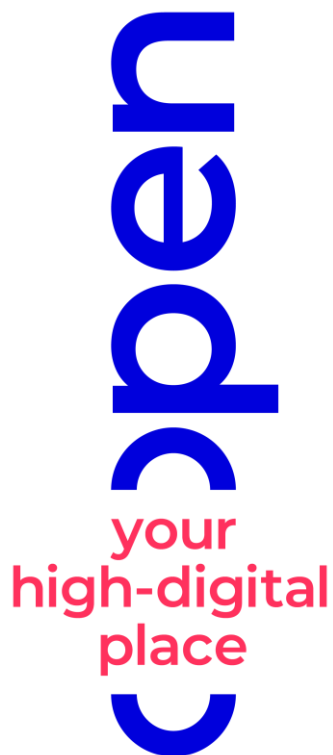




Direction Interdépartementale des Routes Centre-Est (DIR CE) SAGACITE

Dossier d'Architecture Technique

VOTE INTERLOCUTEUR COMMERCIAL :

Saliou SALANE

Tél. : +33 (0)6 58 27 14 10

Saliou.salane@open-groupe.com

VOTRE INTERLOCUTEUR TECHNIQUE :

Michael TESSIER

Tél. : + 33 (0)6 88 80 26 22

Michael.tessier@open-groupe.com

Statut OPEN : En validation

Classification : Protégé

Version : 1.8

Référence : DIRCE_SAGACITE_DAT_219



Propriétaire

Entité	Fonction
DIR-CE	Directeur de Projet

Périmètre de diffusion

Entité	Destinataire
DIR-CE	Jean-Philippe GUILLAUD
DIR-CE	François ROCHAT
DIR-O	Frédéric Le Roux

Version	Date	Rédigé par	Vérifié par (Fonction/Nom)	Validé par (Fonction/Nom)
0.0	15/08/2022	Architectes : POIRIER Jérémy BRUNET Guillaume	Chef de Projets : Jean-Marc RICHON	
		Initialisation du document. Ce dernier annule et remplace le SAGACITE-DAT-Dossier architecture-v2.5		
0.2	27/10/22	Jean-Pierre BERTHON	Chef de Projets : Jean-Marc RICHON	
		Eclatement du document en une partie commune et des annexes listant les spécificités par instance de production		
0.3	07/11/22	Jean-Pierre BERTHON	Chef de Projets : Jean-Marc RICHON	
		Réintégration §8.4.2.2, 8.4.2.3 et 8.4.3.1		
0.4	08/11/22	Jean-Pierre BERTHON	Chef de Projets : Jean-Marc RICHON	
		Corrections mineures		
0.5	22/11/22	Jean-Marc RICHON	Chef de Projets : Jean-Marc RICHON	
		Correction mineure (LDAP) plus évolutions notées sur la FDL V0.0 + ajout ASF (§ 8.4.4)		
0.6	06/04/22	Julien HOLLNER		
		Ajout 8.8.5.1 (partie prod Ansible Sagacité)		
0.7	10/05/23	Jean-Marc RICHON	Chef de Projets : Jean-Marc RICHON	



