiaire appelé '**Reverse-Proxy**'.

Les fonctions principales du '**Reverse-Proxy**' sont :

- ⇒ De rediriger les requêtes WEB des utilisateurs vers les ressources internes portant les services demandés par l'URL transmise.
- ⇒ De répartir la charge du flux sur plusieurs des serveurs si l'architecture de la solution portant les services demandés par l'URL transmise le permet.
- ⇒ De mettre à disposition un cache des services 'backend' de la solution.
- ⇒ D'offrir une couche de sécurité complémentaire (masquage des serveurs applicatifs, filtrage du trafic, chiffrement des flux)

Les fonctionnalités '**Reverse-Proxy**' sont portées par la solution '**ADC**' (**A**pplication **D**elivery **C**ontroller) de la zone DATACENTER[BBS] du SI de l'AP-HP. Cette solution '**ADC**' est assurée par la solution '**RADWARE ALTEON**'.
(Voir les fonctionnalités de l'ADC : Passerelle web d'interconnexion filtrée p.17 et La répartition de charge p.53)

O

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

O

Les **flux web entrants** en provenance **des utilisateurs externes** doivent passer respectivement par les **reverse proxy de la zone DMZ**, puis les **reverse proxy de la zone DATACENTER[BBS]** avant d'être redistribués vers le serveur de présentation hébergeant le service web cible.

I Il est interdit à **des flux web entrants** en provenance **des utilisateurs internes** d'avoir accès en direct au serveur de présentation hébergeant le service web cible, i.e. **une application métier** ne peut être jointe directement par un utilisateur

Si besoin, le '**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).

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 d'une part entre 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. De plus 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.

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.
Cette **sécurité** est assurée par un **certificat TLS** qui doit être porté aussi bien par le ou les '**Reverse-Proxy**' que par le **serveur** de présentation hébergeant le service web cible.

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.

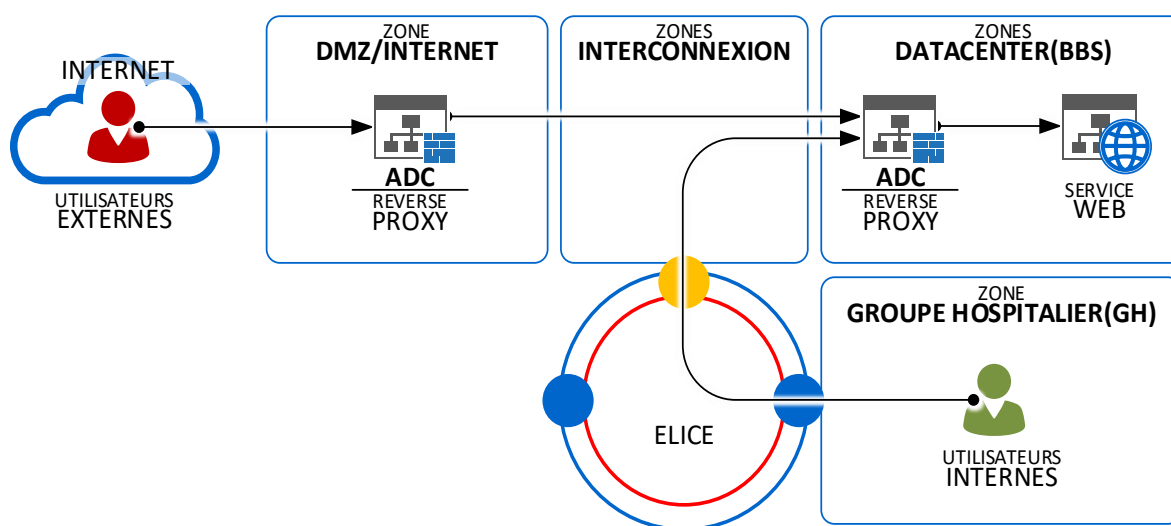


Figure 20 - Flux entrant & reverse-proxy

d) GESTION DES FLUX WEB VERS UNE APPLICATION EXTERNE

Un flux web initié par des utilisateurs internes, par des serveurs CITRIX hébergeant des contextes utilisateurs internes ou des applications internes à destination d'un service Internet, hors du SI AP-HP, passe spécifiquement par un équipement firewall disposant de la fonctionnalité '**URL Filtering**'.

O Tous les flux web initiés au sein SI AP-HP à destination d'Internet doivent **obligatoirement passer par le filtrage firewall '**URL Filtering**'.**

L'équipement firewall 'URL Filtering' est positionné entre le secure LAN et internet

Le rôle d'un firewall 'URL Filtering' en sortie de la plateforme internet est de fournir des mécanismes de filtrage et de connaissance des applications accessibles au travers du protocole HTTP/HTTPS. Il assure le routage à effectuer pour assurer le lien entre une URL saisie et le serveur à contacter.

L'authentification des utilisateurs est de manière nominative grâce à un mécanisme d'interconnexion et d'échange d'information entre de l'AD (Active Directory) et le firewall 'Url Filtering '

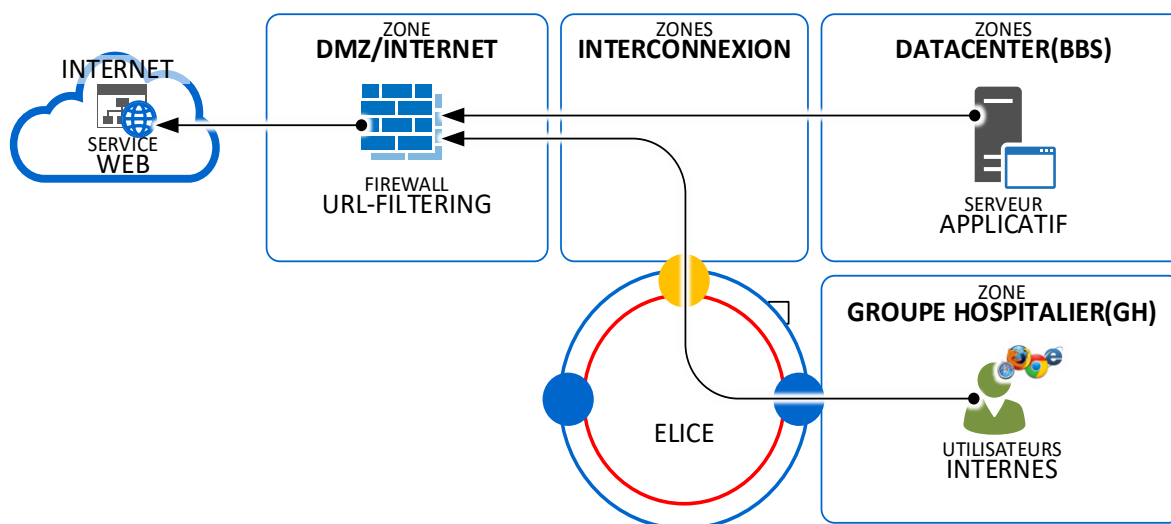


Figure 21 - Flux sortant & firewall url-filtering

I.9. LES RESEAUX LAN ETHERNET DES ETABLISSEMENTS

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

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

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

I.10. WLAN

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

Les réseaux WI-FI public/écoles sont transportés sur le MAN[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 WI-FI publics (authentification, filtrage, proxy, etc.). 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.

1.11. LA QUALITE DE SERVICE (QoS)

La politique de QoS AP-HP marque les flux selon l'importance/la criticité des applications et les exigences techniques des flux, comme ceux nécessitant une faible latence ou la voix. La gestion des priorités est basée sur la norme DIFFSERV.

Un modèle à cinq 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, le cas échéant, 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 leur trafic réseau plus prioritaire.

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 DSN 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 avec les contraintes liées à celle-ci.

Tous les équipements réseau 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.

I.12. CONNEXIONS

I

Les sessions TCP permanentes sont interdites

O

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

I.13. LIVRABLES

O

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 etc.).

Cette **matrice des flux** doit respecter le **modèle fourni par la cellule RESEAU du CSI de l'AP-HP**.

Cette matrice **doit accompagner** le **DAT** (Dossier d'Architecture Technique).

Cette matrice constitue un élément indispensable à la mise en œuvre de toute solution informatique.

II. LES SERVEURS

II.1. LES SYSTEMES MAINFRAME

- I** La mise en place de nouveaux systèmes Mainframes d'IBM ne sont plus autorisés au sein du système d'information de l'AP-HP.

II.2. LES SERVEURS PHYSIQUES

2.1. REGLES GENERALES

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 doit impérativement être installé sur une infrastructure physique quel que soit son niveau d'environnement (développement, qualification, production, etc.).
exemple : Les base de données Oracle

- R** L'implémentation d'une infrastructure physique est limitée aux conditions strictes suivantes :
- ⇒ Condition relative au niveau d'environnement cible : Seuls les environnements 'production', 'pré-production' sont éligibles aux infrastructures physiques (à l'exception de logiciels tiers comme mentionné dans le cadre **[OBLIGATOIRE]** ci-dessus.
 - ⇒ Condition relative au type d'appliquatif embarqué : La liste suivante, non exhaustive, définit les applicatifs éligibles aux infrastructures physiques :
 - Les bases de données
 - Les systèmes distribués (ex : Kubernetes, Mesos...)
 - Les clusters
 - Les solutions SAP (ECC, BI) pour la « central instance »

2.2. FORMAT

- O** Les formats de serveurs physiques autorisés sont :
- ⇒ Le format rack
 - ⇒ Le format châssis/lame
 - ⇒ Le format frame/compute

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

- 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 **'tour'** est **prohibé**.

2.3. ARCHITECTURE

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

- ⇒ L'architecture 'x86'
- ⇒ L'architecture 'Itanium'

O Toute nouvelle infrastructure serveur doit être basée sur l'architecture 'x86/64 bits'.

I L'architecture 'Itanium' n'est plus autorisée au sein du système d'information de l'AP-HP.
EXCEPTION : 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).

2.4. INFRASTRUCTURES CONVERGEES ET HYPERCONVERGEES

O Les infrastructures convergées doivent être conformes aux marchés en vigueur concernant l'acquisition et la mise en œuvre de telles infrastructures.
Actuellement, les infrastructures autorisées sont les suivantes :
⇒ HPE Synergy

O Les infrastructures hyperconvergées doivent être conformes aux marchés en vigueur concernant l'acquisition et la mise en œuvre de telles infrastructures.
Actuellement, les infrastructures autorisées sont les suivantes :
⇒ HPE Simplivity

2.5. INTERFACES RESEAUX

Un serveur doit être capable d'accéder à tous les segments réseaux décrits dans le paragraphe '§A.I.8.4 Les types de réseaux'.

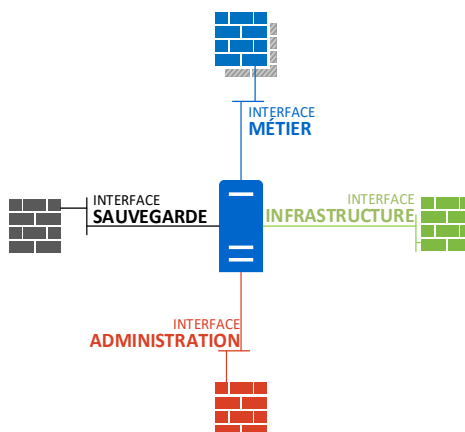


Figure 22 - Interfaces réseau d'un serveur

O Chaque nouveau serveur doit être équipé d'une interface dédiée pour accéder à tous les segments de réseau, chaque interface étant associée uniquement à un segment spécifique.

R Pour les environnements de 'production', il est conseillé de mettre en place une haute disponibilité pour les interfaces réseau suivantes :
⇒ interface réseau d'infrastructure
⇒ interface réseau de sauvegarde

2.6. CARTES GRAPHIQUES

Les GPUs (unités de traitement graphique) sont des processeurs spécialisés initialement conçus pour le rendu graphique. Ces unités de traitement sont devenus essentiels en IA 'Intelligence Artificielle' en raison de leur capacité à effectuer des calculs massivement parallèles, ce qui accélère considérablement l'entraînement des modèles d'apprentissage profond. Grâce à leur architecture rendant possible le traitement rapide de grandes quantités de données, les GPUs sont devenues cruciales pour les algorithmes complexes des IA.

- O Les cartes GPU ne peuvent être installées que sur des infrastructures physiques.

II.3. LA VIRTUALISATION

3.1. LA VIRTUALISATION SYSTEME

a) REGLES GENERALES

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

- O La virtualisation système dans le système d'information de l'AP-HP utilise exclusivement la solution de virtualisation VMware vSphere.

- O Les appliances virtuelles, devant être déployées dans le système d'information de l'AP-HP, doivent être compatibles avec la solution de virtualisation VMware vSphere.

- R Il est conseillé de déployer toute nouvelle solution dans un environnement virtuel, sous forme de VM.

- I Il est interdit de créer des environnements virtuels dont les ressources dépassent les limites suivantes :
⇒ **Ressources limites** autorisées pour une 'VM' : vCPU = 32 et/ou RAM = 128Go (**Monster VM**)
Au de là de ces limites, il est recommandé de privilégier une infrastructure physique.

- I 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, etc.).
exemple : Les bases de données Oracle

- I Lors de la création d'une machine virtuelle, les options de configurations suivantes sont interdites :
⇒ Pass-through VM DirectPath, option qui permet de présenter et de dédier à la VM un composant matériel de l'hyperviseur.
⇒ Affinité CPU, option qui attribue un processeur physique spécifique à la VM.
⇒ Réserve de ressources (CPU/RAM).
⇒ Présentation de stockage en mode bloc de type Raw Device Mapping

b) INFRASTRUCTURES

- O Les serveurs sur lesquels la solution de virtualisation VMware vSphere est installée sont :
⇒ Soit des serveurs physiques
⇒ Soit des systèmes convergés ou hyperconvergés

O Une ferme de serveurs ESXi, dans laquelle des VM hébergées peuvent se déplacer par le mécanisme de vMotion, doit être constituée de serveurs ESXi de modèle identiques.

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

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

c) ARCHITECTURE

O L'architecture pour les serveurs virtuels et l'environnement hôte est autorisé :
⇒ Architecture 'x86' 64 bits.

d) INTERFACES RESEAUX

Les règles sont identiques à celles énoncées pour les serveurs physiques décrits au paragraphe '§A.II.2.5 Interfaces réseaux'.

O La haute disponibilité (HA) des interfaces réseaux est portée par le serveur hôte ESXi. La HA est assurée par les hyperviseurs (load balancing, network failure, notify switches, failback).

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

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 ESXi sont constituées pour :

- ⇒ Répartir l'ensemble des VM en fonction notamment des ressources, grâce au mécanisme de répartition VMWARE DRS.
- ⇒ Pallier au dysfonctionnement d'un ESXi au sein d'une ferme en répartissant les VM concernées sur les autres ESXi 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 de production et de non production, sauf exception explicitement mentionnée dans les livrables de conception.

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

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

R En terme d'extension d'infrastructure d'une ferme ESXi, il est recommandé de ne pas étendre une ferme au delà du frame ou chassis sur lequel la ferme a été créée.

R Il est fortement recommandé qu'une ferme ESX soit composée de serveurs physiques de la même génération.

g) METROCLUSTER VMWARE ESX

La solution métrocluster VMWare est une architecture de haute disponibilité conçue pour assurer la continuité de service entre le DC CLICHY (DC n°1 NOMINAL) et le DC LACHAPELLE (DC n°2 DE REPRISE). Cette solution permet la reprise après sinistre et la migration transparente des charges de travail entre ces 2 sites en cas de défaillance. Cette infrastructure n'est disponible que dans les environnements de 'PRODUCTION'

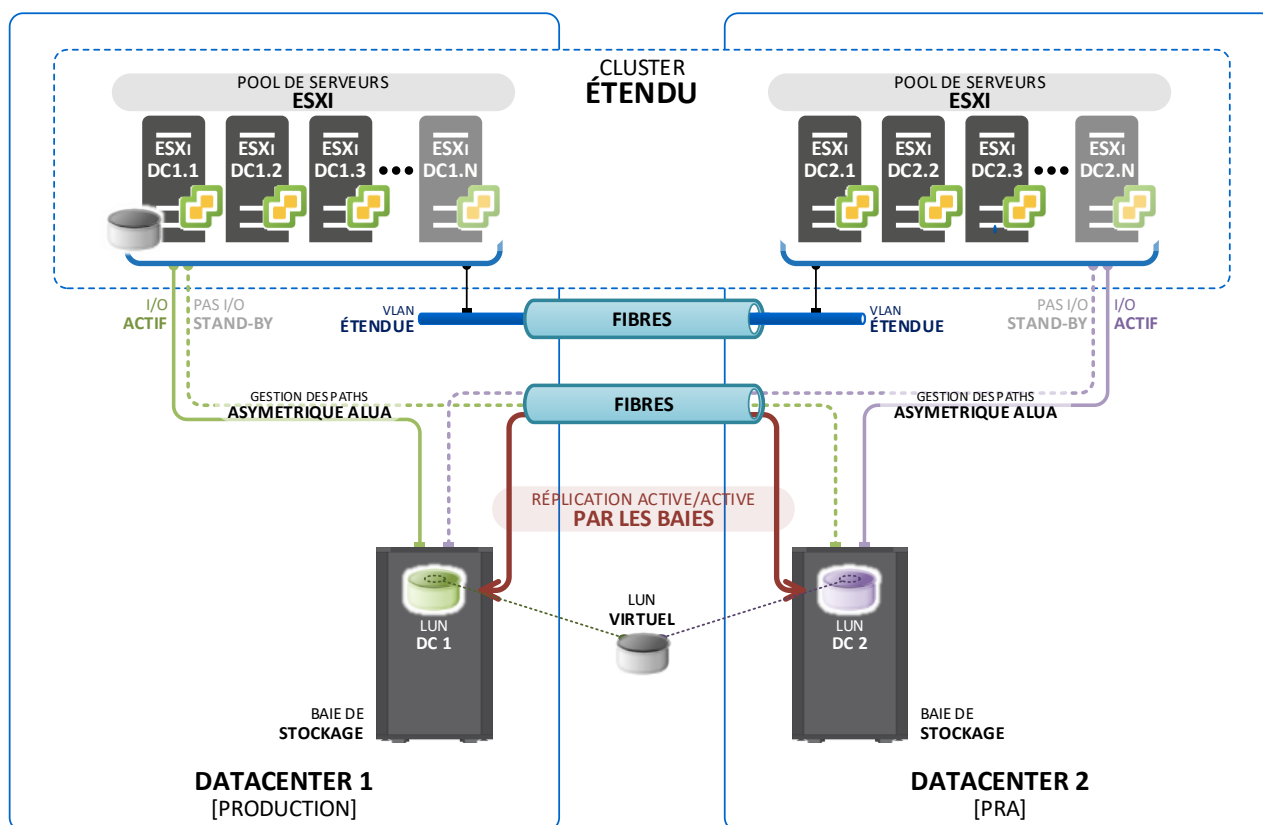


Figure 23 - Architecture du métrocluster VMWARE

O Lors du déploiement d'une solution au sein du métrocluster VMWARE, des règles d'affinités doivent être positionnées spécifiquement pour la solution. Ces règles doivent imposer une localisation DATACENTER unique, i.e. soit dans le DATACENTER n°1 en fonctionnement nominal, soit dans le DATACENTER n°2 lors d'une opération de PRA.

O Quel que soit le niveau d'intégration de l'architecture d'une solution au sein du métrocluster, i.e. hybride (en partie, avec des composants physiques ou virtuels hors du métrocluster) ou totale, le déplacement d'une solution entre le DC NOMINAL et le DC DE REPRISE inclut tous les composants techniques de la dite solution.

I

La répartition d'une solution sur les 2 DATACENTER dans son mode nominal est interdite.

R

Le choix du type de cluster VMware dans lequel une solution peut-être déployée est déterminé par les règles d'éligibilité décrites par le schéma ci-après.