Version	Date	Rédigé par	Vérifié par (Fonction/Nom)	Validé par (Fonction/Nom)
	Ajout protocole d'identification de Keycloak			
1.0	11/05/23	Jean-Marc RICHON	Xavier CLEMENCE	Xavier CLEMENCE
	Validation DAT V0.7			
1.1	25/07/23	Jean-Marc RICHON	Chef de Projets : Jean-Marc RICHON	
	Suppression de la partie DIRSO – ASF pour l'inclure dans l'annexe DIRSO et suppression des BDD rajoutées dans les annexes de chaque DIRs			
1.2	25/07/23	Jean-Marc RICHON	Chef de Projets : Jean-Marc RICHON	
	Suppression du schéma de la V7 à la suite de la migration OSIRIS			
1.3	15/09/23	Jean-Marc RICHON	Pilote Pôle Contrôle : Jean-Pierre BERTHON	Architecte : Xavier CLEMENCE
	Prise en compte des remarques acceptées de la fiche de lecture SAGA_FDL_DAT_DossierArchitectureTechnique_Prod_V1.2			
1.4	05/09/20 24	Laurence Guiblain	SDM : Bruno Boivin	Architecte : Rémy Choupin
	Prise en compte des remarques acceptée de la FDL SAGA_FDL_DAT_DossierArchitectureTechnique_Prod_V1.3			
1.5	12/09/20 24	Laurence Guiblain	SDM : Bruno Boivin	Architecte : Rémy Choupin
	Changement de template DAT – mise à jour des données infra			
1.6	27/09/20 24	Architecte : Rémy Choupin		
	Prise en compte des remarques acceptées de la fiche de lecture SAGA_FDL_DAT_DossierArchitectureTechnique_Prod_V1.5			
1.7	22/10/20 24	Architecte : Rémy Choupin		
	Version modifiée avec les remarques suite à la relecture du 10/10/2024			
1.8	22/12/20 25	Architecte : Thomas Couton	SDM : Marc Louchart	Pilote Pôle Contrôle : Laurent Caulfuty
	Version modifiée avec les ajouts de la DIRA, de la DIRNO et des mises à jour techniques : & 5.5 Architecture Réseau et Sécurité : modification du schéma global ; & 5.6.6 Sauvegardes : modification des préconisations			



Sommaire

1	OBJET DU DOSSIER D'ARCHITECTURE TECHNIQUE	6
2	DOCUMENTS APPLICABLES ET DE REFERENCE	7
2.1	Documents de référence	7
3	TERMINOLOGIE ET CONVENTIONS.....	7
3.1	Sigles et acronymes généraux	7
4	CONTEXTE DU PROJET ET SYNTHESE DES FONCTIONNALITES.....	9
4.1	Présentation des DIR	9
4.2	Répartition géographique du périmètre	9
4.2.1	Listes par DIR des différents PC.....	9
4.2.2	Adresses des PC hébergeant SAGACITE.....	10
4.3	Synthèse des fonctionnalités majeures.....	10
4.4	Contraintes majeures à respecter	10
4.4.1	Exigences en matière de sécurité des SI	10
4.5	Composants logiciels V8.D	11
4.5.1	Vue globale des VMs SAGACITE	11
4.5.2	Vue interne des différents composants	11
4.5.3	Cluster middleware @way	13
4.5.4	Cluster services @way	14
4.5.5	Serveur d'authentification @way AUTH.....	15
4.5.6	Base de données Atway-BD	15
4.5.7	Base de données Atway-HISTO	16
5	ARCHITECTURE TECHNIQUE DE PRODUCTION.....	17
5.1	Description du cluster VMware.....	17
5.2	Description détaillée des équipements matériel	17
5.2.1	Schéma de câblage du cluster VMware	17
5.2.2	Connexion réseaux des switches SAN.....	18
5.2.3	Connexions réseaux des switches LAN.....	19
5.2.4	Baie de stockage	19
5.2.5	Hyperviseurs ESX.....	21
5.3	Infrastructure Production par DIR.....	22
5.3.1	Sites de production.....	22
5.3.2	Liste des serveurs physiques	22
5.3.3	Plan des baies.....	22
5.3.4	Matrice de câblage.....	23



5.3.5	Schéma d'infrastructure	23
5.4	Plateforme système	23
5.4.1	Socle de virtualisation.....	23
5.4.2	Machines virtuelles.....	23
5.4.3	Rôles, services et fonctionnalités.....	24
5.5	Architecture réseau et sécurité	24
5.5.1	Schéma global (vue macro)	24
5.5.2	Périmètre	25
5.5.3	Plan d'adressage IP.....	25
5.5.4	Interconnexions VPN	26
5.5.5	Architecture OpenVPN Sagacité.....	26
5.5.6	Matrices de flux	28
5.5.7	Inventaire équipements réseaux	28
5.5.8	Informations liaisons opérateurs.....	29
5.6	Services mutualisés OPEN.....	29
5.6.1	Serveurs de Rebond	29
5.6.2	Serveur OCS – CMDB.....	30
5.6.3	Supervision Centreon	31
5.6.4	Dépôt Debian 11.....	34
5.6.5	Centralisation des logs de sécurité	34
5.6.6	Sauvegarde.....	35
5.6.7	Anti-Virus ESET	35
5.6.8	Gestion de l'observabilité.....	35
5.7	Dossier d'exploitation	36



1 Objet du dossier d'architecture technique

Ce document constitue le Dossier d'Architecture Technique (DAT) infra de l'infrastructure d'hébergement production du Système d'Aide à la Gestion de Trafic (SAGT) SAGACITÉ.

2 Documents applicables et de référence

2.1 Documents de référence

Date	Type	Contenu	Référence
	CCTP	Cahier des clauses techniques particulières	AMO_TMA_SAGT_SAGACITE_CCTPv3
	MT	Mémoire technique	OPEN_SAGACITE_PRP_2021-0719_V1.0
	ANNEXE au CCTP	ANNEXE 3 au CCTP : Clauses sécurité AMO & TMA SAGACITE	CCTP Sagacité - Annexe 3 - Clauses sécurité AMO & TMA
	DAT	DAT Solution SAGACITE dans Archimate	

Les documents de référence sont les documents qui ne sont pas créés durant le projet, mais sur lesquels les documents applicables s'appuient.

On peut citer :

- Le cahier des charges ou autre document de ce type (CCTP, CCAP, ...) ;
- La réponse OPEN ;
- Les RFC des protocoles utilisés ;
- Les documentations techniques des environnements et des outils de développement utilisés ;
- ...

3 Terminologie et conventions

3.1 Sigles et acronymes généraux

Acronyme	Description
SAGT	Systèmes d'Aide à la Gestion de Trafic



DIR	Directions Interdépartementales des Routes
DIRCE	DIR Centre-Est
DIRE	DIR Est
DIRMC	DIR Massif-Central
DIRO	DIR Ouest
DIRSO	DIR Sud-Ouest
DIRCO	DIR Centre-Ouest
DIRA	DIR Atlantique
DIRNO	DIR Nord-Ouest
PC	Postes de contrôle
CIGT	Centres d'Ingénierie et de Gestion du Trafic - idem PC
VMware ESXi	Elastic Sky X Integrated – hyperviseur du constructeur Vmware
VMWare NSX	Network Virtualization and Security Platform – virtualisation réseau et sécurité Vmware
VM	Virtual Machine - machine virtuelle en français
(V)LAN	(Virtual) Local Area Network – réseau local (virtuel)
WAN	Wide Area Network – réseau à grande échelle géographique
VPN	Virtual Private Network – réseau privé virtuel
IPsec	Internet Protocol Security – suite de protocoles garantissant la sécurisation d'une communication inter-machines (utilisée dans le cadre de VPN)



SPOF	Single Point Of Failure – élément à risque dans une infrastructure (très souvent, car il y a un manque de robustesse)
(D)DOS	(Distributed) Deny Of Service



4 Contexte du projet et synthèse des fonctionnalités

4.1 Présentation des DIR

Les Directions Interdépartementales des Routes (DIR) sont des services déconcentrés du Ministère de la transition écologique et Solidaire. Pour mener à bien leurs missions de gestion et d'exploitation du réseau routier national, les DIR s'appuient sur des PC* (Postes de Contrôle) répartis sur leur territoire d'intervention.

Ces PC diffusent notamment de l'information sur les conditions de circulation à destination des usagers au moyen d'équipements dynamiques. Les DIR ont, de plus, en charge la mise en place d'équipements dynamiques, le développement de réseaux de télécommunications ainsi que la mise en œuvre de systèmes informatiques permettant le bon fonctionnement des PC.

Pour certains PC, les DIR ont déployé des Systèmes d'Aide à la Gestion de Trafic, systèmes informatiques permettant d'optimiser les missions des opérateurs des PC en offrant une seule interface pour différentes tâches gérées usuellement par des systèmes informatiques différents.