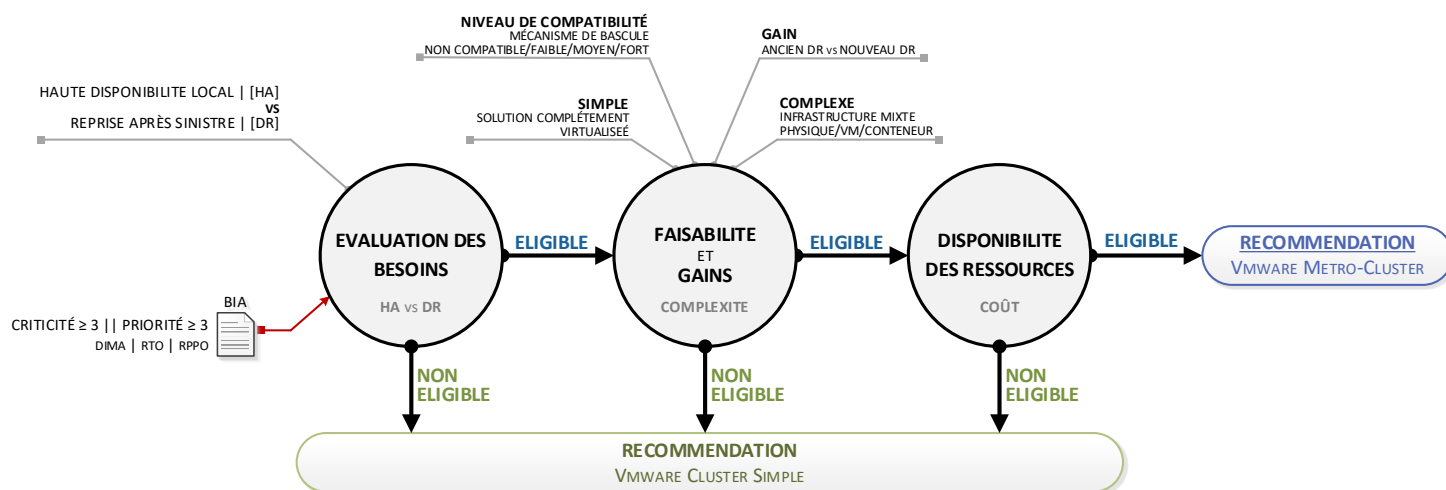


Figure 24 - Règles d'éligibilité au métrocluster VMWARE

3.2. 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).

O

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

O

ContainerD est le **moteur de conteneurisation** du SI de l'AP-HP.

a) INFRASTRUCTURES SERVEURS K8S

L'infrastructure cluster K8S est découpée en 4 zones distinctes afin de respecter le principe de cloisonnement :

- ⇒ Une zone 'ORCHESTRATION' : serveurs/nœuds dits 'MASTER' en cluster
- ⇒ Une zone 'FRONT-END' : serveurs/nœuds dits 'WORKER' dédiés à l'hébergement des conteneurs de services de présentation des solutions déployées dans Kubernetes.
- ⇒ Une zone 'BACK-END' : serveurs/nœuds dits 'WORKER' dédiés à l'hébergement des conteneurs de services applicatifs des solutions déployées dans Kubernetes.
- ⇒ Une zone 'DATA' : serveurs/nœuds dits 'WORKER' dédiés à l'hébergement des conteneurs de services de stockages (service de base de données, ...).

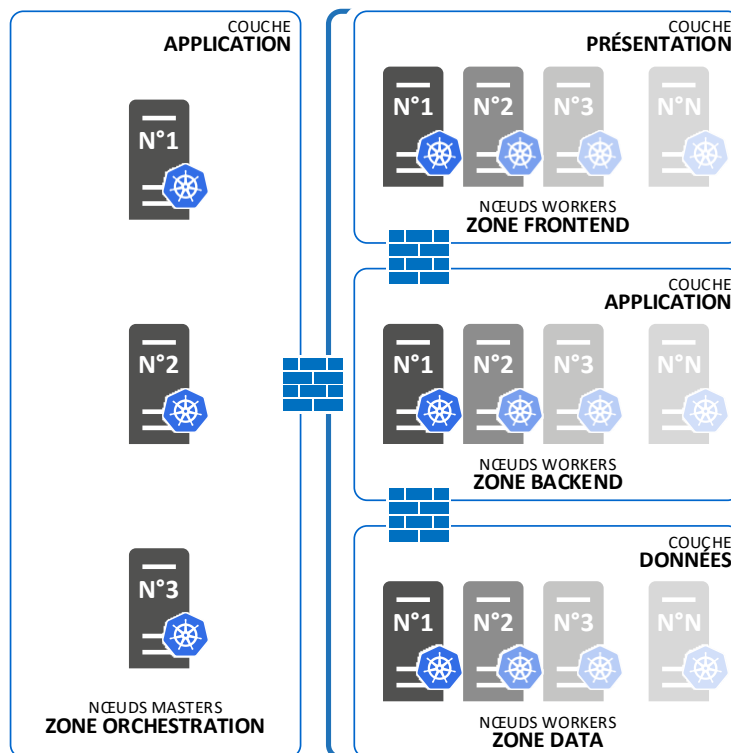


Figure 25 - Cluster Kubernetes

b) ACCES 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', également en conteneurs dans Kubernetes, sont positionnés sur tous les nœuds 'WORKER' de la zone 'FRONT-END'.

- L'accès aux services de présentation des applications conteneurisées doit obligatoirement utiliser une IP virtuelle ayant pour cible les 'INGRESS' des nœuds 'WORKER' du cluster Kubernetes. Cette IP virtuelle doit être portée par une infrastructure matérielle ou logicielle offrant les fonctionnalités de reverse-proxy, de load-balancing et de web application firewall.

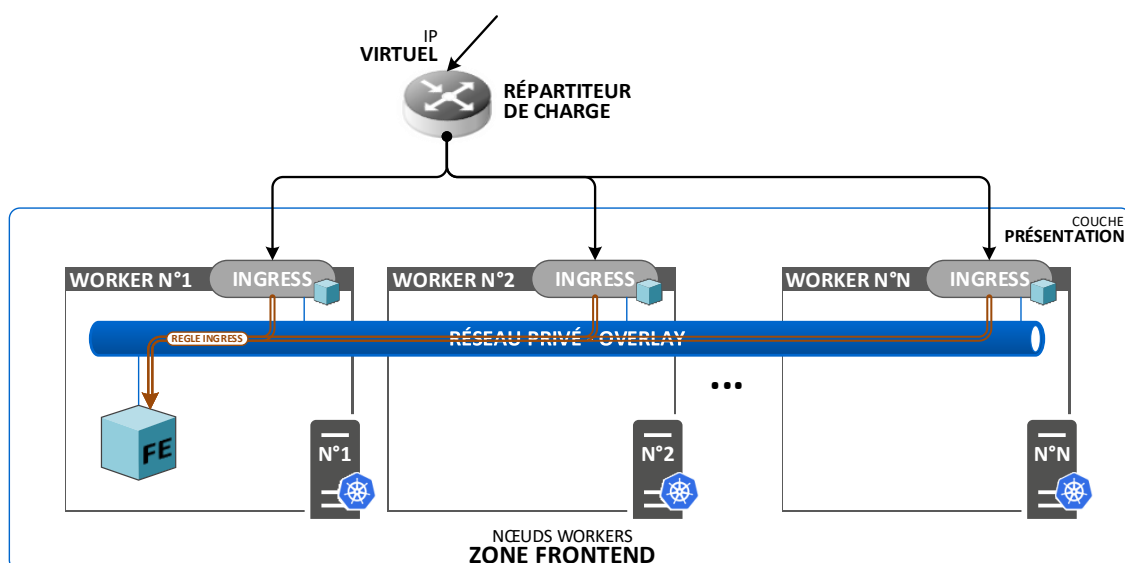


Figure 26 - Accès à un service conteneurisé

O Tout conteneur fournissant un service devant être accédé depuis l'extérieur du cluster Kubernetes doit utiliser une règle 'INGRESS' d'exposition de ce service.

O **NGINX** est la solution **INGRESS** du cluster **Kubernetes** du SI de l'AP-HP.

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

C) LE RESEAU 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 remplir le rôle de 'CNI' doit supporter toutes les fonctionnalités de la politique de filtrage implémentées dans Kubernetes.

O **CALICO** est la **solution 'CNI'** du cluster **Kubernetes** du SI de l'AP-HP.

I La solution 'CNI' ne doit pas utiliser le protocole BGP.

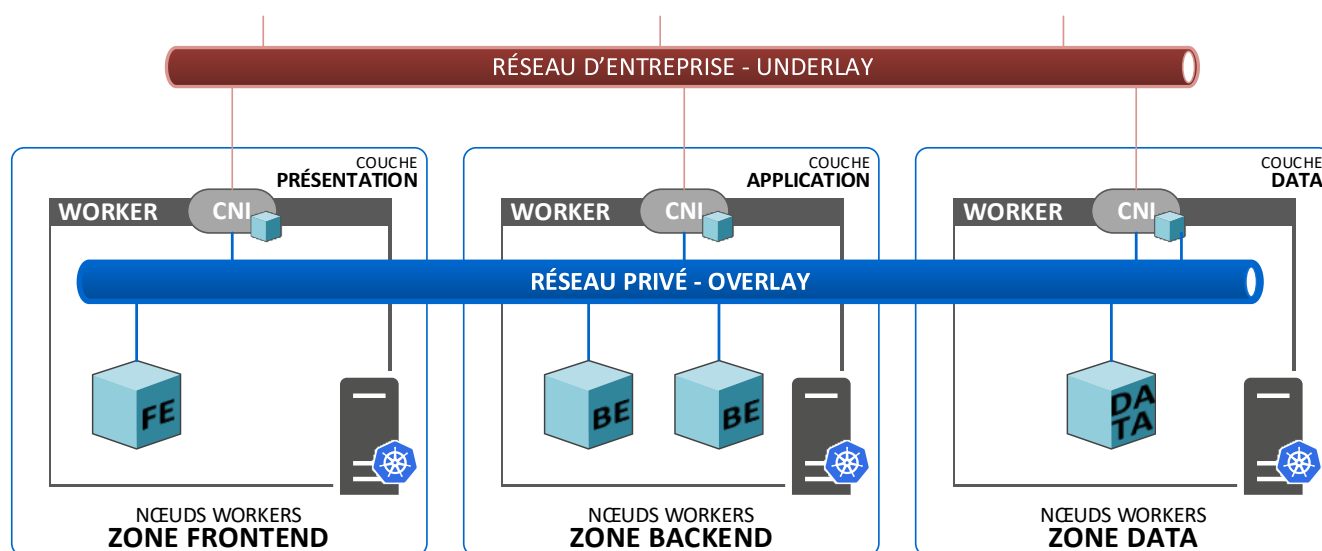


Figure 27 - Réseau de conteneurs (CNI)

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 un cluster virtuel.

O Toute solution applicative déployée au sein d'un cluster Kubernetes **doit être déployée** dans **un ou plusieurs 'NAMESPACE' dédiés**.

O Toute création de '**NAMESPACE**' s'accompagne d'une **limitation des ressources** '**COMPUTE**' [CPU], '**MEMOIRE**' [RAM] et '**STOCKAGE**' [DONNEES EPHEMERES].

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'

⇒ A destination d'autres 'NAMESPACES'

Par défaut, les 'NAMESPACES' sont étanches les uns vis-à-vis des autres.

I Il est **interdit de manipuler les 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**' [CPU] et '**MEMOIRE**' [RAM].

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'** (hors '**CONTENEUR**' d'initialisation).

I Il est **interdit** au '**CONTENEUR**' d'un '**POD**' de **manipuler des données persistantes** se trouvant **localement** dans leur propre image.

- Identification d'un pod

- 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 déploiementL'utilisation des labels et des annotations est obligatoire pour renseigner toutes ces informations

- Choix des workers

La localisation d'un POD au sein des nœuds workers K8S est déterminée par le type de service rendu par le POD déployé.

- Un POD ne peut être déployé que dans l'une des 3 zones suivantes :
 - ⇒ La zone 'FRONT-END' : 'WORKER' dédiés à l'hébergement des conteneurs de services de présentation des solutions.
 - ⇒ La zone 'BACK-END' : 'WORKER' dédiés à l'hébergement des conteneurs de services applicatifs des solutions.
 - ⇒ La zone 'DATA' : 'WORKER' dédiés à l'hébergement des conteneurs de services de stockages (service de base de données, ...).

- 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'.

- Tout flux identifié entre un 'POD' et l'extérieur à K8S doit faire l'objet d'une politique réseau K8S 'INGRESS' (flux en entrée) et/ou 'EGRESS' (flux en sortie).

- Tout 'POD' déployé au sein du cluster K8S 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'AP-HP 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 AP-HP.
- ⇒ **les images d'entreprise** : durcissement et adaptation spécifique AP-HP 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.

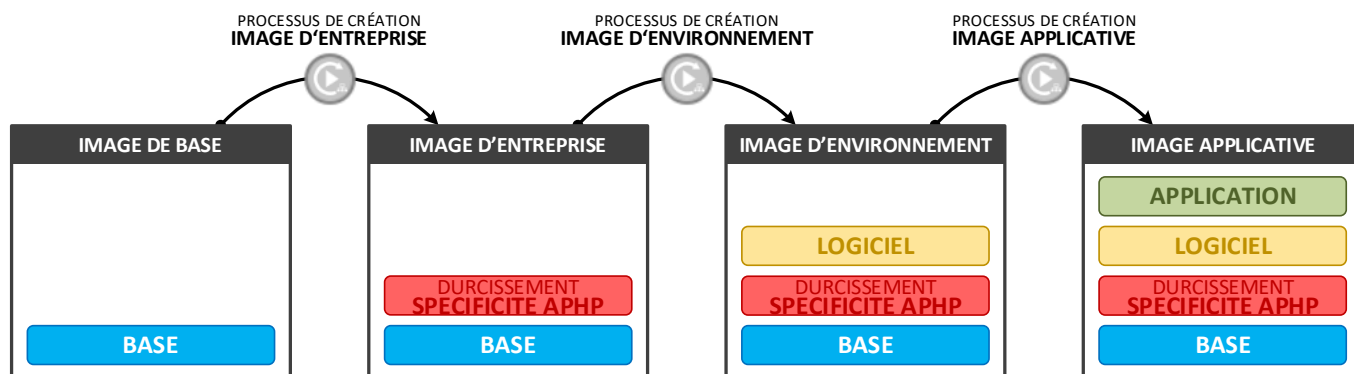


Figure 28 - Création des images

- L'**image de base** est l'image fournie par l'éditeur **Red Hat** (image non modifiée de l'éditeur).
- Les images d'entreprise et d'environnement sont créées dans un workflow interne non spécifique à une solution applicative.
- Toutes les images applicatives utilisées au sein du SI AP-HP sont créées :
 - ⇒ Dans un workflow interne spécifique à la solution à déployer.
 - ⇒ A partir des images d'environnement.
- 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.
- ! Il est interdit d'utiliser une image téléchargée sur Internet.
- ! Il est interdit d'ajouter des composants à une image directement téléchargée d'internet.

g) [LE CONTENEUR](#)

Un conteneur est une instance en cours d'exécution créée à partir d'une image , fournissant un environnement isolé pour exécuter le service d'une application.

- ! Il est interdit à un conteneur de se mettre à jour lors de son démarrage.

h) [LE STOCKAGE PERSISTANT](#)

Le stockage persistant dans un contexte d'un conteneur fait référence à la capacité de conserver des données même après la fin de la vie d'un conteneur. Les conteneurs sont éphémères par nature, ce qui signifie que lorsque les conteneurs sont supprimés, leurs données disparaissent aussi, à moins qu'elles ne soient stockées de manière persistante.

○ La solution de 'stockage persistant' doit fournir un 'plugin' permettant l'interface entre le CSI 'Container Storage Interface' de K8S et la solution de stockage persistant.

○ La solution de stockage persistant pour K8S doit offrir les fonctionnalités :

- ⇒ De provisionnement des 'volumes persistants' : statiquement et dynamiquement.
- ⇒ De redimensionnement des 'volumes persistants' : à froid et à chaud.
- ⇒ Les modes d'accès aux 'volumes persistants' :
 - En RWO – Lecture/Écriture depuis un nœud worker unique (l'accès par de multiples PODs est toujours autorisé depuis cet unique nœud).
 - En ROX – Lecture seule depuis l'ensemble des nœuds workers.
 - En RWX – Lecture/Écriture depuis l'ensemble des nœuds workers.
 - En RWOP – Lecture/Écriture depuis un 'POD' unique.
- ⇒ De snapshot et cloning de 'volumes persistants'.

La solution doit également permettre les types de stockages fichiers et blocs.

○ **CEPH** avec le plugin CEPH-CSI est la **solution de stockage persistant** pour les **infrastructures K8S** du système d'information AP-HP

- Le volume persistant | PV

○ La demande de création d'un 'PV' passe exclusivement par un 'PVC | Persistent Volume Claims'. Cet objet K8S permet s'assurer le découplage de l'application déployée de l'infrastructure de stockage, facilitant ainsi la portabilité de l'application entre de multiples infrastructure K8S.

○ Lors de la création d'un volume persistant, l'option de réclamation des données du volume est à positionner obligatoirement sur 'RETAIN', i.e. la suppression physique des données portées par le solution de stockage n'est pas automatiquement déclanchée lors de la destruction de l'objet 'PVC' Kubernetes quelque soit la manière de suppression de cet objet.

I Il est strictement interdit de créer un volume persistant avec l'option de réclamation des données du volume, positionnée à 'DELETE'.

II.4. LES SYSTEMES D'EXPLOITATION

4.1. CHOIX DES SYSTEMES D'EXPLOITATION

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

- ⇒ 'Linux'
- ⇒ 'Windows Serveur'

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 **Red Hat Entreprise**.

R Dans le cas où **une application** est **compatible** avec **les deux 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

I Il est **interdit de déployer** le système d'opération **Unix HP/UX** pour la mise en place de toute nouvelle solution au sein du SI AP-HP.

4.2. MISE A 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 Red Hat Entreprise Linux : Red Hat 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)

III. LE STOCKAGE

III.1. 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.
- ⇒ Les données générées par la sauvegarde des données se trouvant sur le stockage primaire. Ces données sont stockées sur du stockage dit secondaire.

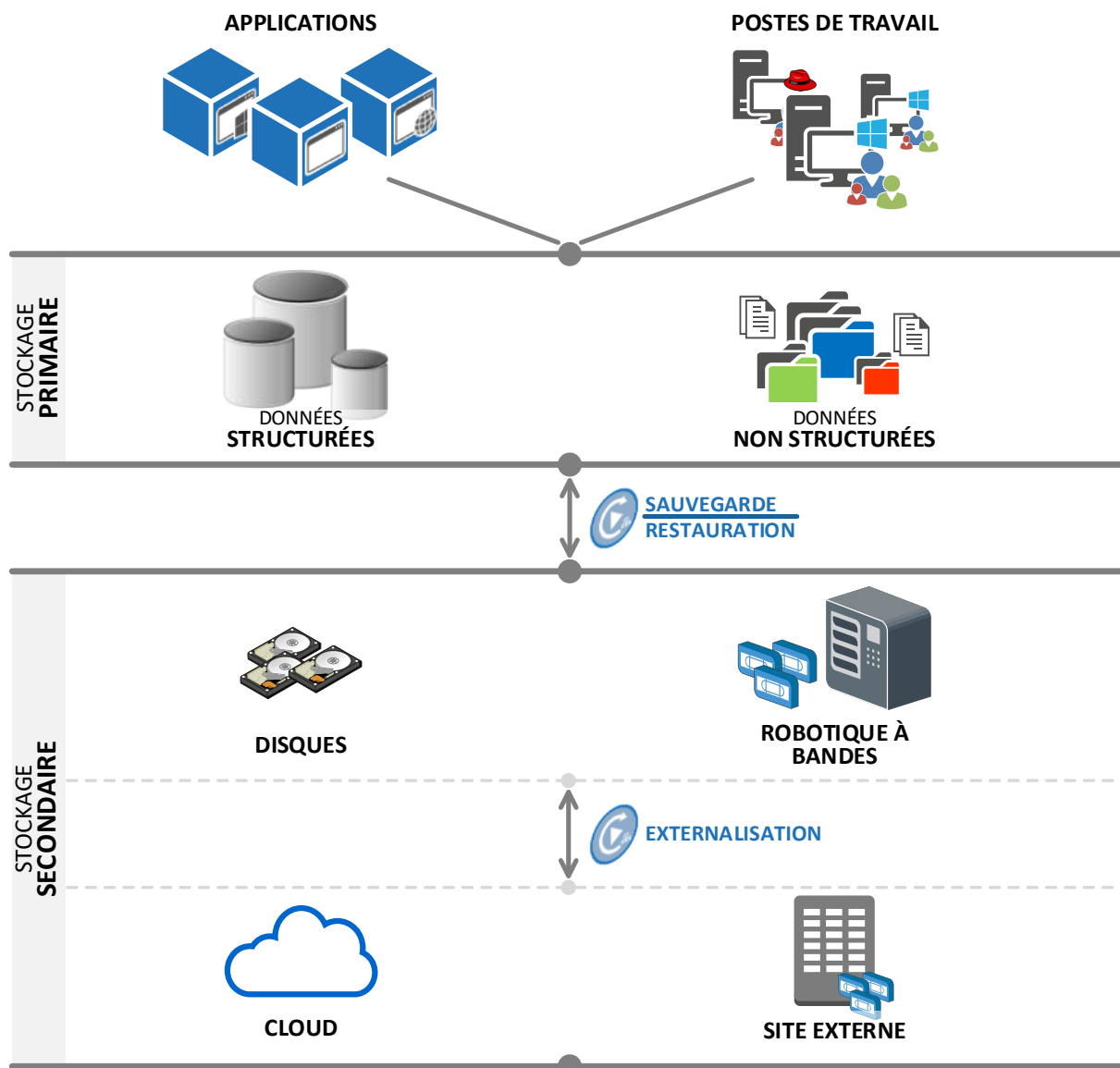


Figure 29 - Catégories de stockage

III.2. LE STOCKAGE PRIMAIRE

2.1. LE STOCKAGE DES SYSTEMES

- 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 des infrastructures serveur physique.

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

2.2. LE STOCKAGE DES DONNEES

a) REGLES GENERALES

- 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) RESEAU DE STOCKAGE SAN

- O** Dans le cas de LUN (Logical Unit Number) 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 répartis sur les deux datacenters.

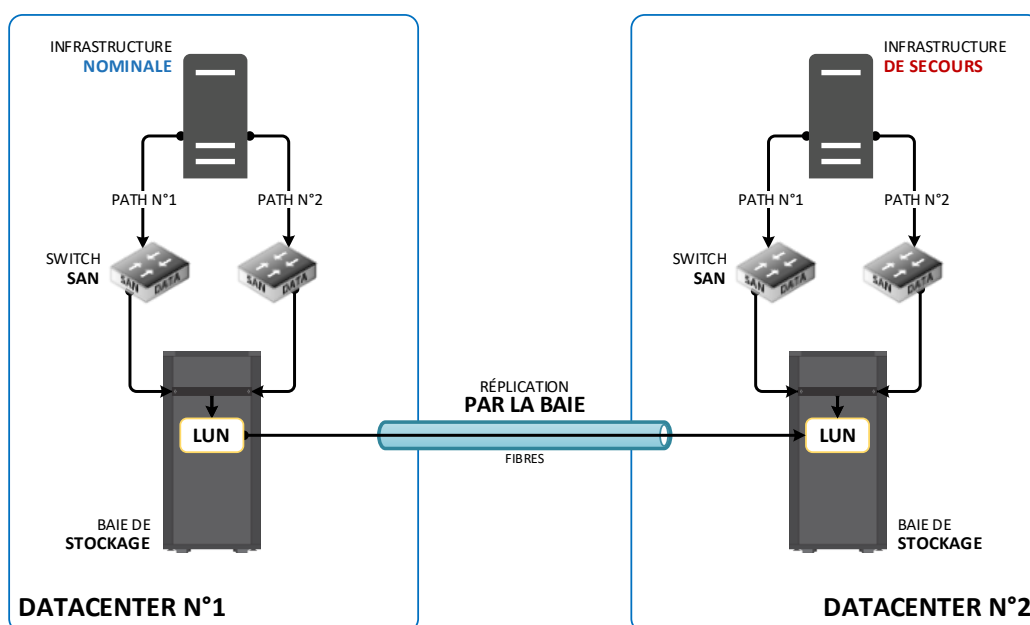


Figure 30 - Multipathing SAN

2.3. 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 termes 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 termes d'IOPS doivent privilégier des infrastructures de stockage à base de disques SATA.

III.3. LE STOCKAGE SECONDAIRE

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 : **'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)

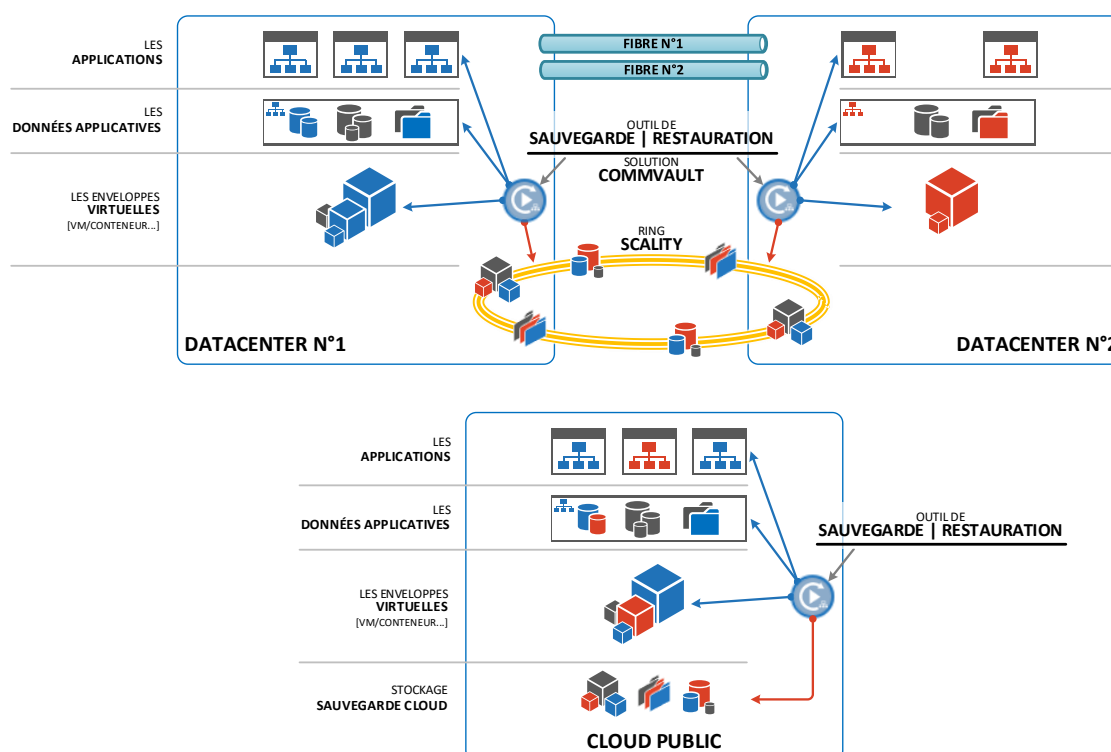


Figure 31 - Utilisation du stockage secondaire

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)

IV. LES HEBERGEMENTS

IV.1. HEBERGEMENT PROPRE

1.1. STRATEGIE D'HEBERGEMENT

- 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.

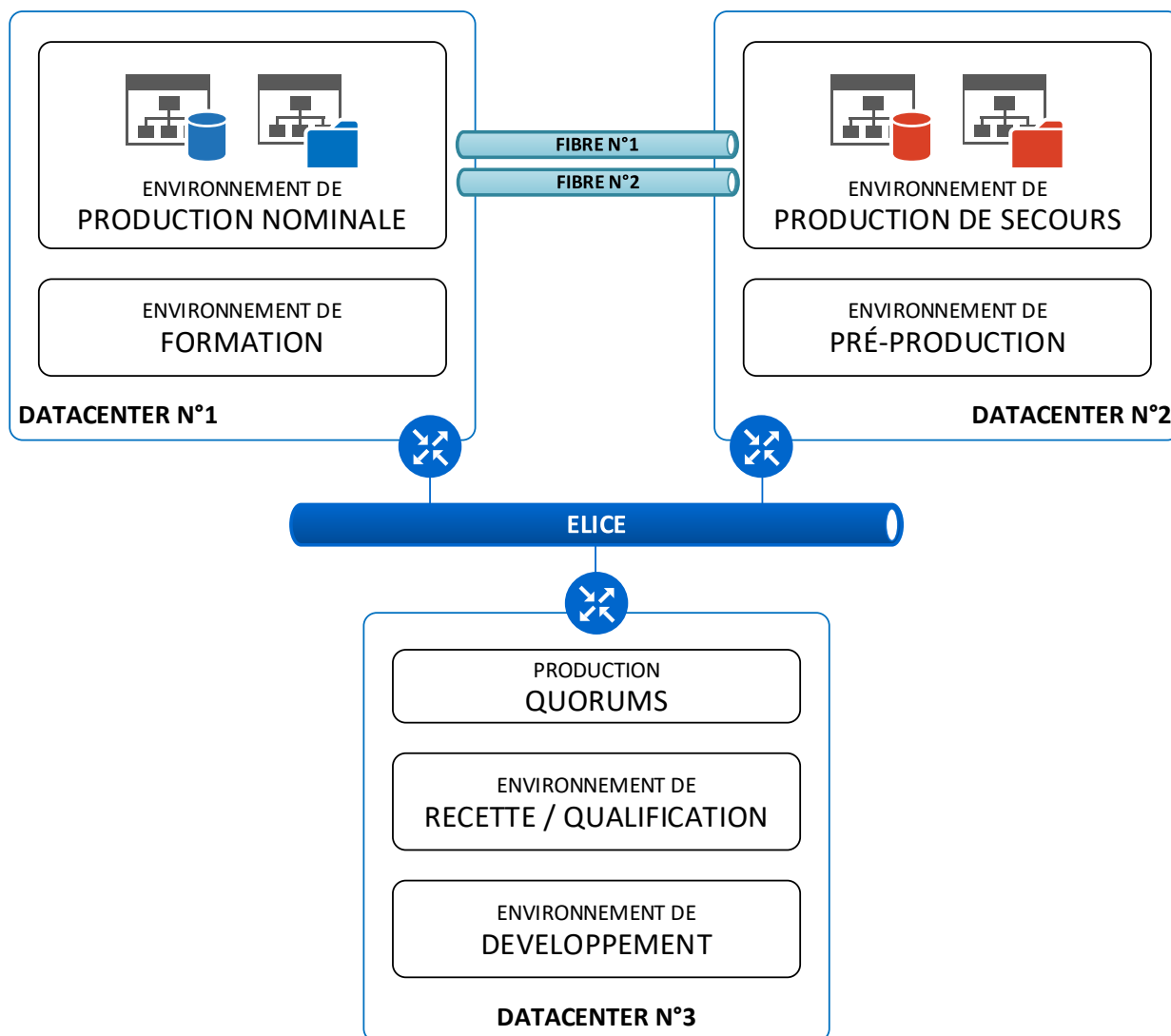


Figure 32 - Stratégie d'hébergement

- 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

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

O Les infrastructures portant les environnements de formation doivent être hébergées dans le même datacenter que celui hébergeant les infrastructures portant les environnements de production nominale.

O Les infrastructures portant les environnements de pré-production doivent être hébergées dans le même datacenter que celui hébergeant les infrastructures portant les environnements de production de secours.

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.

IV.2. CLOUD PRIVE

Les règles associées à l'hébergement **Cloud Privé** sont en cours d'étude au sein de la DSN AP-HP. En attendant une contextualisation, les recommandations sont les suivantes:

R Bien que les datacenters privés, tels que nos datacenters (Clichy, La Chapelle et Bicêtre) et les clouds privés, diffèrent en flexibilité, gestion et modèles de services, ils se rapprochent en termes d'isolation et de contrôle.

Il est donc recommandé, dans un premier temps, de respecter l'ensemble des règles décrites dans ce document pour toutes les solutions déployées dans un cloud privé.

IV.3. CLOUD PUBLIC

3.1. REGLES GENERALES

O Seul un **Cloud Public** étant officiellement reconnu comme **Hébergeur de Données de Santé** (certification HDS), et disposant de la certification '**SECNUMCLOUD**' délivrée par l'ANSSI, i.e. **souverain** dont les données sont stockées et traitées dans des centres de données localisés en France ou en Europe, et soumis exclusivement aux lois françaises ou européennes **sans être soumis à des lois extraterritoriales**, peut être utilisé pour **héberger une solution informatique de l'AP-HP manipulant des données de santé**.

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 et/ou Privé quel qu'il soit**.

3.2. ARCHITECTURE

O L'**architecture** à mettre en œuvre est de type '**HUB**' (zone centrale) & '**SPOKE**' (zone satellite) :

- ⇒ Une **zone centrale** 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.
- ⇒ La **zone satellite** 'SPOKE' rassemblant l'ensemble des composants d'**une solution applicative**.

O **Chaque nouvelle application** déployée dans le **Cloud Public** fait l'objet de la définition d'une nouvelle zone satellite 'SPOKE'.

- O** Cette architecture doit se décliner selon les environnements :
- ⇒ Une architecture 'HUB' (zone centrale) & 'SPOKE' (zone satellite) de production.
 - ⇒ Une architecture 'HUB' (zone centrale) & 'SPOKE' (zone satellite) de pré-production.
 - ⇒ Une architecture 'HUB' (zone centrale) & 'SPOKE' (zone satellite) de qualification.
- Et ainsi de suite pour tout nouvel environnement.

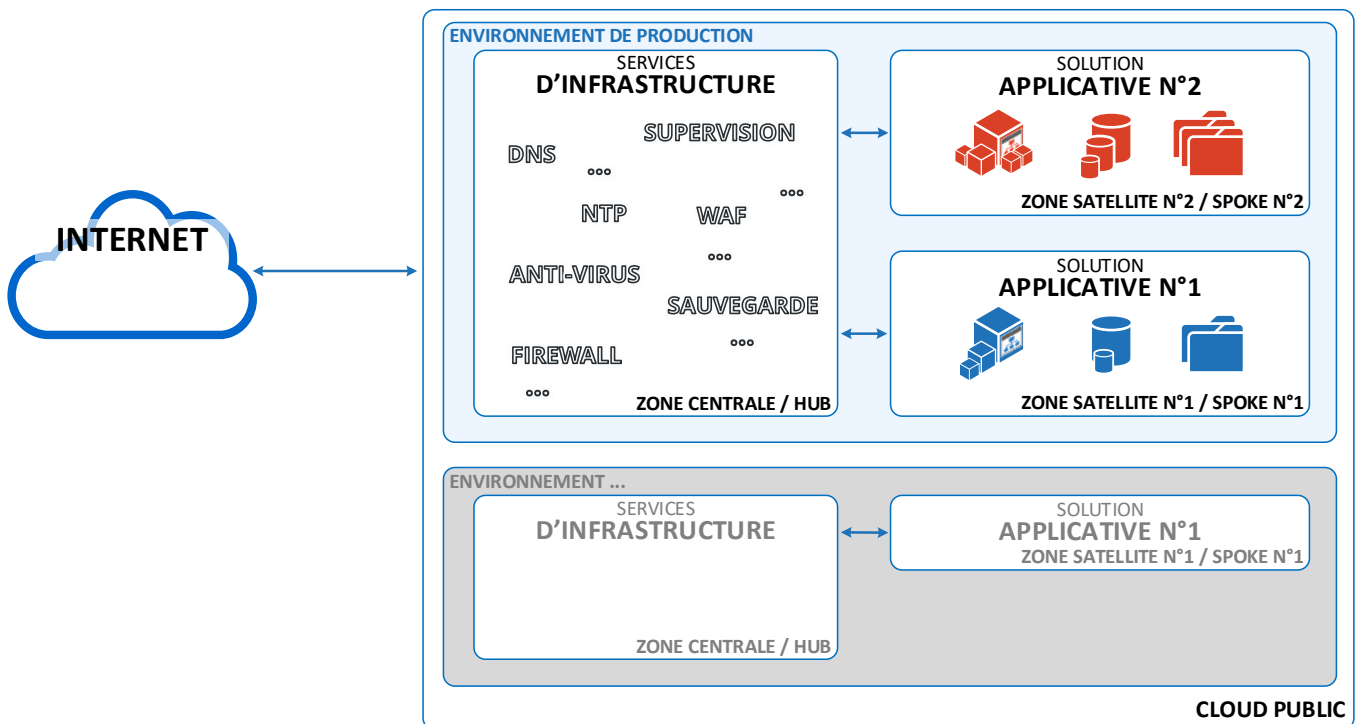


Figure 33 - Cloud public Architecture Hub & Spoke

- 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'infrastructures dans le Cloud Public utilisé pour minimiser le nombre de flux de communication entre ce Cloud Public et le SI de l'AP-HP.

V. 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.

V.1. MATERIEL

1.1. 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).

1.2. POSTES MOBILES

- R** Il est recommandé de privilégier le déploiement d'ordinateur portable plutôt que de tablette pour les situations nécessitant de la mobilité.

- R** 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.

V.2. SYSTEME

- O** Le système d'exploitation de tout nouveau poste de travail de type portable est Microsoft Windows 10.

- O** Tout nouveau poste de travail doit être intégré à l'outil de gestion de parc Microsoft SCCM.

V.3. SECURITE

- O** Tous les **postes de travail** doivent être **protégés** par la **solution anti-virus** de l'AP-HP : **Cortex XDR**.

- O** Tout nouveau poste de travail doit être intégré à l'outil de gestion des mises à jour Microsoft SCCM.

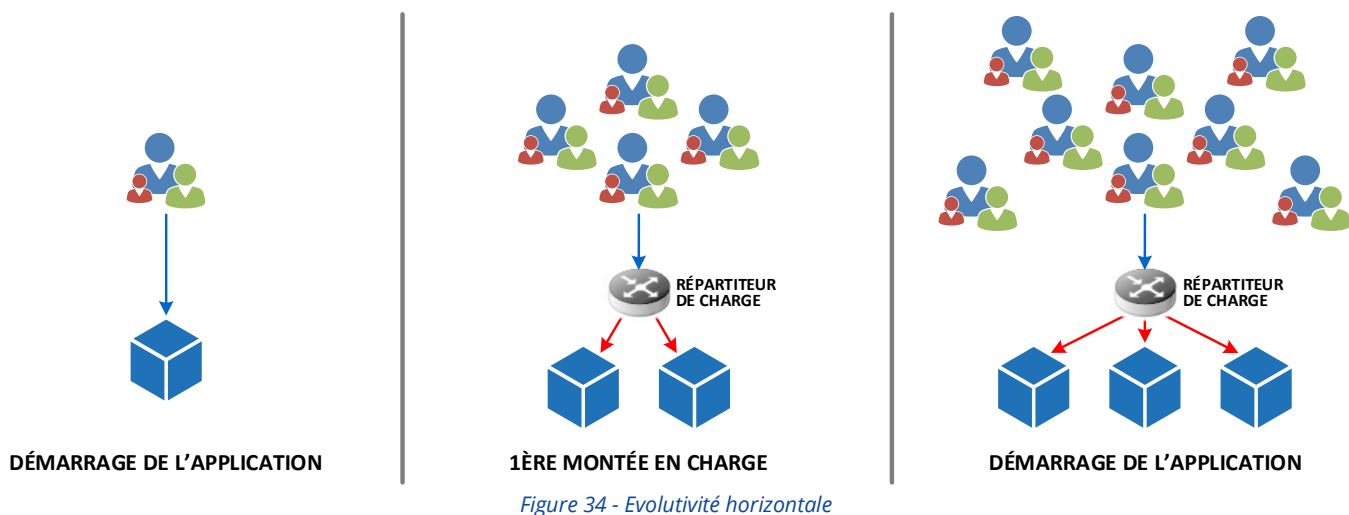
V.4. LOGICIELS

- 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.
 - ⇒ Microsoft Edge.
 - ⇒ LAPS UI.
 - ⇒ Framework .Net.
 - ⇒ Citrix Receiver.
 - ⇒ Cortex XDR.

VI. LES SERVICES D'INFRASTRUCTURE

VI.1. LA REPARTITION DE CHARGE

- Les applications conçues ou à déployer dans le SI de l'AP-HP, pour lesquelles un volume élevé de connexions simultanées est anticipé en raison de l'activité des utilisateurs, doivent être capables de s'adapter horizontalement. Cela signifie qu'elles doivent pouvoir répartir cette charge sur plusieurs instances identiques de leurs composants, sans affecter l'expérience utilisateur (sans perte de contexte).



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

- 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).