(*) Selon les DIR, les PC sont également appelés "CIGT" pour Centres d'Ingénierie et de Gestion du Trafic. Ce document n'emploiera que la dénomination de "PC" pour l'ensemble des DIR.

4.2 Répartition géographique du périmètre

4.2.1 Listes par DIR des différents PC

DIR	PC/CIGT	Instances de production
DIR Centre-Est	PC Genas (Lyon) (Host)	1
	PC Hyrondelle (Saint-Étienne)	
	PC Gentiane à Grenoble	1
	PC Osiris à Albertville	1
DIR Est	CISGT de Metz (MYRABEL)	1
DIR Massif-Central	CIGT d'Issoire (Host)	1
	CIGT de Clermont-l'Hérault	
DIR Ouest	CIGT de Rennes (Host)	1
	CIGT Triskell (mutualisé sur 2 sites St-Brieuc et à Vannes)	
	CIGT Nantes	
DIR Sud-Ouest	CIGT de Toulouse (ERATO) (Host)	1
	CIGT de Saint-Paul-de-Jarrat	
DIR Centre-Ouest	CISGT de Limoges	1
DIR Atlantique	CIGT de Lormont	1
DIR Nord-Ouest	CIGT de Darnetal	1



4.2.2 Adresses des PC hébergeant SAGACITE

SAGACITE est installée dans les PCs aux adresses suivantes :

DIR	Adresse des sites de production
DIR CE Genas	Lieu-dit "Les grandes terres" - 69740 Genas
DIR CE Gentiane	17 boulevard Joseph VALLIER – CS 40215 – 38030 Grenoble Cedex 2
DIR CE Osiris	1, route de Grignon 73200 Albertville
DIR Ouest	L'Armorique - 10 rue Maurice Fabre – CS 63108 - 35031 Rennes Cedex
DIR Sud-Ouest	2, Impasse Alphonse Brémont - 31200 TOULOUSE
DIR Massif Central	District nord - Route de l'ancien pont d'Orbeil - 63500 Issoire
DIR Est	La Maison Rouge A31 Echangeur Metz-Sud 57160 Moulins-les-Metz
DIR Est	SIR Lorrain (Service d'Ingénierie Routière) 10 et 16 promenade des Canaux BP 82120 54021 Nancy cedex
DIR Centre Ouest	Rue de Boisseuil, 87220 Feytiat
DIR Atlantique	31 rue du Prince Noir 33310 Lormont
DIR Nord-Ouest	6 rue de Verdun, 76160 DARNETAL

4.3 Synthèse des fonctionnalités majeures

Les principales fonctions du SAGT sont :

- **Superviser le trafic** : Acquérir les données terrain (comptage, PMV,...), calculer les niveaux de trafic et les temps de parcours, gérer les alarmes et alertes, gérer les événements et visualiser les données sur le synoptique.
- **Appliquer la politique d'exploitation** : Aide aux mesures d'exploitation, suivre les actions, piloter les équipements, diffuser l'information.
- **Exploiter le réseau** : informer les usagers et partenaires, échanger avec l'extérieur et gérer les chantiers.
- **Gérer le SAGT** : Configuration du référentiel, Historisation et archivage.
- **Superviser le SAGT** : Supervision des défaillances, maintenir et superviser les équipements, gérer l'heure.

4.4 Contraintes majeures à respecter

4.4.1 Exigences en matière de sécurité des SI

Les exigences en matière de sécurité des SI sont référencées dans le document suivant :

CCTP Sagacité - Annexe 3 - Clauses sécurité AMO & TMA

4.5 Composants logiciels V8.D

4.5.1 Vue globale des VMs SAGACITE

Le schéma ci-dessous présente les machines virtuelles (VM), ainsi que les clusters et les VIP (adresses IP virtuelles) déployés en production.