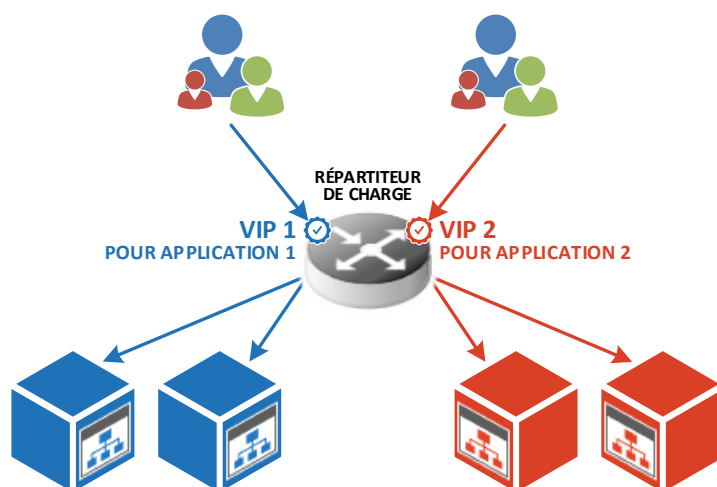


Figure 35 - Gestion des VIP (I)

- O Une VIP est affectée à un et un seul service.

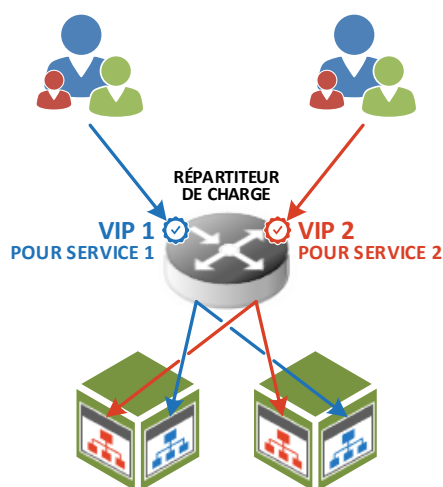


Figure 36 - Gestion des VIP (II)

- O La répartition de charge des flux métiers doit être faite par la solution '**ADC**' (Application Delivery Controller). La solution adoptée par l'AP-HP est la solution '**RADWARE Alteon**'. (Voir les fonctionnalités de l'ADC : Passerelle web d'interconnexion filtrée p.17 et Gestion des flux web utilisateurs vers une application interne p.27)

- R La solution de répartition de charge '**NGINX**' est tolérée dans des cas d'usage non couvert 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.

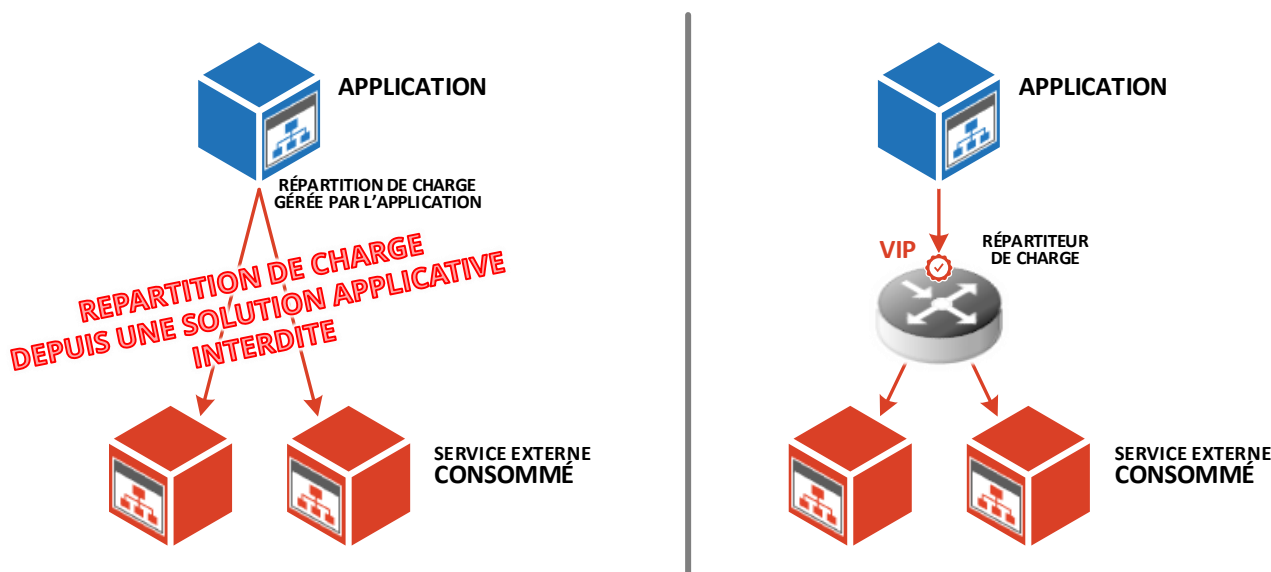


Figure 37 - Consommation d'un service redondé

VI.2. LA HAUTE DISPONIBILITE

2.1. CONCEPTS

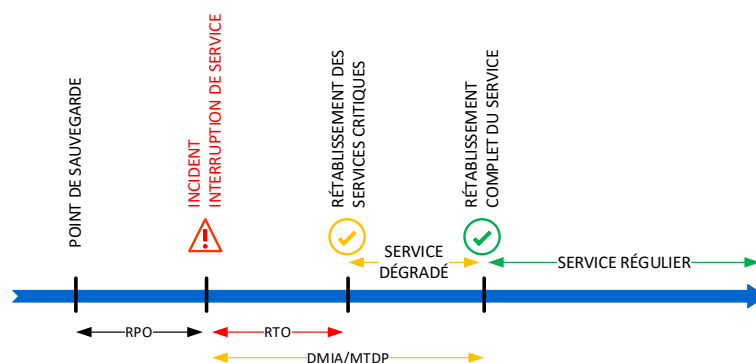


Figure 38 - Principes RPO / RTO

Les solutions de haute-disponibilité (HA) à mettre en œuvre doivent s'appuyer sur trois indicateurs (Voir la norme ISO 22301) :

- ⇒ Le **RPO** (Recovery Point Objective) désigne, en cas d'incident sur une application, le moment auquel les données doivent être restaurées une fois l'incident résolu. Cet indicateur définit le délai maximal acceptable entre l'incident et le dernier point de sauvegarde des données, c'est-à-dire la quantité de données que l'on peut se permettre de perdre.
- ⇒ Le **RTO** (Recovery Time Objective) correspond au temps maximum pendant lequel une application peut être indisponible après un incident, jusqu'à ce qu'elle soit rétablie en mode dégradé. Cet indicateur fixe donc le délai dans lequel une reprise partielle des opérations doit être possible.
- ⇒ La **DMIA/MTDP** (Maximum Tolerable Period of Disruption) représente le temps maximal pendant lequel une application peut rester indisponible après un incident, jusqu'à son rétablissement complet en mode nominal, assurant ainsi une reprise totale des activités. Cette indicateur marque le délai critique au-delà duquel une reprise complète est nécessaire pour éviter des conséquences graves ou irréversibles.

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.

2.2. REGLES GENERALES

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 ne sera mise en place.

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

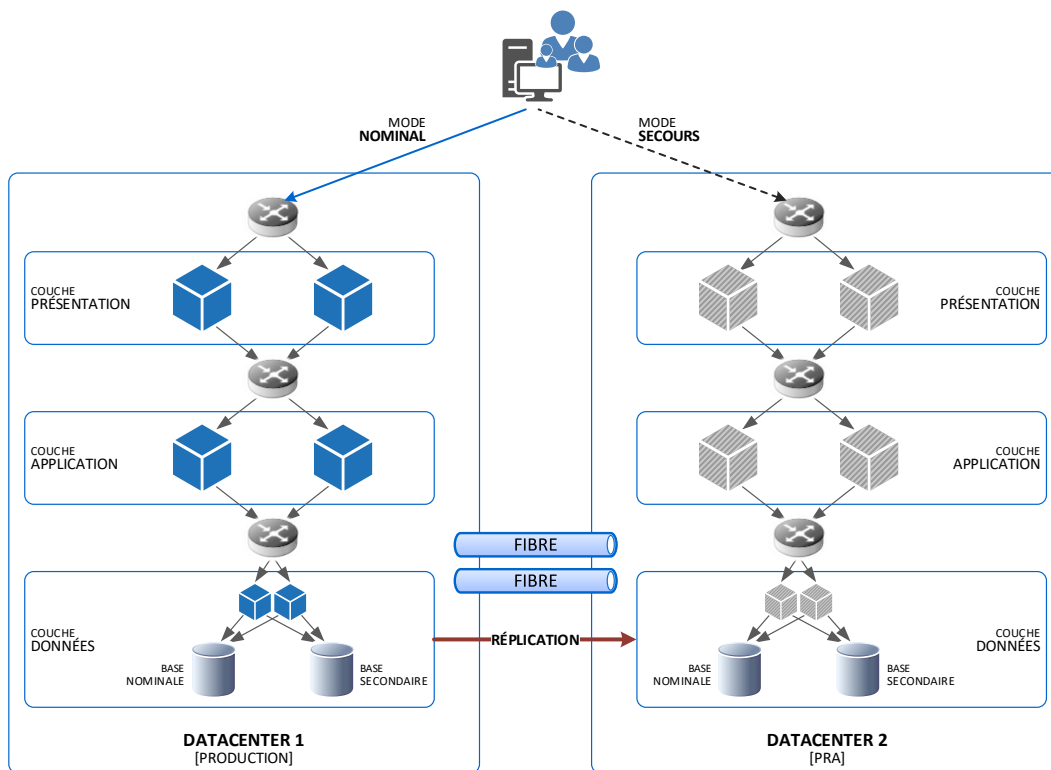


Figure 39 - Haute-disponibilité (I)

I Il est interdit de basculer partiellement vers le 'datacenter' de secours une application en architecture trois tiers traditionnelle (présentation/application/base de données) qui bénéficie d'une haute disponibilité afin d'éviter les flux inter-datacenters et de mieux maîtriser les échanges entre les deux 'datacenters' principaux.

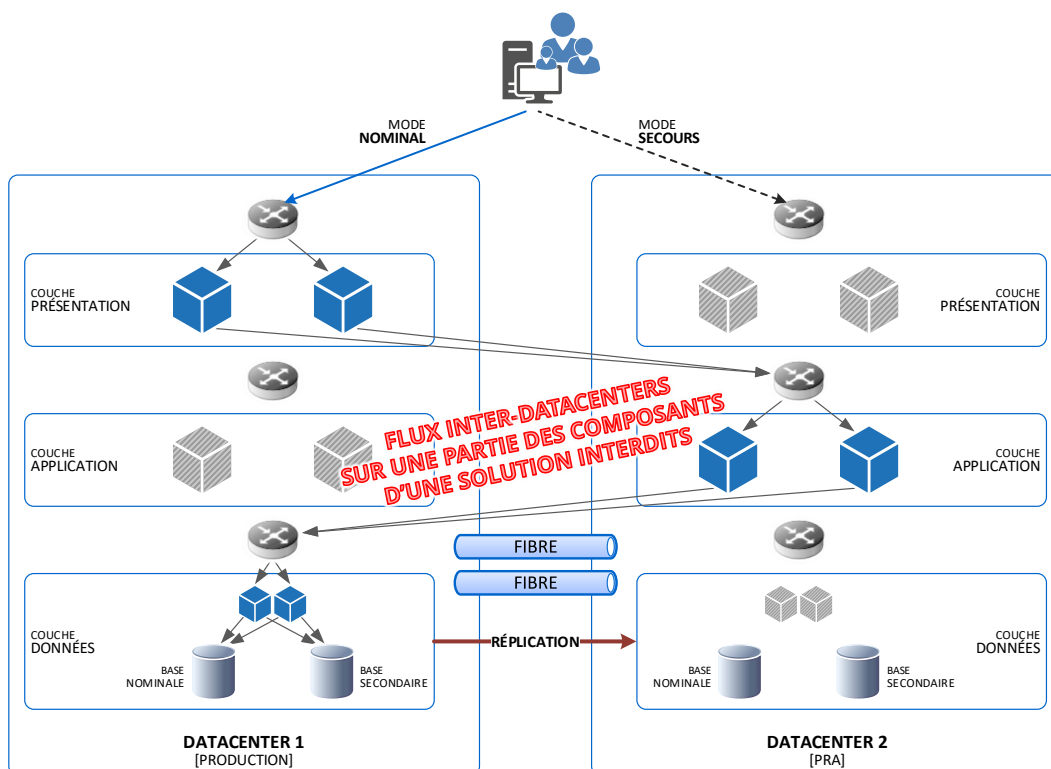


Figure 40 - Haute disponibilité (II)

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

O La mise en place de l'ensemble des composants d'un cluster est :
⇒ Soit effectuée sur le même datacenter de production nominal (cluster HA en mode ACTIF/PASSIF ou en mode ACTIF/ACTIF).
⇒ Soit distribuée sur les deux datacenters principaux (cluster PRA en mode ACTIF/PASSIF). Dans ce cas précis, la décision du basculement ACTIF/PASSIF doit exclusivement provenir d'une décision humaine, i.e. que le basculement ne peut pas être initié par un quelconque automate.
Le service de surveillance du cluster 'Quorum' doit être installé sur le 3^{ème} datacenter.

R Les solutions de clustering recommandées sont :
⇒ Pacemaker / Corosync pour les environnements Linux
⇒ PGPOOL pour une base de données PostgreSQL
⇒ Safekit pour les solutions IAM
⇒ Safeguard pour les environnements HP-UX

VI.3. L'AUTHENTIFICATION

3.1. 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

O La délégation de l'authentification à Active Directory doit se faire :
⇒ Soit par un bind LDAPS
⇒ Soit par l'utilisation, par ordre priorité, d'un web service mis à disposition par l'AP-HP

- Accessible en REST API
- Accessible en SOAP

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 SAMLv2)

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.

3.2. AUTHENTIFICATION MULTI-FACTEURS/MFA

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

B. LES SERVICES APPLICATIFS

I. LES BASES DE DONNEES

I.1. 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.

I Le déploiement de nouveaux services de base de donnée Oracle (nouveau schéma, nouvelle instance, nouveau serveur, etc.) ne sont plus autorisés dans le système d'information de l'AP-HP.

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

- ⇒ Red Hat Entreprise Linux
- ⇒ Microsoft Windows Serveur

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

- ⇒ SGBD open source
 - PostgreSQL
 - MySQL ou MariaDB
- ⇒ SGBD propriétaire
 - Microsoft SQL Server

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.

I.2. 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

2.1. LES BASES DE DONNEES ORIENTEES DOCUMENT

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

Usages : 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**'

2.2. LES BASES DE DONNEES CLE/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 simples.

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

- R** Les bases de données NoSQL à clé/valeur recommandées sont :
- ⇒ **'REDIS'**
 - ⇒ **'ETCD'**

2.3. 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.

Usages : 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** Les bases recommandées sont :
- ⇒ **'HBase (Hadoop DB)'**
 - ⇒ **'Cassandra'**

2.4. LES BASES ORIENTEES 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.

1.3. LA REPLICATION DES DONNEES

- 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'**
 - ⇒ **'MySQL'** ou **'MariaDB'**
 - ⇒ **'Microsoft SQL Server'**

- R** 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
 - ⇒ MySQL ou MariaDB : réplication des binary logs
 - ⇒ Pour Microsoft SQL Server : Always On

II. LES ECHANGES 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 et la sécurité de ses échanges inter-applicatif l'AP-HP a mis en place des solutions de management des flux. L'ensemble des solutions technique de management des flux est référencé dans ce document sous le terme '**Socle Technique - Transport de la Donnée**'.

Note : Cet ensemble '**Socle Technique - Transport de la Donnée**' sera représenté dans les schémas de topologie des flux ci-après par l'élément graphique suivant :

SOCLE TECHNIQUE
TRANSPORT DE
LA DONNÉE

II.1. LES SOLUTIONS DE GESTION DES FLUX

1.1. EAI - CENTRAL

La **solution** d'intégration **EAI** est entièrement **développée par l'AP-HP**. La solution implémente plusieurs types de services, dont le traitement par lots et le traitement au fil de l'eau. Ces traitements peuvent inclure 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.

1.2. EAI - ETABLISSEMENT

La solution EAI établissement est la **solution MIRTH**. MIRTH est une plateforme d'intégration open source utilisée principalement dans le domaine de la santé. MIRTH est utilisée au sein des établissements pour l'intégration des flux inter-applicatifs locaux et comme point de communication avec le système d'échange central.

1.3. API MANAGEMENT

L'API Management est une solution permettant de gérer les flux reposant sur les API REST. La **solution d'APIM** du système d'information de l'AP-HP est la solution **GRAVITEE**.

1.4. REGLES GENERALES

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-applicatif **doit transiter** par l'une des **solutions de gestion des flux** du système d'information de l'AP-HP :

- ⇒ **EAI Central.**
- ⇒ **EAI Etablissement**
- ⇒ **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.

- O 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

II.2. MODELES DE FLUX INTER-APPLICATIF INTERNE

2.1. SI CENTRAL → SI CENTRAL

- I Aucun échange métier (synchrone ou asynchrone) inter-applicatif entre deux applications de la zone DATACENTER n'est autorisé directement.



Figure 41 - Flux inter-applicatifs - Topologie SI → SI interdite

- O Tout échange inter-applicatifs entre deux solution déployées dans la zone DATACENTER doit transiter par le socle technique 'transport de la donnée'.

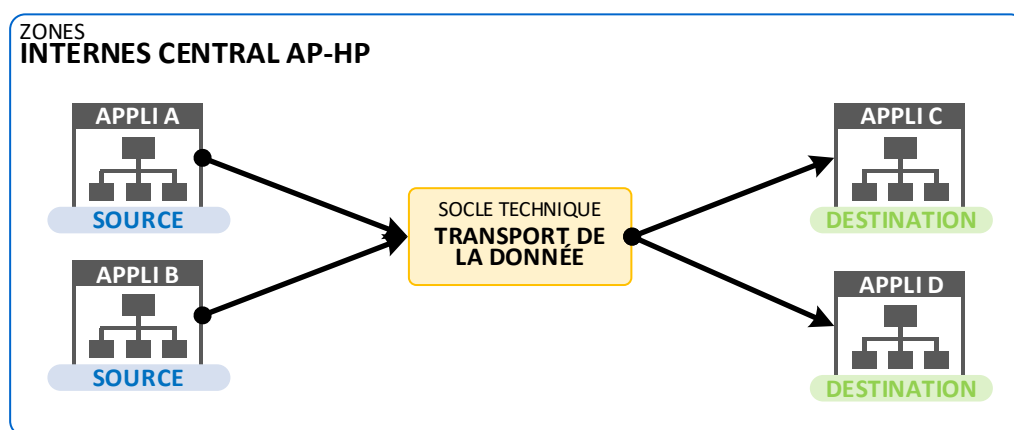


Figure 42 - Flux inter-applicatifs - Topologie SI → SI obligatoire

2.2. SI CENTRAL ↔ SI GHU

I Aucun échange métier (synchrone ou asynchrone) inter-applicatif entre une application de la zone DATACENTER et une application de la zone GH (étendue ou non étendue), ou le socle technique de transport de la donnée de cette même zone GH, n'est autorisé directement.

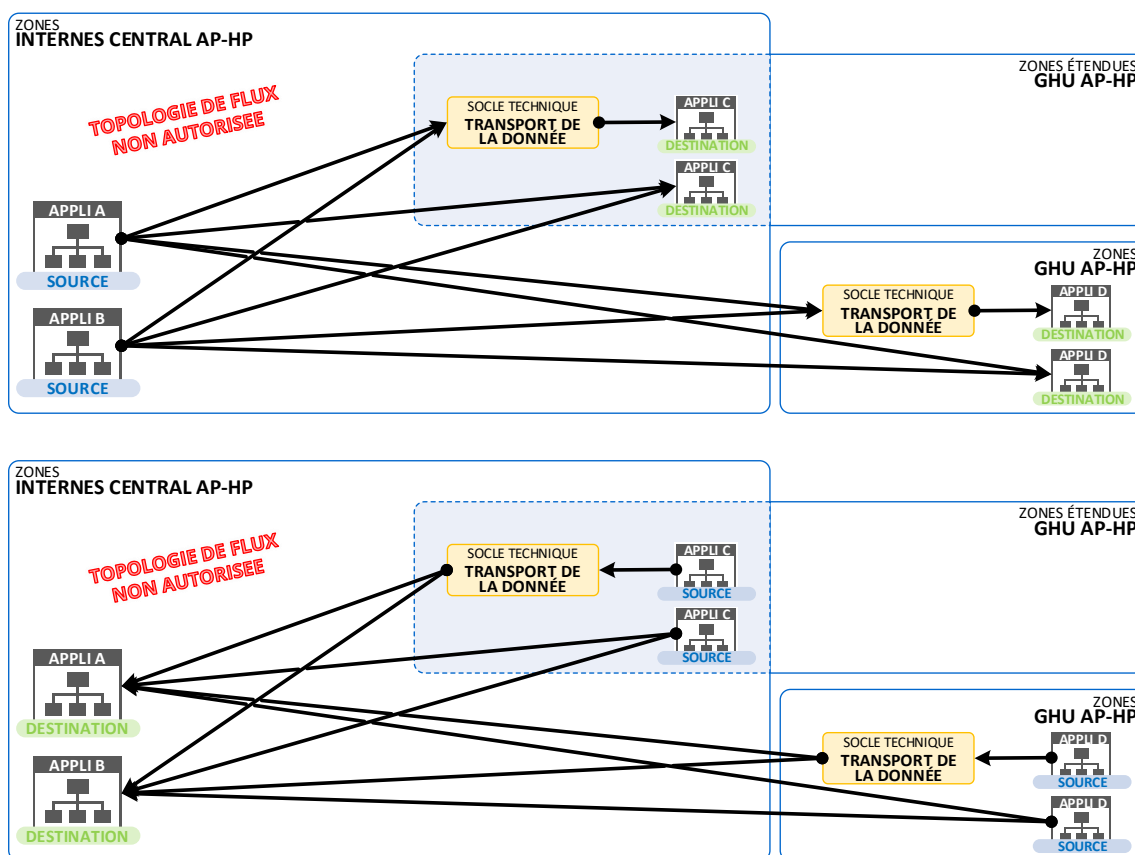
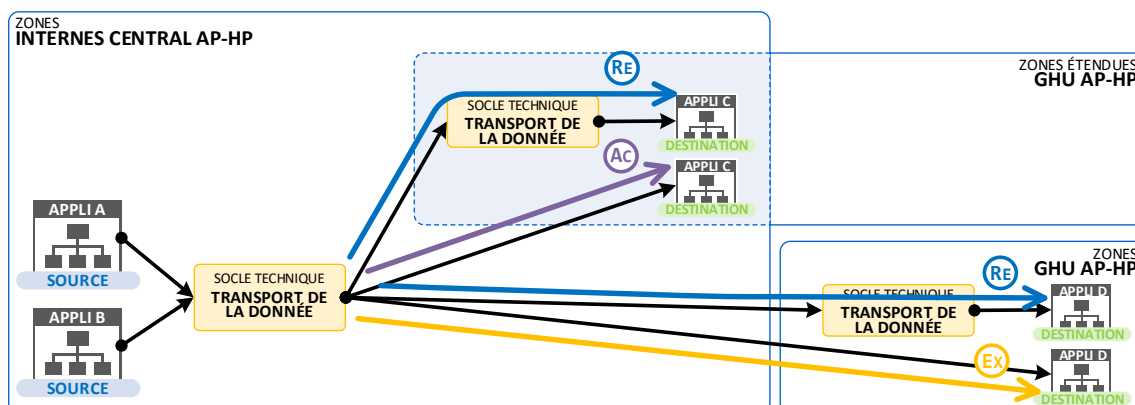


Figure 43 - Flux inter-applicatifs - Topologie SI ↔ GHU interdite

O Tout échange métier (synchrone ou asynchrone) inter-applicatifs entre une application de la zone DATACENTER et une application de la zone GH (étendue ou non étendue) doit transiter par le socle technique 'transport de la donnée' central.

3 topologies sont à suivre dans l'ordre de préférence suivant :

- ⇒ Flux **RE**commandé
- ⇒ Flux **AC**ceptable
- ⇒ Flux **EX**ceptionnel



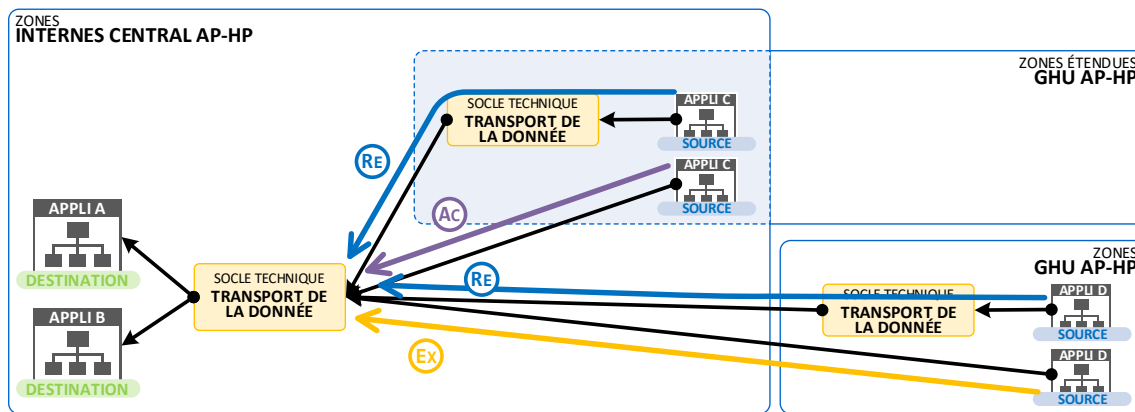


Figure 44 - Flux inter-applicatifs - Topologie SI ↔ GHU obligatoire

2.3. SI CENTRAL ↔ SI CLOUD PRIVE

I Aucun échange métier (synchrone ou asynchrone) inter-applicatif entre une applications de la zone DATACENTER et une application d'une zone CLOUD PRIVE, ou le socle technique de 'transport de la donnée' de cette même zone CLOUD PRIVE, n'est autorisé directement.

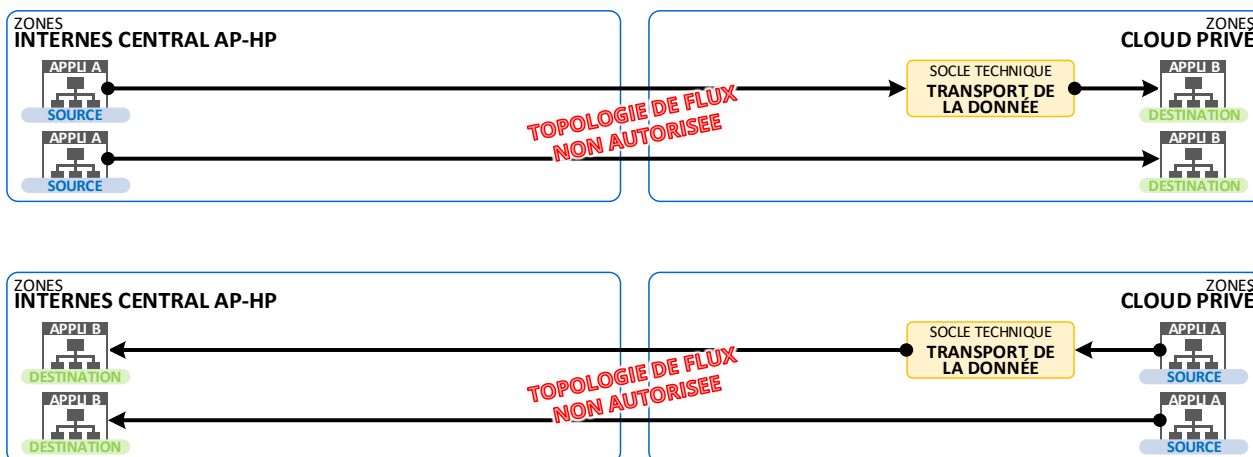
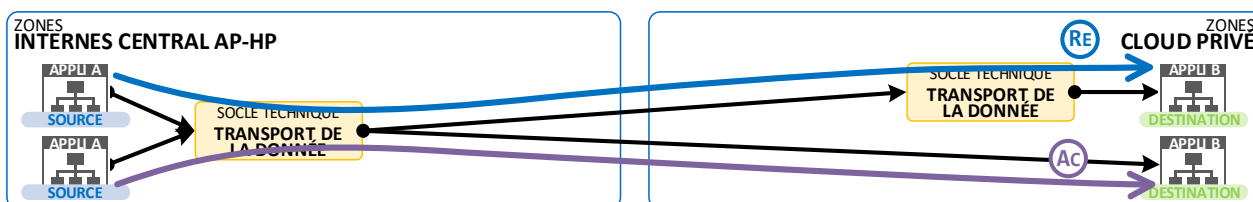


Figure 45 - Flux inter-applicatifs - Topologie SI ↔ CLOUD PRIVE interdite

O Tout échange métier (synchrone ou asynchrone) inter-applicatif entre une application d'une zone DATACENTER et une application d'une zone CLOUD PRIVÉ doit transiter par le socle technique 'transport de la donnée' central et local au cloud privé.

2 topologies sont à suivre dans l'ordre de préférence suivant :

- ⇒ Flux **RE**commandé
- ⇒ Flux **AC**ceptable



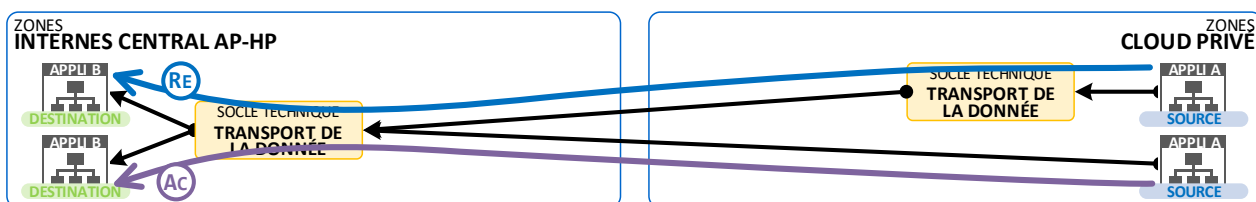


Figure 46 - Flux inter-applicatifs - Topologie SI ↔ CLOUD PRIVE obligatoire

2.4. SI GHU ↔ SI GHU

I Aucun échange métier (synchrone ou asynchrone) inter-applicatif entre une application d'une zone GH (étendue ou non étendue) et une autre application d'une zone GH (identique ou non, étendue ou non étendue) n'est autorisé directement.

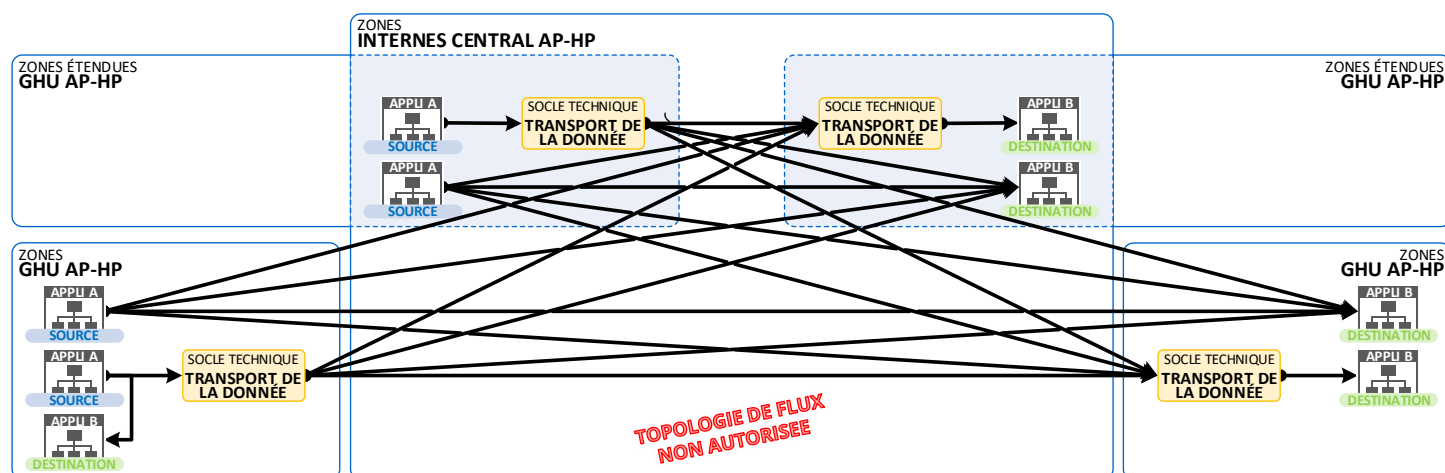


Figure 47 - Flux inter-applicatifs - Topologie GHU ↔ GHU interdite

O Tout échange métier (synchrone ou asynchrone) inter-applicatif entre une application d'une zone GH (étendue ou non étendue) et une autre application d'une zone GH (identique ou non, étendue ou non étendue) doit transiter par le socle technique 'transport de la donnée', tant au niveau local que central.

3 topologies sont à suivre dans l'ordre de préférence suivant :

- ⇒ Flux **RE**commandé
- ⇒ Flux **AC**ceptable
- ⇒ Flux **EX**ceptionnel

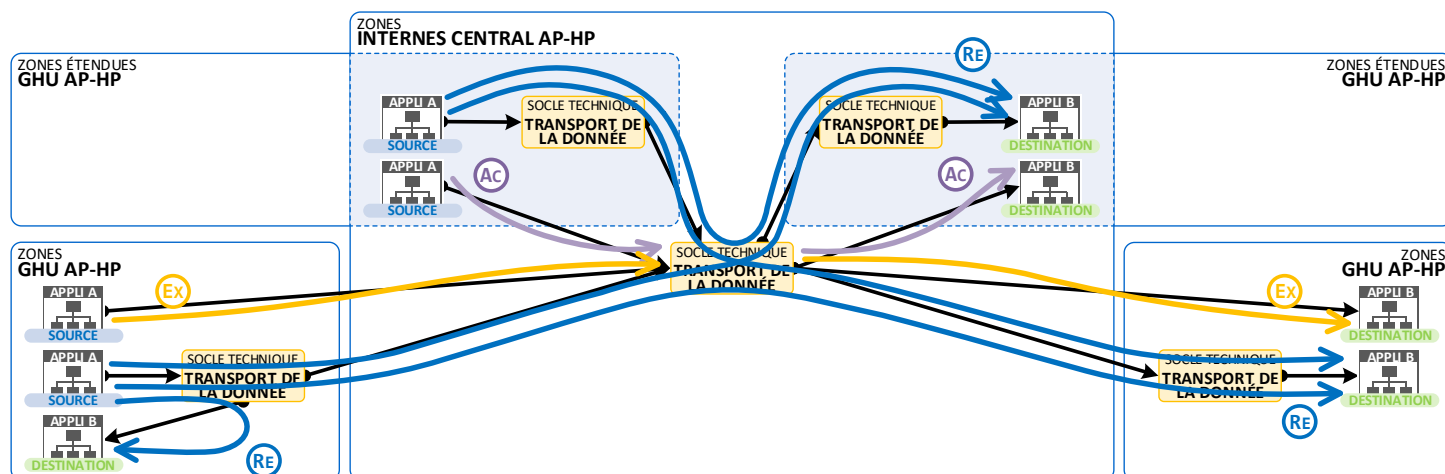


Figure 48 - Flux inter-applicatifs - Topologie GHU ↔ GHU obligatoire

II.3. MODELES DE FLUX INTER-APPLICATIF EXTERNE

3.1. SI CENTRAL ↔ APPLICATIF SAAS CLOUD

I Aucun échange métier (synchrone ou asynchrone) inter-applicatif entre une application de la zone DATACENTER et une application en SAAS CLOUD n'est autorisé, que cela soit directement ou en transitant par le socle technique de 'transport de la donnée' de la zone DMZ/INTERNET.

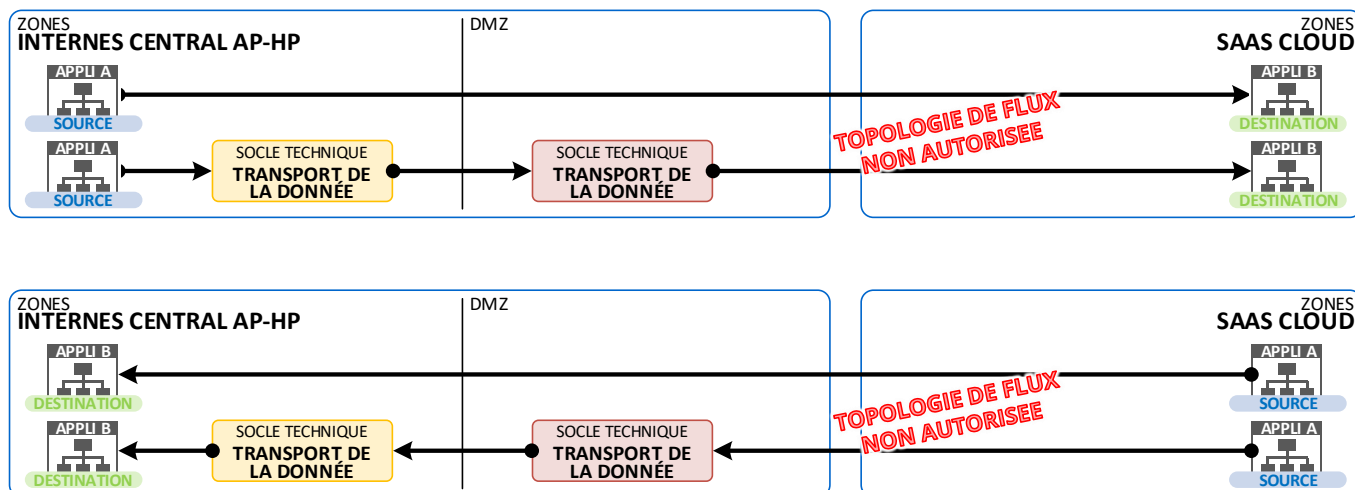


Figure 49 - Flux inter-applicatifs - Topologie SI↔CLOUD PRIVE interdite

Note : les composants techniques situés en DMZ ne sont plus autorisés.

O Tout échange métier (synchrone ou asynchrone) inter-applicatif entre une application de la zone DATACENTER et une application en SAAS CLOUD doit transiter par le socle technique 'transport de la donnée' central.

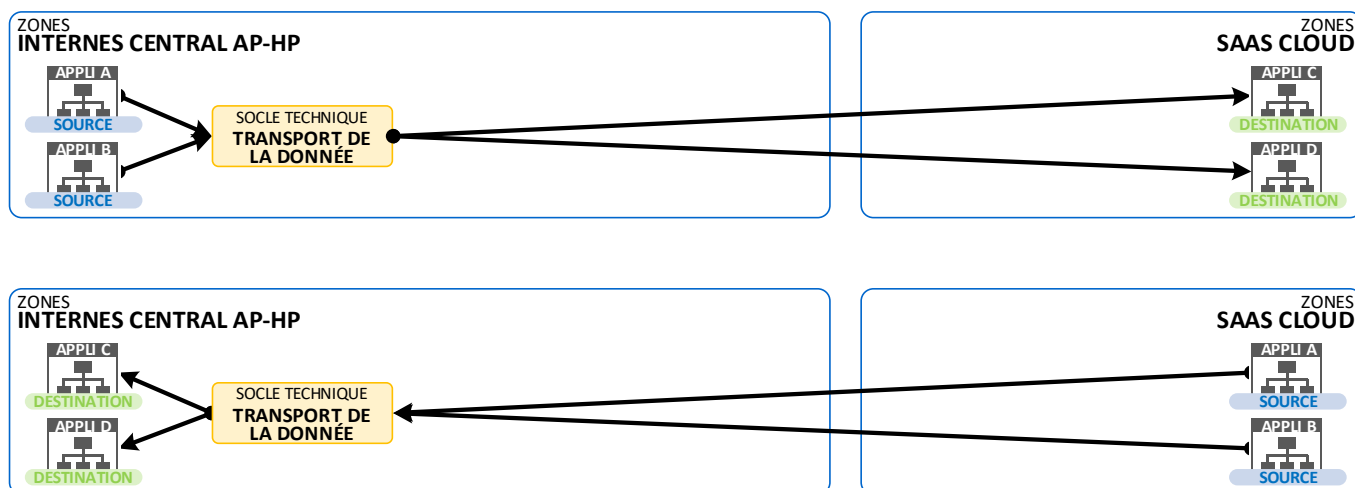


Figure 50 - Flux inter-applicatifs - Topologie SI↔CLOUD PRIVE obligatoire

3.2. SI GHU ↔ APPLICATIF SAAS CLOUD

I Aucun échange métier (synchrone ou asynchrone) inter-applicatif entre une application d'une zone GH (étendue ou non étendue) et une application en SAAS CLOUD n'est autorisé, que ce soit directement ou en transitant par le socle technique de 'transport de la donnée' de la zone DMZ/INTERNET.