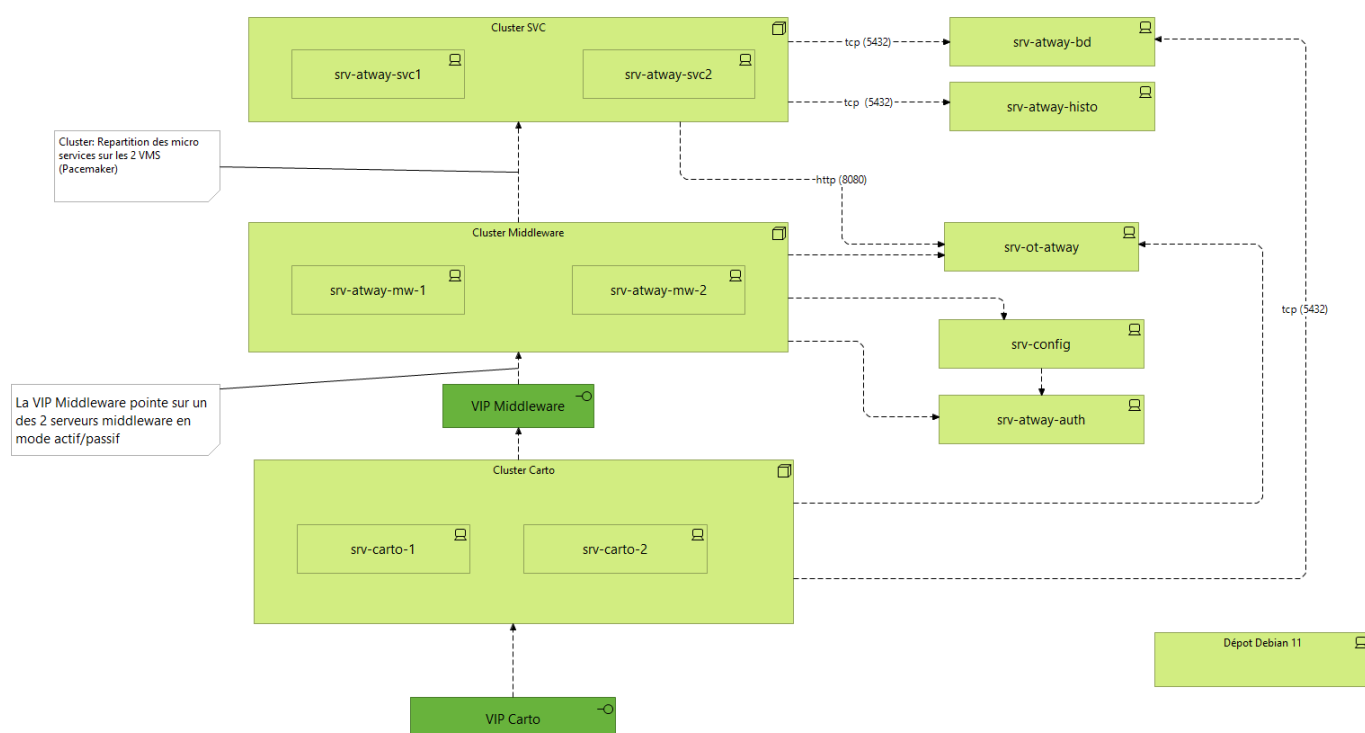


Figure 1 – Vue globale des VMs SAGACITE

4.5.2 Vue interne des différents composants

Le schéma suivant est une illustration des différents composants utilisés dans SAGACITE.