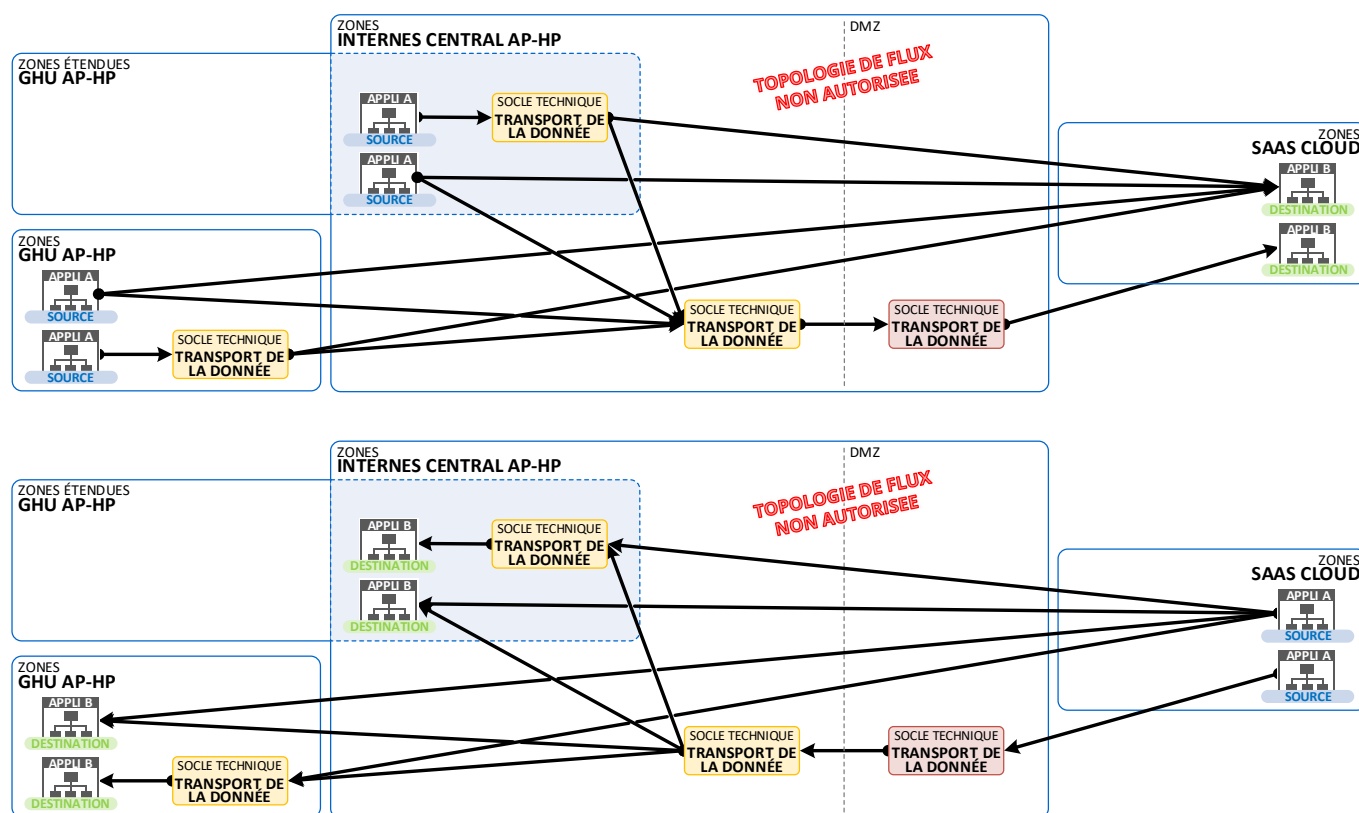


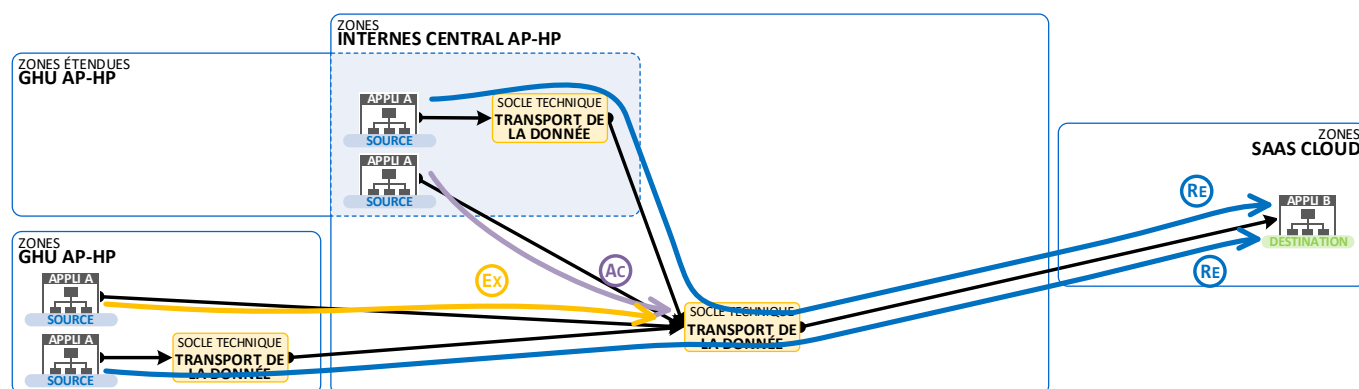
Figure 51 - Flux inter-applicatifs - Topologie GHU↔SAAS CLOUD interdit

Note : les composants techniques situés en DMZ ne sont plus autorisés.

O Tout échange métier (synchrone ou asynchrone) inter-applicatif entre une application d'une zone GH (étendue ou non étendue) et une application en SAAS CLOUD doit transiter par le socle technique 'transport de la donnée', tant au niveau local que central.

3 topologies sont à suivre dans l'ordre de préférence suivant :

- ⇒ Flux **RE**commandé
- ⇒ Flux **AC**ceptable
- ⇒ Flux **EX**ceptionnel



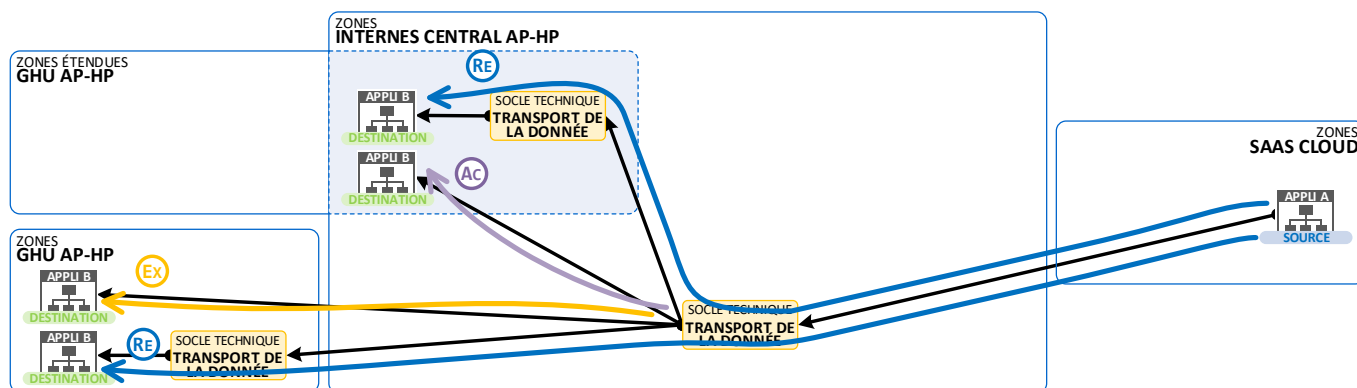


Figure 52 - Flux inter-applicatifs - Topologie GHU↔SAAS CLOUD

3.3. PUBLIC → SI CENTRAL

I Aucun échange métier (synchrone ou asynchrone) inter-applicatif entre une application de la zone PUBLIC INTERNET et une application de la zone DATACENTER n'est autorisé, que ce soit directement ou en transitant par le socle technique de 'transport de la donnée' de la zone DMZ/INTERNET.

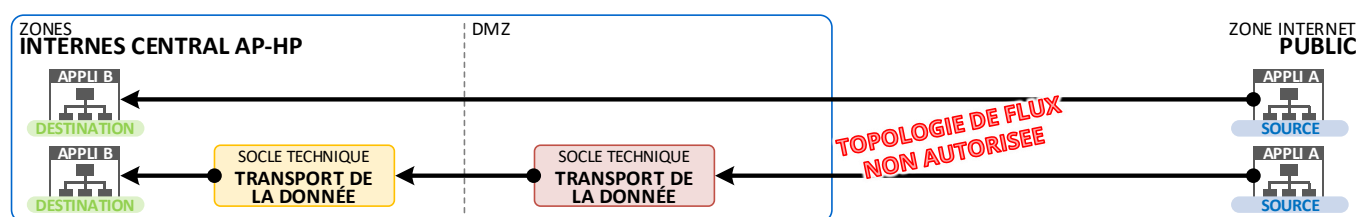


Figure 53 - Flux inter-applicatifs - Topologie PUBLIC→SI interdit

Note : les composants techniques situés en DMZ ne sont plus autorisés.

O Tout échange métier (synchrone ou asynchrone) inter-applicatif entre une application de la zone PUBLIC INTERNET et une application de la zone DATACENTER doit transiter par le socle technique 'transport de la donnée' central.

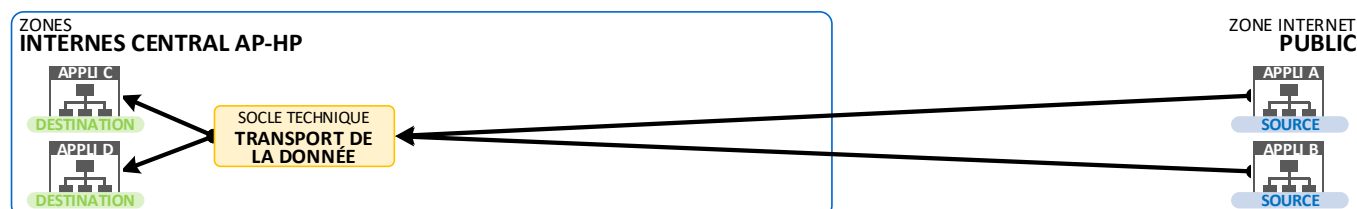


Figure 54 - Flux inter-applicatifs - Topologie PUBLIC→GHUI autorise

3.4. PUBLIC → SI GHU

I Aucun échange métier (synchrone ou asynchrone) inter-applicatif entre une application de la zone PUBLIC INTERNET et une application de la zone GH (étendue ou non étendue), ou le socle technique de transport de la donnée de cette même zone GH, n'est autorisé, que ce soit directement ou en transitant par le socle technique de 'transport de la donnée' de la zone DMZ/INTERNET.

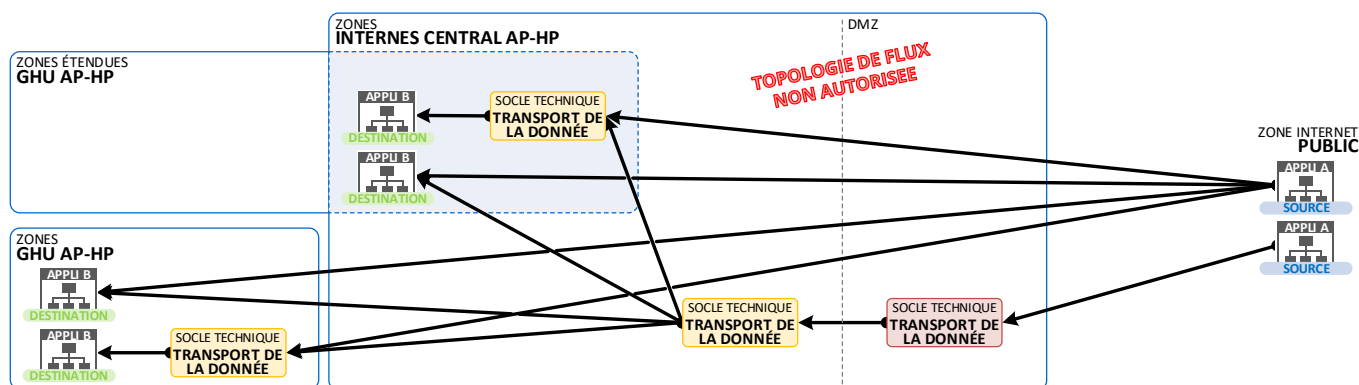


Figure 55 - Flux inter-applicatifs - Topologie PUBLIC→GHU interdit

Note : les composants techniques situés en DMZ ne sont plus autorisés.

- O** Tout échange métier (synchrone ou asynchrone) inter-applicatif entre une application de la zone PUBLIC INTERNET et une application d'une zone GH (étendue ou non étendue) doit transiter par le socle technique 'transport de la donnée', tant au niveau central, en entrée du système d'information de l'AP-HP, qu'au niveau local.
- 3 topologies sont à suivre dans l'ordre de préférence suivant :
- ⇒ Flux **RE**commandé
 - ⇒ Flux **AC**ceptable
 - ⇒ Flux **EX**ceptionnel

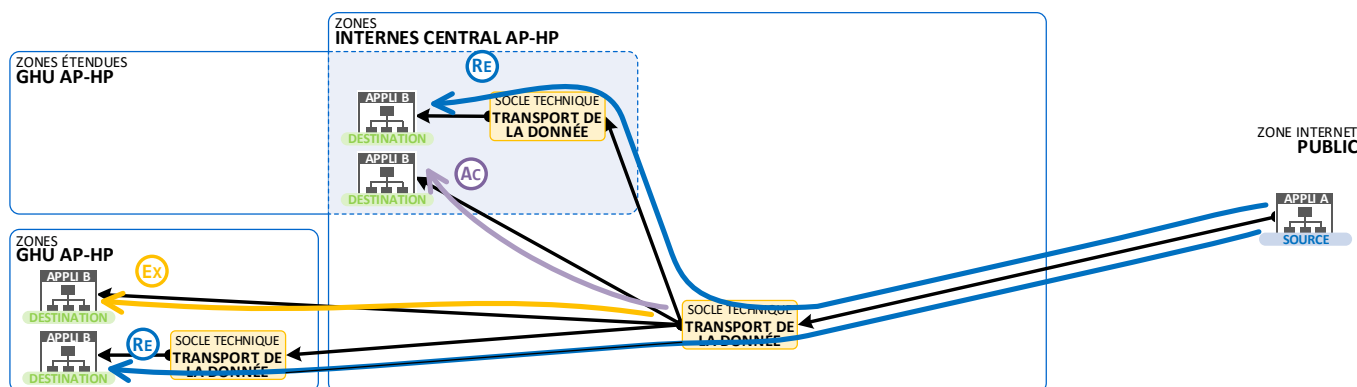


Figure 56 - Flux inter-applicatifs - Topologie PUBLIC→GHU autorisé

II.4. CHIFFREMENT DES ECHANGES

- O** Tous les échanges inter-applicatifs sortants du système d'information de l'AP-HP ou entrant dans le système d'information de l'AP-HP doivent être chiffrés.

O Tous les échanges inter-applicatifs au sein de la zone de sensibilité HDS (Hébergement de Données de Santé), ainsi que ceux qui en sortent ou y entrent dans le système d'information de l'AP-HP, doivent être chiffrés.

R Le chiffrement des flux est fortement recommandé pour des échanges inter-applicatifs ayant le même niveau de confidentialité autre que HDS.

II.5. PROTOCOLES D'ÉCHANGE

I Les protocoles, même s'ils sont 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

II.6. AUTHENTIFICATION DES ÉCHANGES

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

R Pour l'authentification par jeton, il est recommandé d'utiliser un jeton JSON Web Token (JWT).

II.7. FLUX D'ÉCHANGE INTERNE AU SI DE L'AP-HP

I L'utilisation du protocole JDBC directement depuis une application ou un EAI (Enterprise Application Integration) vers la base de données d'une autre application est interdite. Cette 'autre' application doit fournir un accès à ses données via une interface dédiée, telle qu'une API REST, qui respecte les règles d'intégrité et de sécurité.

I L'utilisation et la mise en œuvre de DBLINK pour connecter deux bases de données appartenant à des applications différentes sont interdites.

R Le protocole FTP, qu'il soit chiffré (FTPS, FTPES) 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 nécessite pas de sécurisation particulière du flux.

Liste des protocoles d'échange recommandés :

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

R 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) ainsi que des API pour échanger des données.

II.8. FLUX D'ÉCHANGE AVEC DES PARTENAIRES EXTERNES AU SI DE L'AP-HP

I Le protocole FTP, qu'il soit chiffré (FTPS, FTPES) ou non, est interdit pour les échanges entre une application externe au système d'information de l'AP-HP et une application interne au système d'information de l'AP-HP.

R Le protocole d'échange recommandé est :
⇒ HTTPS

II.9. LES FORMATS D'ÉCHANGE

R Les formats les plus couramment utilisés au sein du système d'information de l'AP-HP 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

Note : Voir le référentiel des standards de l'AP-HP pour plus de détail sur ce point.

II.10. LES ÉCHANGES DE FICHIERS

R Afin de minimiser les besoins en 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, accessibles aux différents composants concernés par le flux (émetteur, EAI, récepteur) sous forme de points de montage

- ⇒ NFS (version 3 ou supérieure)
- ⇒ SMB (version 2 ou supérieure)

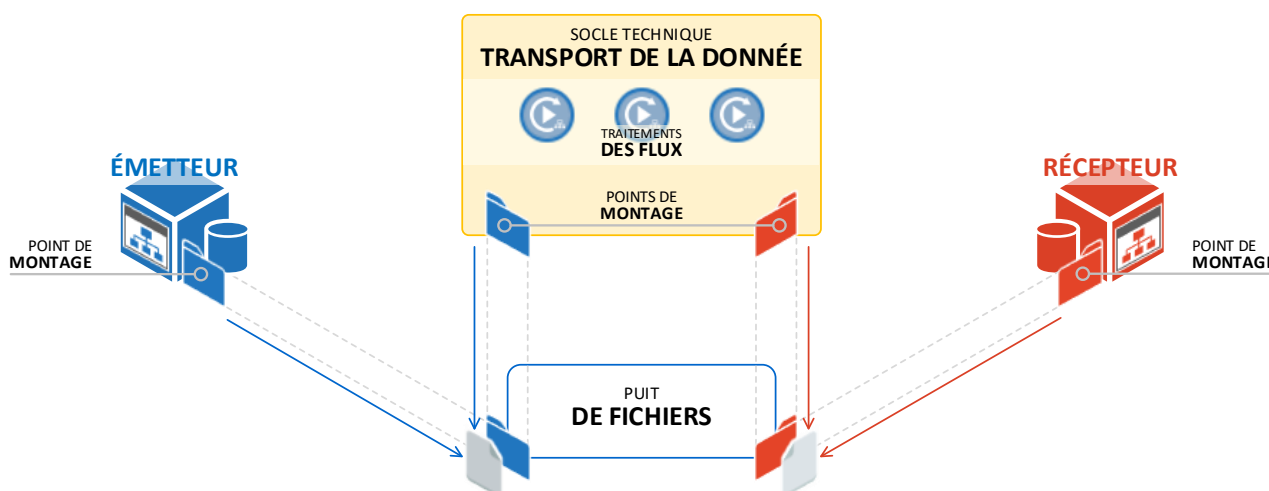


Figure 57 - Puit de fichiers pour les flux

I Il est interdit de mettre en œuvre des points de montage NFS ou CIFS au travers du WAN AP-HP, notamment pour les échanges entre un émetteur hébergé dans la zone GH et un récepteur hébergé dans la zone DATACENTER[BBS].

III. 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, tâches planifiées Windows)

O Les traitements ou les tâches d'arrière-plan récurrents doivent être planifiés par l'ordonnanceur du système d'information de l'AP-HP : **VTOM**

IV. ORCHESTRATION

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

V. SERVEUR DE PUBLICATION

Afin de faciliter la gestion, la compatibilité et l'accessibilité des progiciels utilisés au sein de son système d'information, l'AP-HP a mis en place une solution de publication d'applications et de sessions avec '**Citrix XenApp**'. Grâce à cette solution, les applications ne sont plus installées au sens traditionnel du terme sur les postes clients, mais directement sur les serveurs Citrix.

O Toute nouvelle solution/application développée spécifiquement doit être accessible exclusivement par client léger (Navigateur Web).

O Tout progiciel nécessitant l'installation d'un 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.

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

R Dans le cas où une application est accessible à la fois par client lourd et par client léger (navigateur web), il est recommandé de privilégier la solution client léger

VI. AUTRES

VI.1. SERVEUR D'APPLICATIONS JAVA

Un serveur d'applications Java est un logiciel qui fournit un environnement d'exécution pour les applications Java. Il implémente l'intégralité des spécifications Java EE (Enterprise Edition) ou Jakarta EE, et offre des services :

⇒ de gestion des transactions

- ⇒ de persistance des données
- ⇒ de sécurité
- ⇒ de communications réseau pour les applications d'entreprise.

1.1. EN ENVIRONNEMENT CONTENEURISE – MICROSERVICE

Dans le cadre de la conteneurisation, où les microservices sont éphémères et déployés à la demande, la légèreté (c'est-à-dire inclure uniquement ce qui est nécessaire à l'application) et la rapidité au démarrage sont essentielles (paradigme du conteneur). Par conséquent, les serveurs d'applications Java traditionnels, avec leur lourdeur, ne sont plus considérés comme des solutions techniques envisageables.

I Il est interdit de déployer en conteneur dans l'infrastructure Kubernetes (K8S) des applications JAVA utilisant des technologies traditionnelles non optimisées pour la conteneurisation.

R Il est recommandé d'utiliser le framework d'application JAVA 'QUARKUS' pour toute solution ou application construite sous forme de développement spécifique JAVA orienté microservices.

R La compilation JAVA de l'application en un exécutable natif avec GraalVM (fonctionnalité de QUARKUS) est recommandée pour réduire l'empreinte mémoire et disque du conteneur ainsi que l'image de conteneur.

C. LES COMPOSANTS APPLICATIFS

I. JAVA

'JAVA' est un langage de programmation orienté objet et une plateforme informatique développée initialement par Sun Microsystems, désormais une filiale d'Oracle Corporation.

'JAVA' est conçu pour minimiser les dépendances afin de permettre aux développeurs de "coder une fois, exécuter partout" (WORA / Write Once, Run Anywhere). Autrement dit, les applications écrites en 'JAVA' devraient pouvoir fonctionner sur n'importe quelle machine dotée d'une machine virtuelle Java (JVM), sans nécessiter de modifications spécifiques liées à la plateforme.

O Du fait de l'évolution changeante et de la complexité des droits de licence sur la distribution 'JAVA' par l'éditeur Oracle, seules les distributions de 'JAVA' exemptes de tout droit de licence envers l'éditeur ORACLE sont autorisées à être téléchargées, mises à jour et/ou déployées au sein des systèmes d'information de l'AP-HP (SI central, SI local, serveurs, postes de travail, etc.).

Les distributions autorisées, par ordre de préférence, sont les suivantes :

- ⇒ Les distributions dites 'OpenJDK', libres de droits, distribuées sous licence GPLv2 avec Classpath Exception.
- ⇒ Les distributions 'JAVA' de l'éditeur Oracle exclusivement dans le cadre d'un accord entre l'éditeur Oracle et l'éditeur de la solution à déployer au sein du SI de l'AP-HP, autorisant une utilisation sans droit d'usage (un document contractuel devra obligatoirement être fourni dans ce cas).

I Il est strictement interdit de télécharger, mettre à jour et/ou déployer toutes les distributions de 'JAVA' de l'éditeur Oracle dans le système d'information de l'AP-HP, quelle que soit leur utilisation (développement interne, prérequis technique pour des solutions logicielles de poste de travail, etc.), en raison des restrictions de licence commerciale imposées par l'éditeur Oracle.

ARCHITECTURE D'ADMINISTRATION

A. LA SECURITE DES SYSTEMES D'INFORMATION

I. PRINCIPES GENERAUX DE LA PGSI

L'AP-HP a défini en 2010 et actualisé en mai 2023 une Politique Générale de Sécurité de l'Information (PGSI). Cette politique vise à garantir la préservation et la sécurisation de l'intégralité du système d'information de l'AP-HP.

Les règles énoncées dans la PGSI de l'AP-HP, ayant 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 applique le principe de défense en profondeur des systèmes d'information conformément aux recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : La défense en profondeur appliquée aux systèmes d'information.

De plus, l'AP-HP suit les bonnes pratiques de sécurité préconisées par l'ANS (Agence du Numérique en Santé).

II. ENVIRONNEMENT TECHNIQUE DE SECURITE DU SI DE L'AP-HP

II.1. POSTE DE TRAVAIL WINDOWS

L'ensemble des postes de travail et serveurs informatiques WINDOWS et LINUX sont protégés par un antivirus. Cet antivirus intègre des fonctions de détection et d'éradication des codes informatiques malveillants en temps réel. Il s'interface avec le pare-feu hôte et son 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.

II.2. MESSAGERIE ELECTRONIQUE

La solution EXCHANGE de MICROSOFT est utilisé pour la messagerie électronique.

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

Le protocole DKIM est mis en œuvre pour garantir l'intégrité des messages acheminés sur internet.

III. EXIGENCES TECHNIQUES DE SECURITE

O Les prestations qui nécessitent l'usage de mot de passe suivent, sans restriction, les recommandations de la CNIL : '[Délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés et abrogeant la délibération n° 2017-012 du 19 janvier 2017 - Légifrance \(legifrance.gouv.fr\)](#)'.

- O 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 dit 'libre') à la date de notification du marché jusqu'à sa date de fin d'exécution.

III.1. 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](#)' 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](#)' éditée par l'ANSSI.

- R 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](#)' éditée par l'ANSSI.

III.2. 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](#)' et '[Problématiques de sécurité associées à la virtualisation des systèmes d'information](#)' éditées par l'ANSSI.

III.3. 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](#)' éditée par l'ANSSI.

- O 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](#)' éditée par l'ANSSI

III.4. 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](#)' éditée par l'ANSSI.

III.5. JOURNALISATION

- 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](#)' éditée par l'ANSSI.

III.6. TELEASSISTANCE INFORMATIQUE

- 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](#)' éditée par l'ANSSI.

- Les prestations qui nécessitent l'usage de la téléassistance devront obligatoirement passer par la solution de **bastion WALLIX** afin d'accéder au SI AP-HP. Cette solution assure la gestion des accès privilégiés et permet de contrôler, superviser et tracer les accès des usages de la téléassistance.

III.7. CRYPTOGRAPHIE

- 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](#)' du Référentiel Général de Sécurité (RGS v2.0) disponible publiquement sur le site Internet de l'ANSSI.

III.8. APPLICATIONS WEB

- 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](#)' éditée par l'ANSSI.

III.9. RESEAUX

- 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.

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

- 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](#)' éditée par l'ANSSI

- Les versions du protocole TLS inférieures à 1.2 sont interdites.

- 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](#)' et '[Recommandations pour un usage sécurisé d'\(Open\)SSH](#)' éditées par l'ANSSI.

- O 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](#)' éditée par l'ANSSI

III.10. 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](#)' éditée par l'ANSSI

III.11. 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](#)' 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](#)' éditée par l'ANSSI

III.12. SECURITE PHYSIQUE ET DISPOSITIFS DE VIDEO PROTECTION

- O Les prestations qui nécessitent l'usage de dispositifs de sécurité physique suivent, sans restriction, les recommandations de la note technique intitulée '[recommandations-sur-la-securisation-des-systemes-de-contrôle-d'accès-physique-et-de-videoprotection](#)' éditée par l'ANSSI

- O Les prestations qui nécessitent l'usage de dispositifs de sécurité physique sont compatibles sans restriction avec les cartes CPS de l'ASIP Santé : La [carte CPS](#) & les [caractéristiques de la carte CTP3](#)

- O 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](#)' éditée par l'ANSSI

III.13. 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

B. LA PROTECTION DES DONNEES

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

C. LA SUPERVISION

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

A. ANNEXE 1 - DOCUMENTS DE REFERENCE

REFERENTIEL GENERAL D'INTEROPERABILITE (RGI)	CADRE DE RECOMMANDATIONS REFERENÇANT DES NORMES ET DES STANDARDS QUI FAVORISENT L'INTEROPERABILITE AU SEIN DES SYSTEMES D'INFORMATION DE L'ADMINISTRATION HTTPS://WWW.NUMERIQUE.GOUV.FR/PUBLICATIONS/INTEROPERABILITE
REFERENTIEL GENERAL D'ACCESSIBILITE POUR LES ADMINISTRATIONS (RGAA)	DOCUMENT DECRIVANT DES BONNES PRATIQUES A METTRE EN ŒUVRE POUR ASSURER L'ACCESSIBILITE DES APPLICATIONS A TOUS LES PUBLICS HTTPS://REFERENCES.MODERNISATION.GOUV.FR/ACTUALITES/ACCESSIBILITE-NUMERIQUE-LA-QUATRIEME-VERSION-DU-RGAA-EST-PUBLIEE/
REFERENTIEL GENERAL DE SECURITE (RGS)	DOCUMENT DEFINISSANT DES REGLES ET BONNES PRATIQUES EN MATIERE DE SECURITE DES SYSTEMES D'INFORMATION HTTPS://WWW.NUMERIQUE.GOUV.FR/PUBLICATIONS/REFERENTIEL-GENERAL-DE-SECURITE
RECOMMANDATIONS DE LA CNIL SUR LE THEME DE LA SANTE	HTTPS://WWW.CNIL.FR/FR/THEMATIQUES/SANTE
REFERENTIELS GMSIH ET ANAP	LES REFERENTIELS ET DOSSIERS PUBLIES PAR LE GROUPEMENT POUR LA MODERNISATION DES SYSTEMES D'INFORMATION HOSPITALIERS (GMSIH) ET CEUX PUBLIES PAR L'ANAP (AGENCE NATIONALE D'APPUI A LA PERFORMANCE DES ÉTABLISSEMENTS DE SANTE ET MEDICO-SOCIAUX), ACCESSIBLES SUR LE SITE DE L'ANAP A L'ADRESSE SUIVANTE : HTTPS://WWW.ANAP.FR/S/PUBLICATIONS-ET-OUTILS [LE GMSIH A ETE INTEGRE A L'ANAP EN OCTOBRE 2009]
PROBLEMATIQUES DE SECURITE ASSOCIEES A LA VIRTUALISATION DES SYSTEMES D'INFORMATION	ANALYSE DES RISQUES ET DES ENJEUX DE SECURITE LIES A LA VIRTUALISATION DES SYSTEMES D'INFORMATION. L'OBJET DE CE DOCUMENT EST DE PRESENTER CES RISQUES ET LES PRINCIPAUX MOYENS DE S'EN PREMUNIR. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/SECURITE-DES-SYSTEMES-DE-VIRTUALISATION
RECOMMANDATIONS DE SECURITE RELATIVES A LA TELE-ASSISTANCE	CONSEILS POUR SECURISER LES SYSTEMES DE TELE-ASSISTANCE, INCLUANT DES MESURES TECHNIQUES ET ORGANISATIONNELLES. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/LA-TELE-ASSISTANCE-SECURISEE
LA CARTE CPS3	PRESENTATION DES FONCTIONNALITES ET DES USAGES DE LA CARTE CPS3 DANS LE DOMAINE DE LA SANTE. HTTPS://INDUSTRIELS.ESANTE.GOUV.FR/PRODUITS-ET-SERVICES/SOCLE-TECHNIQUE-CPS HTTPS://INDUSTRIELS.ESANTE.GOUV.FR/PRODUITS-ET-SERVICES/CPS-ET-SOCLE-TECHNIQUE/CARACTERISTIQUES-DE-LA-CPS3
RECOMMANDATIONS DE SECURITE RELATIVES AUX ENVIRONNEMENTS D'EXECUTION JAVA SUR LES POSTES DE TRAVAIL MICROSOFT WINDOWS	CONSEILS POUR SECURISER LES ENVIRONNEMENTS JAVA SUR LES POSTES DE TRAVAIL WINDOWS. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/SECURISER-UN-ENVIRONNEMENT-DEXECUTION-JAVA-SOUS-WINDOWS
MECANISMES CRYPTOGRAPHIQUES	GUIDE SUR LES MECANISMES CRYPTOGRAPHIQUES RECOMMANDES POUR SECURISER LES DONNEES. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/MECANISMES-CRYPTOGRAPHIQUES
RECOMMANDATIONS DE SECURITE RELATIVES AUX RESEAUX WI-FI	CONSEILS POUR SECURISER LES RESEAUX WI-FI EN ENTREPRISE ET CHEZ LES PARTICULIERS. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/SECURISER-LES-ACCES-WI-FI
RECOMMANDATIONS DE SECURITE RELATIVES A UN SYSTEME GNU/LINUX	CONSEILS DE SECURITE POUR LA MISE EN PLACE ET L'EXPLOITATION DE SYSTEMES GNU/LINUX. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/RECOMMANDATIONS-DE-SECURITE-RELATIVES-UN-SYSTEME-GNULINUX
RECOMMANDATIONS POUR LA SECURISATION DES SITES WEB	CONSEILS POUR PROTEGER LES SITES WEB CONTRE LES MENACES ET LES ATTAQUES. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/SECURISER-UN-SITE-WEB
RECOMMANDATIONS DE SECURITE RELATIVES AUX ORDIPHONES	MESURES POUR SECURISER LES SMARTPHONES ET AUTRES DISPOSITIFS MOBILES. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/SECURISER-SON-ORDIPHONE
RECOMMANDATIONS POUR LA MISE EN ŒUVRE D'UNE POLITIQUE DE RESTRICTIONS LOGICIELLES SOUS WINDOWS	DIRECTIVES POUR APPLIQUER DES RESTRICTIONS LOGICIELLES SUR LES SYSTEMES WINDOWS AFIN DE RENFORCER LA SECURITE. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/METTRE-EN-OEUVRE-UNE-POLITIQUE-DE-RESTRICTIONS-LOGICIELLES-SOUS-WINDOWS

RECOMMANDATIONS DE SECURITE RELATIVES A UN SYSTEME GNU/LINUX	CONSEILS DE SECURITE POUR LA MISE EN PLACE ET L'EXPLOITATION DE SYSTEMES GNU/LINUX. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/RECOMMANDATIONS-DE-SECURITE-RELATIVES-UN-SYSTEME-GNULINUX
RECOMMANDATIONS POUR UN USAGE SECURISE D'OPENSSH	DIRECTIVES POUR SECURISER LES CONNEXIONS VIA OPENSSEH. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/USAGE-SECURISE-DOPENSSEH
RECOMMANDATIONS SUR LA SECURISATION DES SYSTEMES DE CONTROLE D'ACCES PHYSIQUE ET DE VIDEOPROTECTION & RECOMMANDATIONS DE SECURITE POUR LA MISE EN ŒUVRE DE DISPOSITIFS DE VIDEOPROTECTION	CONSEILS POUR SECURISER LES SYSTEMES DE CONTROLE D'ACCES PHYSIQUE ET DE VIDEOPROTECTION (LA V2 DU DOCUMENT INCLUS LES RECOMMANDATIONS DE SECURITE). HTTPS://CYBER.GOUV.FR/PUBLICATIONS/SECURISATION-DES-SYSTEMES-DE-CONTROLE-DACCES-PHYSIQUE-ET-VIDEOPROTECTION
L'USAGE DE MOT DE PASSE SUIVENT, SANS RESTRICTION, LES RECOMMANDATIONS DE LA CNIL	DELIBERATION N° 2022-100 DU 21 JUILLET 2022 PORTANT ADOPTION D'UNE RECOMMANDATION RELATIVE AUX MOTS DE PASSE ET AUTRES SECRETS PARTAGES ET ABROGEANT LA DELIBERATION N° 2017-012 DU 19 JANVIER 2017. HTTPS://WWW.LEGIFRANCE.GOUV.FR/JORF/ID/JORFTEXT000046432885
RECOMMANDATIONS DE SECURISATION D'UNE ARCHITECTURE DE TELEPHONIE SUR IP	CONSEILS POUR SECURISER LES INFRASTRUCTURES DE TELEPHONIE SUR IP. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/SECURISER-UNE-ARCHITECTURE-DE-TELEPHONIE-SUR-IP
RECOMMANDATIONS DE SECURITE RELATIVES A TLS	DIRECTIVES POUR SECURISER LES COMMUNICATIONS VIA TLS. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/RECOMMANDATIONS-DE-SECURITE-RELATIVES-TLS
RECOMMANDATIONS DE SECURITE RELATIVES A ACTIVE DIRECTORY	CONSEILS POUR RENFORCER LA SECURITE DES SERVICES ACTIVE DIRECTORY. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/RECOMMANDATIONS-DE-SECURITE-RELATIVES-ACTIVE-DIRECTORY
RECOMMANDATIONS DE CONFIGURATION MATERIELLE DE POSTES CLIENTS ET SERVEURS x86	CONSEILS POUR LA CONFIGURATION SECURISEE DU MATERIEL DES POSTES CLIENTS ET SERVEURS x86. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/RECOMMANDATIONS-DE-CONFIGURATION-MATERIELLE-DE-POSTES-CLIENTS-ET-SERVEURS-X86
RECOMMANDATIONS DE SECURISATION D'UNE ARCHITECTURE DE TELEPHONIE SUR IP	CONSEILS POUR SECURISER LES INFRASTRUCTURES DE TELEPHONIE SUR IP. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/SECURISER-UNE-ARCHITECTURE-DE-TELEPHONIE-SUR-IP
RECOMMANDATIONS DE SECURITE RELATIVES A IPSEC POUR LA PROTECTION DES FLUX RESEAU	DIRECTIVES POUR SECURISER LES FLUX RESEAU AVEC IPSEC. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/RECOMMANDATIONS-DE-SECURITE-RELATIVES-IPSEC
RECOMMANDATIONS DE SECURITE POUR LA MISE EN ŒUVRE D'UN SYSTEME DE JOURNALISATION	CONSEILS POUR LA MISE EN PLACE ET LA GESTION SECURISEE DES SYSTEMES DE JOURNALISATION. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/RECOMMANDATIONS-DE-SECURITE-POUR-LARCHITECTURE-DUN-SYSTEME-DE-JOURNALISATION
RECOMMANDATIONS DE CONFIGURATION MATERIELLE DE POSTES CLIENTS ET SERVEURS x86	CONSEILS POUR LA CONFIGURATION SECURISEE DU MATERIEL DES POSTES CLIENTS ET SERVEURS x86. HTTPS://CYBER.GOUV.FR/PUBLICATIONS/RECOMMANDATIONS-DE-CONFIGURATION-MATERIELLE-DE-POSTES-CLIENTS-ET-SERVEURS-X86