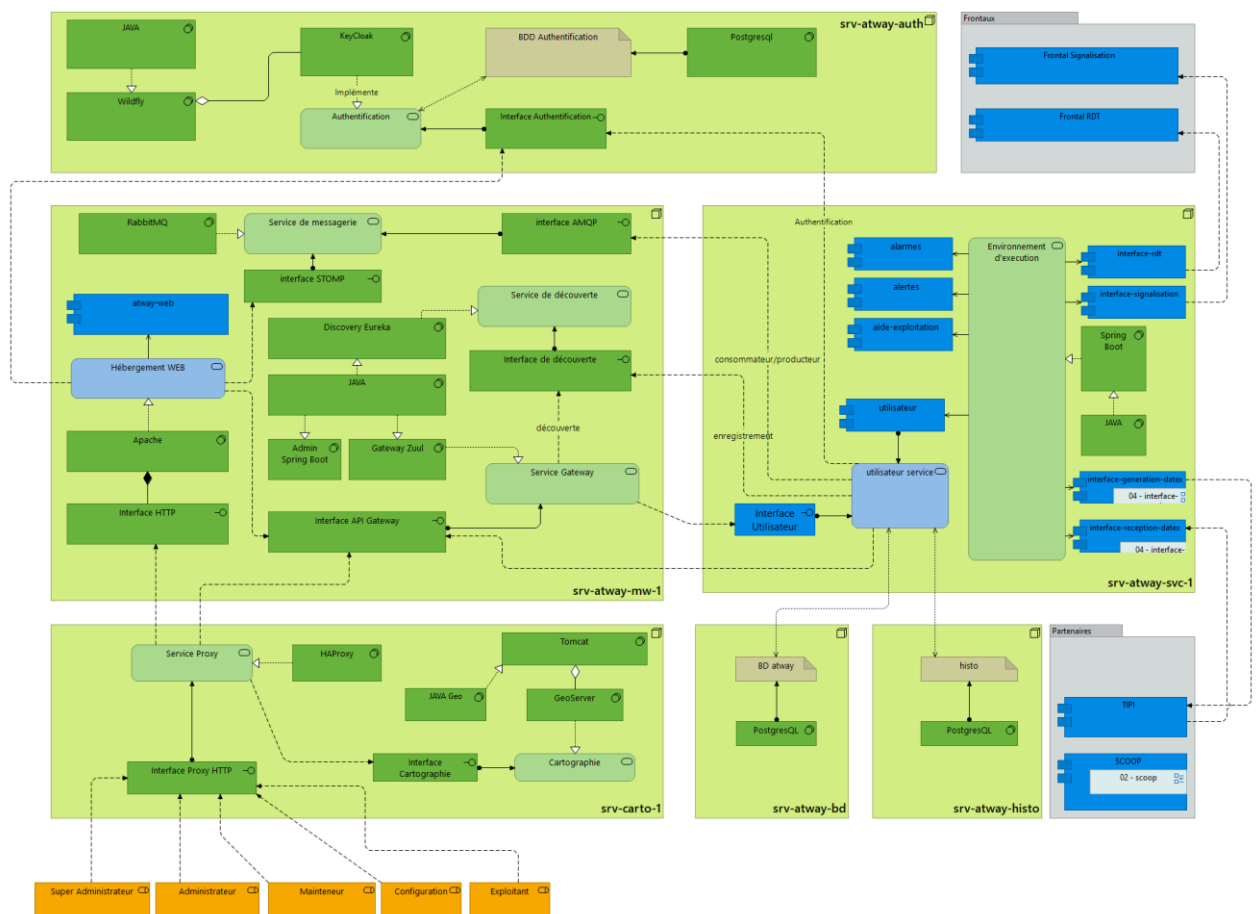


Figure 2 - Vue des composants applicatifs SAGACITE

4.5.2.1 Cluster CARTO

- Le cluster Cartographie est le cluster frontal
- Le cluster CARTO utilise « pacemaker » et est composé de deux nœuds.
- Il est configuré à la fois en ACTIF/PASSIF (« Service Proxy ») et LOAD-BALANCING (« Service Tomcat »)