Date de dernière validation des liens : 07/2024

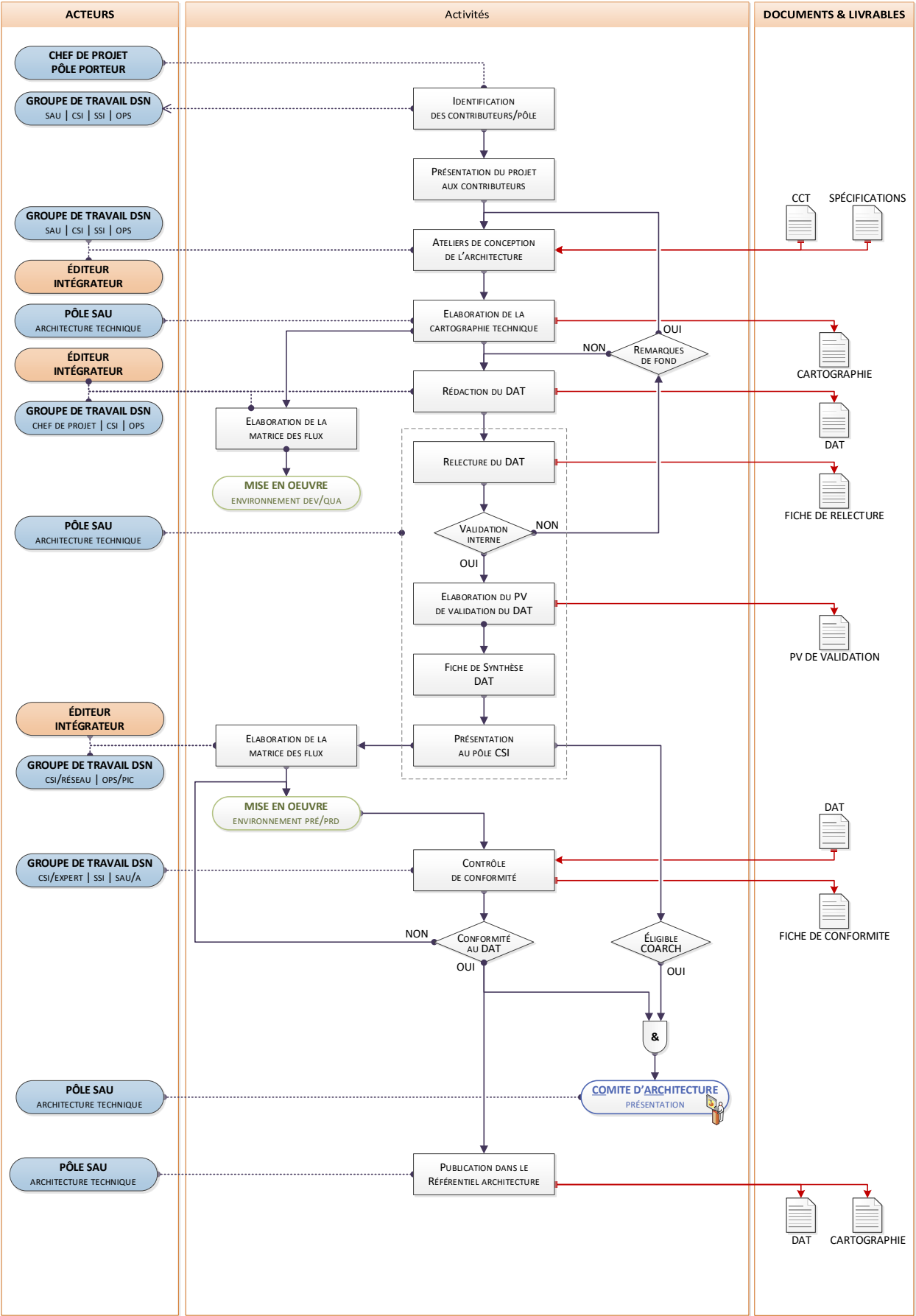
B. ANNEXE 2 - GLOSSAIRE

TERMES	DEFINITIONS
AP-HP	ASSISTANCE PUBLIQUE – HOPITAUX DE PARIS
API	APPLICATION PROGRAMMING INTERFACE
BGP	BORDER GATEWAY PROTOCOL
CCT	CADRE DE COHERENCE TECHNIQUE
CNI	CONTAINER NETWORK INTERFACE
CPU	CENTRAL PROCESSING UNIT : UNITE CENTRALE DE TRAITEMENT
COS	CLASS OF SERVICE
CSA	POLE CENTRE DE SOLUTIONS APPLICATIVES
CSI	POLE CENTRE DE SOLUTIONS DES INFRASTRUCTURES (CSI)
CSU	POLE CENTRE DE SUPPORT UNIFIE
DDOS	DISTRIBUTED DENIAL OF SERVICE
DIMA	DUREE MAXIMALE D'INTERUPTION ADMISSIBLE
DISIC	DIRECTION DES SYSTEMES D'INFORMATION ET DE COMMUNICATION DE L'ÉTAT (VOIR SGMAP)
DNS	DOMAIN NAME SYSTEM
DRS	DISTRIBUTED RESSOURCE SCHEDULER
DSCP	DIFFERENTIATED SERVICES CODE POINT
DSFP	DIRECTION SPECIALISEE DES FINANCES PUBLIQUES
DSN	DIRECTION DES SYSTEMES NUMERIQUES
DWDM	DENSE WAVELENGTH DIVISION MULTIPLEXING
EAI	ENTERPRISE APPLICATION INTEGRATION (INTEGRATION D'APPLICATIONS D'ENTREPRISE)
ETALAB	MISSION EN CHARGE DE L'OUVERTURE DES DONNEES PUBLIQUES DE L'ÉTAT (VOIR SGMAP)
ETL	EXTRACT TRANSFORM LOAD. OUTIL D'EXTRACTION DE DONNEES D'UNE BASE DE DONNEES, PERMETTANT DE LES MODIFIER ET DE LES Y REPLACER.
FC	FIBER CHANNEL
FTP	FILE TRANSFER PROTOCOL
GED	GESTION ELECTRONIQUE DE DOCUMENTS
GH	GROUPEMENT HOSPITALIER
HDS	HEBERGEUR DE DONNEES DE SANTE
HTTP	HYPERTEXT TRANSFER PROTOCOL
HTTPS	HTTP SECURISE PAR SSL
IAAS	INFRASTRUCTURE AS A SERVICE
ID	POLE INNOVATIONS & DONNEES
IOPS	INPUT / OUTPUT OPERATIONS PER SECOND
IP	INTERNET PROTOCOL
IPS	INTRUSION PREVENTION SYSTEM
ISO	INTERNATIONAL STANDARDIZATION ORGANIZATION

TERMES	DEFINITIONS
JDBC	JAVA DATABASE CONNECTIVITY
JWT	JSON WEB TOKEN
K8S	KUBERNETES
LAN	LOCAL AREA NETWORK, EN FRANÇAIS RESEAU LOCAL.
LTO	LINEAR TAPE-OPEN
MOA	MAITRE D'OUVRAGE
MOE	MAITRISE D'ŒUVRE
MPLS	MULTI PROTOCOL LABEL SWITCHING
MTA	MAIL TRANSFER AGENT
NAS	NETWORK ATTACHED STORAGE
NFS	NETWORK FILE SYSTEM
NIS	NETWORK INFORMATION SERVICE
NTP	NETWORK TIME PROTOCOL
OPS	POLE OPERATIONS
OS	« OPERATING SYSTEM » : SYSTEME D'EXPLOITATION
PGSSI	POLITIQUE GENERALE DE LA SECURITE DU SYSTEME D'INFORMATION
QOS	QUALITY OF SERVICE
RAC	REAL APPLICATION CLUSTER
RGAA	REFERENTIEL GENERAL D'ACCESSIBILITE POUR LES ADMINISTRATIONS
RGI	REFERENTIEL GENERAL D'INTEROPERABILITE
RGS	REFERENTIEL GENERAL DE SECURITE
RPO	RECOVERY POINT OBJECTIVE
RTO	RECOVERY TIME OBJECTIVE
SAAS	SOFTWARE AS A SERVICE
SAE	SYSTEME D'ARCHIVAGE ELECTRONIQUE
SAN	STORAGE AREA NETWORK
SCCM	SYSTEM CENTER CONFIGURATION MANAGER
SCSI	SMALL COMPUTER SYSTEM INTERFACE
SEDA	STANDARD D'ECHANGE DE DONNEES POUR L'ARCHIVAGE
SGBDR	SYSTEME DE GESTION DE BASE DE DONNEES RELATIONNELLES
SGMAP	SECRETIARIAT GENERAL POUR LA MODERNISATION DE L'ACTION PUBLIQUE (ADMINISTRATION REGROUPANT LA DISIC, ETALAB ET LA DIRECTION INTERMINISTERIELLE POUR LA MODERNISATION DE L'ACTION PUBLIQUE)
SAU	POLE STRATEGIE, ARCHITECTURE, URBANISATION
SI	SYSTEME D'INFORMATION
SIAP	SYSTEME D'INFORMATION DE L'ASSISTANCE PUBLIQUE – HOPITAUX DE PARIS
SIF	SYSTEME D'INFORMATION FINANCIER
SNMP	SIMPLE NETWORK MANAGEMENT PROTOCOL
SQL	STRUCTURED QUERY LANGUAGE
SSL	SECURE SOCKET LAYER

TERMES	DEFINITIONS
SSO	SINGLE SIGN ON
TCP	TRANSMISSION CONTROL PROTOCOL
TOIP	TELEPHONY OVER IP
VM	VIRTUAL MACHINE
VMDK	VIRTUAL MACHINE DISK
VPN	VIRTUAL PRIVATE NETWORK
VOIP	VOICE OVER IP
VRRP	VIRTUAL ROUTER REDUNDANCY PROTOCOL
WAF	WEB APPLICATION FIREWALL
WAL	WRITE-AHEAD LOGGING
WSUS	WINDOWS SERVER UPDATE SERVICES

C. ANNEXE 3 - PROCESSUS DE CONCEPTION/VALIDATION DU DAT



D. ANNEXE 4 - SOLUTIONS TECHNIQUES PAR DOMAINES FONCTIONNELS

CATEGORIES	LOGICIELS (PAGES ASSOCIEES)	DESCRIPTION/FONCTION
API MANAGEMENT	GRAVITEE (60)	GESTION DES API ET DES FLUX INTER-APPLICATIFS
BASES DE DONNEES	ETCD (59), REDIS (59), CASSANDRA (59), HBASE (59), MONGODB (58), MSSQL (58, 59), MySQL & MARIADB (58, 59), ORACLE (58), POSTGRESQL (58, 59), ORIENTDB (59)	SOLUTIONS DE STOCKAGE DE DONNEES STRUCTUREES ET NON STRUCTUREES
CLUSTERING	PACEMAKER/COROSYNC (57), PGPOOL (57), SAFEGUARD (57), SAFEKIT (57)	OUTILS POUR HAUTE DISPONIBILITE ET CLUSTERING DE SERVEURS
CONTENEURISATION	CONTAINERD (37), KUBERNETES (37)	OUTILS DE GESTION DE CONTENEURS ET D'ORCHESTRATION
DEVELOPPEMENT	JAVA ORACLE (73), OPENJDK (73)	ENVIRONNEMENTS D'EXECUTION ET DEVELOPPEMENT JAVA
PLANIFICATION	VTOM (71)	OUTILS DE PLANIFICATION ET D'AUTOMATISATION DES TACHES
PROTECTION DES DONNEES	COMMMVAULT (78)	SOLUTION DE SAUVEGARDE ET DE PROTECTION DES DONNEES
REPARTITION DE CHARGE	NGINX (39,54), RADWARE ALTEON (18, 27, 54), ADC (18, 27, 54), VIP (53, 54), REVERSE-PROXY (27), WAF (18)	SOLUTIONS POUR LA REPARTITION DE CHARGE ET PROXY INVERSE
RESEAU	CALICO (39)	SOLUTION DE MISE EN RESEAU POUR KUBERNETES
SECURITE	CORTEX XDR (51)	SOLUTION D'ANTI-VIRUS ET DE SECURITE DES POSTES DE TRAVAIL
STOCKAGE	CEPH (43)	OUTIL DE STOCKAGE DISTRIBUE ET SCALABLE
SUPERVISION	CENTREON (78)	OUTIL DE MONITORING ET SUPERVISION DES INFRASTRUCTURES
SYSTEMES D'EXPLOITATION	HP-UX, REDHAT ENTERPRISE LINUX & WINDOWS SERVEUR (44)	SYSTEMES D'EXPLOITATION POUR SERVEURS
VIRTUALISATION	VMWARE ESXi (34), vSPHERE (34)	OUTILS POUR LA GESTION ET LA VIRTUALISATION DES SERVEURS

INDEX

A

ADC	VOIR APPLICATIONS DELIVERY CONTROLLER
ANTI-VIRUS	
CORTEX XDR	51
API MANAGEMENT	
GRAVITEE	60
APPLICATIONS DELIVERY CONTROLLER	
REPARTITION DE CHARGE	54
REVERSE-PROXY	27
VIP	54
WAF	18
ARCHITECTURES	
ITANIUM	33
X86-64BITS	33, 35
AUTHENTIFICATION	
* LES REGLES	57
FLUX INTER-APPLICATIFS	69
MFA	57

B

BASES DE DONNEES	
* LES REGLES	58
CLE/VALEUR	
ETCD	59
REDIS	59
EN COLONNES	
CASSANDRA	59
HBASE	59
NOSQL	
MONGODB	58
ORIENTEES GRAPHES	59
RELATIONNELLES	
MSSQL	58, 59
MYSQL & MARIADB	58, 59
ORACLE	58
POSTGRESQL	58, 59

C

CALICO	39
CASSANDRA	59
CENTREON	78
CEPH	43
CLUSTER VMWARE	VOIR VMWARE

CLUSTERING

PACEMAKER/COROSYNC	57
PGPOOL	57
SAFEGUARD	57
SAFEKIT	57
COMMVAULT	78
CONTAINERD	37
CONTENEURISATION	
CONTAINERD	37
KUBERNETES	37
MOTEUR DE CONTENEURISATION	37
STOCKAGE PERSISTANT	42
CORTEX XDR	51
CRYPTOGRAPHIE	76

D

DATACENTERS	15, 21
-------------------	--------

E

EAI

MIRTH	60
SOLUTION EAI AP-HP	60
ECHANGES INTER-APPLICATIFS	60
* LES REGLES	60
API MANAGEMENT	60
GRAVITEE	60
AUTHENTIFICATION	69
EAI	
MIRTH	60
EAI	
SOLUTION EAI AP-HP	60
FLUX	
EXTERNE	65, 66, 67, 68
INTERNE	61, 62, 63, 64
FORMAT	70
PROTOCOLES	69, 70
SECURITE	68, 69, 70
ELICE	12, 13, 15
EOL LOGICIELS	75
ESXI	VOIR VMWARE
ETCD	59

F

FERMES ESXI.....	VOIR VMWARE
FILTRAGE	21, 23
FIREWALL.....	15, 16, 17, 18, 21, 22, 24, 29
FTP.....	76

G

GPU	34
GRAVITEE	60

H

HA.....	VOIR HAUTE DISPONIBILITE
HAUTE DISPONIBILITE	55
* LES REGLES	55
CONCEPTS	55
DMIA/MTDP	55
ISO 22301	55
RPO	55
RTO	55
SOLUTION DE CLUSTERING	
PACEMAKER/COROSYNC	57
PACEMAKER/SAFEGUARD.....	57
PGPOOL.....	57
SAFEKIT.....	57
HBASE	59
HDS	27, 49, 57
HEBEGEMENTS	
CLOUD PRIVE	
* LES REGLES	49
CLOUD PUBLIC	
* LES REGLES	49
ARCHITECTURE.....	49
HUB	49
SPOKE	49
ZONE CENTRALE.....	49
ZONE SATELLITE	49
PRIVE	
STRATEGIE.....	48
HPE OPERATIONS ORCHESTRATION.....	71
HP-UX.....	44
HTTP.....	76

I

INFRASTRUCTURES	
MAINFRAME.....	32
PHYSIQUES	32
CONVERGEES	

HPE SYNERGY.....	33
HYPERCONVERGEES	
HPE SIMPLIVITY	33
VIRTUELS	34
INGRESS	
NGINX.....	39
INGRESS KUBERNETES.....	38
INTERFACES RESEAUX	
SERVEURS PHYSIQUES.....	33
SERVEURS VIRTUELS	35
IPAM.....	15
IPS.....	18

J

JAVA	
* LES REGLES	73
JAVA ORACLE	73
OPENJDK	73

K

KUBERNETES	
ARCHITECTURE SERVEURS.....	37
CALICO.....	39
CONTAINER NETWORK INTERFACE/CNI	39
INGRESS	38
NGINX.....	39
NAMESPACE	40
POD.....	40

L

LIVRABLE	
MATRICE DES FLUX	31

M

MAN[ELICE]	12, 13, 15
MARIADB	58, 59
METROCLUSTER VMWARE.....	36, 37
MIRTH	60
MONGODB	58
MSSQL.....	58, 59
MYSQL.....	58, 59

N

NGINX	39, 54
-------------	--------

O

ORACLE.....	58
ORCHESTRATION	
HPE OPERATIONS ORCHESTRATION	71
TACHES TECHNIQUES	71

P

PACEMAKER/COROSYNC	57
PGPOOL.....	57
PLANIFICATION	
VTOM	71
POD	40
POSTE DE TRAVAIL	
LOGICIELS.....	52
MATÉRIEL	51
POSTES FIXES	51
POSTES MOBILES	51
SECURITE.....	51
CORTEX XDR	51
SYSTEME	51
POSTGRESQL	58, 59
PROTECTION DES DONNEES	
COMMAULT	78
SAUVEGARDE	78
PROTOCOL	
FTP.....	76
HTTP	76
REXEC	76
RLOGIN	76
TELNET	76
TLS.....	76
PROXY	29

Q

QUALITE DE SERVICE/QOS	30
------------------------------	----

R

RADWARE ALTEON	
APPLICATIONS DELIVERY CONTROLLER.....	18
REPARTITION DE CHARGE.....	54
REVERSE-PROXY	27
VIP	54
WAF.....	18
REDHAT ENTREPRISE LINUX.....	44
REDIS.....	59
REPARTITION DE CHARGE	
* LES REGLES	53

NGINX.....	54
RADWARE ALTEON	54
REPLICATION	
BASES DE DONNEES	59
RESEAU	
* LES REGLES	12
CONNEXIONS	31
CONNEXIONS DES PARTENAIRES.....	19
FILTRAGE	21, 23
FIREWALL	
IPS.....	18
INTERCONNEXION DES SITES AP-HP	13
IPAM.....	15
LES ACCES INTERNET	16
LES COUCHES	25
LES DATACENTERS.....	15, 21
LES NIVEAUX DE SENSIBILITES	27
LES ZONES DE SECURITE HOMOGENE	12
CLOUD.....	12
DATACENTER[BBS].....	12
DMZ	12
GROUPEMENTS HOSPITALIERS/GH	12
INTERCONNEXION.....	12
MAN[ELICE]	12
WIFI PUBLIC	12
LIVRABLE/MATRICE DES FLUX.....	31
MAN[ELICE]	12, 13, 15
MPLS	
APN 3G	20
PARTENAIRES	19
ROSES.....	20
PASSERELLE D'INTERCONNEXION	17
PETALES	13
PROXY	29
QUALITE DE SERVICE/QOS	30
REVERSE PROXY	27
SEGMENTATION.....	23
URL FILTERING.....	29
VIP.....	53, 54
VLAN.....	21
WAF	
CLOUD.....	18
DMZ	18
WLAN.....	29
ZONE DE SENSIBILITE	27
REVERSE PROXY	27
REXEC.....	76
RING SCALITY	47
RLOGIN	76
ROSES.....	20

S

SAFEGUARD	57
SAFEKIT	57
SAUVEGARDE	
RING SCALITY	47
SECNUMCLOUD.....	49
SECURITE	74
ANTIVIRUS	77
APPLICATION WEB	76
CPS/CPS3.....	77
CRYPTOGRAPHIE.....	76
FIREWALL	15, 16, 17, 18, 21, 22, 24, 29
MESSAGERIE	74
MS ACTIVE DIRECTORY	75
OS/LINUX	75
PGSI	74
POSTE DE TRAVAIL	74, 75
PROTOCOL	
FTP.....	76
HTTP	76
REXEC	76
RLOGIN.....	76
TELNET	76
TLS.....	76
SERVEUR	75
VIDEO PROTECTION	77
SERVEUR D'APPLICATION	71
EN CONTENEUR	
QUARKUS	72
SERVEUR DE PUBLICATION	71
CITRIX XENAPP	71
SERVICES D'INFRASTRUCTURE	53
STOCKAGE	
CONCEPTS	45
PRIMAIRE.....	46
* LES REGLES	46
GESTION	47
SAN	46
SAUVEGARDE	
RING SCALITY	47
SECONDAIRE	47
SUPERVISION	78
CENTREON	78
SUPPORT	
VERSION LOGICIELS.....	75
SYSTEMES D'EXPLOITATION	
* LES REGLES	44
MISE A JOUR	
REDHAT SATELLITE.....	44
WSUS	44
OS	
HP-UX.....	44

REDHAT ENTREPRISE LINUX	44
WINDOWS SERVEUR	44

T

TELNET	76
TLS	76

U

URL FILTERING	29
---------------------	----

V

VERSION LOGICIELS	75
VIP	53, 54
RADWARE ALTEON	54
VIRTUALISATION	
APPLICATIVE/CONTENEUR	37
SYSTEMES/VM	34
MONSTER VM	34
VMWARE	
ESXI	34
FERME	35
METROCLUSTER	36, 37
VMDK	35
VMOTION	35
VSPHERE	34
VSWITCH	35
VIRTUELLE IP	53, 54
VLAN.....	21
VMDK	35
VMOTION.....	35
VMWARE	
ESXI	34
FERME/CLUSTER ESXI.....	35
METROCLUSTER.....	36, 37
VMDK.....	35
VMOTION	35
VSPHERE.....	34
VSWITCH	35
VSPHERE	34
VSWITCH	35
VTOM	71

W

WAF	
CLOUD	18
DMZ	18

WINDOWS SERVEUR44

WSUS..... 44