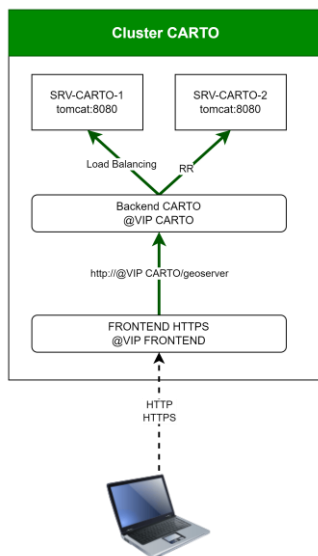


Figure 4 - Cluster Carto

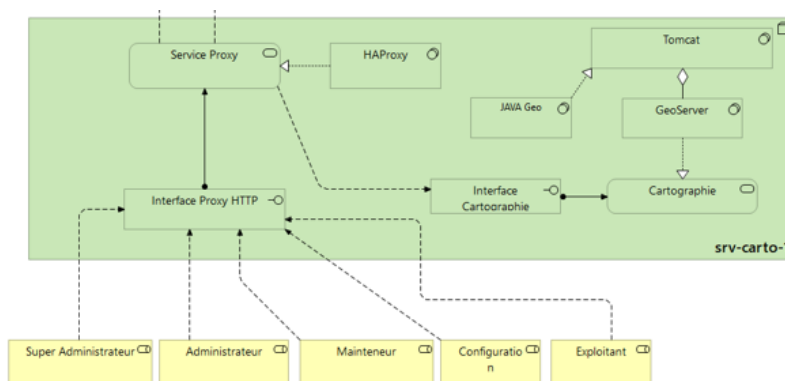


Figure 3 - Composants applicatifs d'un nœud VM Carto

4.5.3 Cluster middleware @way

- Le cluster MW utilise la couche logiciel « pacemaker » et est composé de deux nœuds.
- Il est configuré en ACTIF/PASSIF associé à une VIP

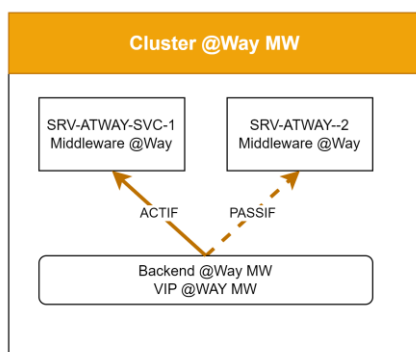


Figure 6 - Cluster Middleware

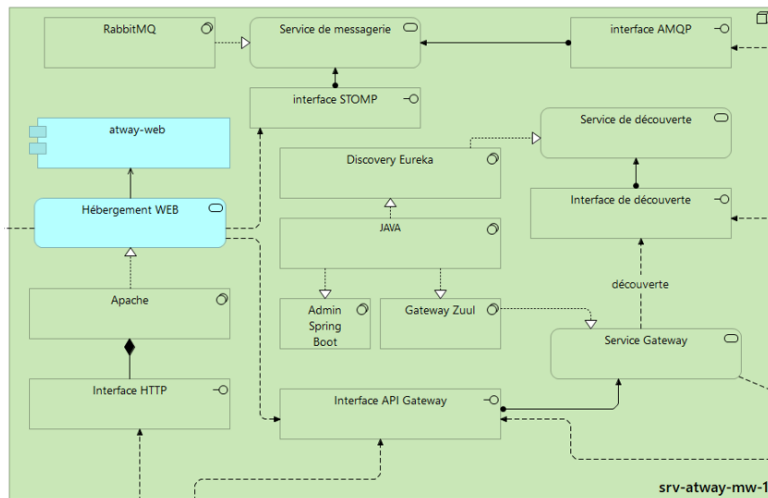


Figure 5 - Composants applicatifs d'un nœud Middleware

4.5.4 Cluster services @way

- Le cluster Services héberge la totalité des micro-services @way.
- Le cluster « Services » utilise la couche logiciel « pacemaker » et est composé de deux nœuds.
- Il est configuré en ACTIF/ACTIF en mode « Load-Balancing »
- Il n'y a pas de VIP associé au cluster
- L'emplacement des micro-services dans le cluster sont connus via le service « Gateway » hébergé sur le cluster Middleware.

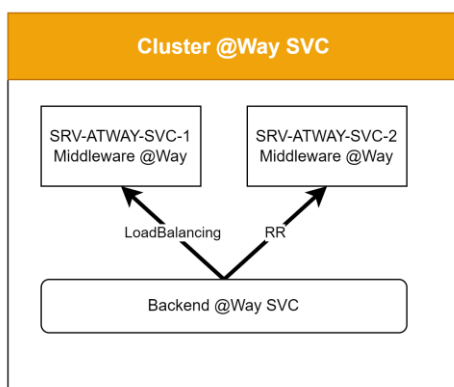


Figure 8 - Cluster SVC

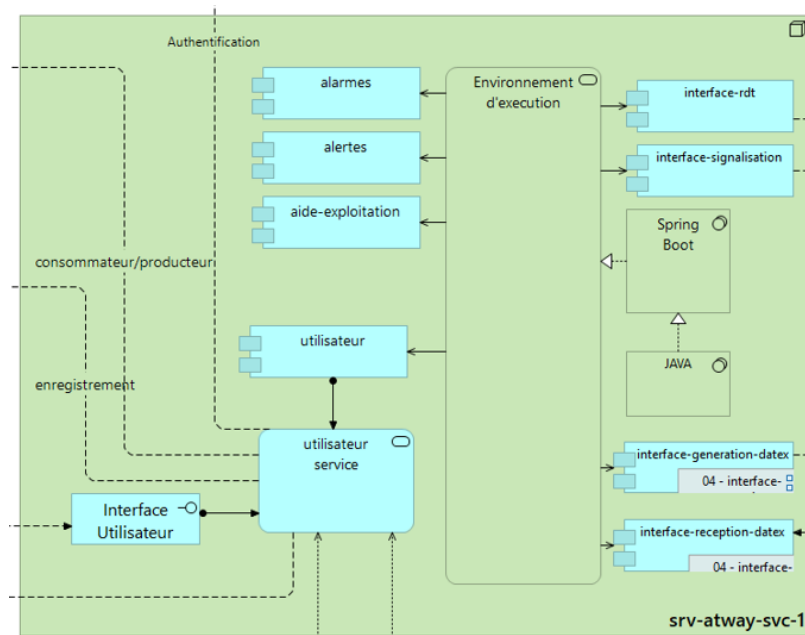


Figure 7 - Composants applicatifs d'un nœud Services

4.5.5 Serveur d'authentification @way AUTH

Le serveur d'authentification utilise « Keycloak » associé à une base PostgreSQL.

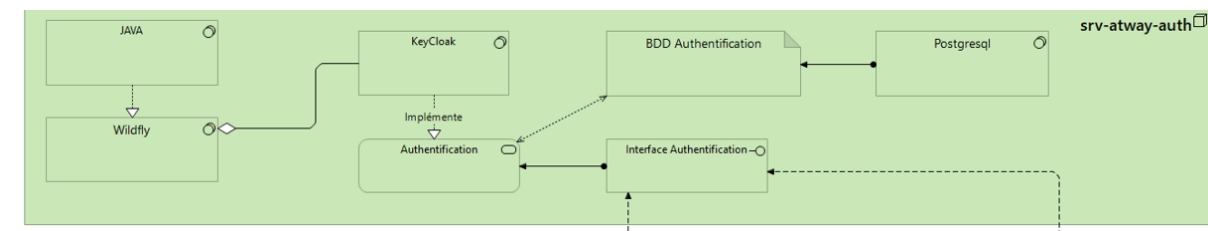


Figure 9 - VM AUTH

4.5.6 Base de données Atway-BD

La base de données « Atway-BD » stocke les événements de la journée ainsi que les référentiels statiques et dynamiques du SAGT.

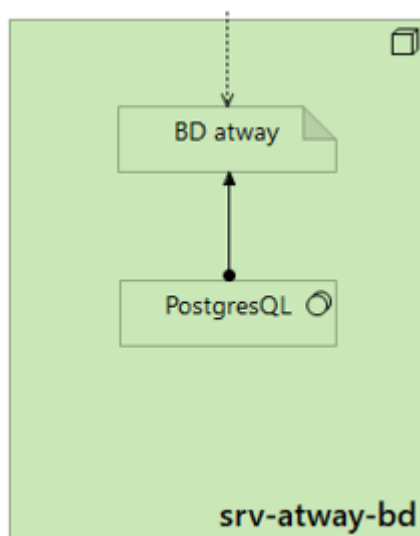


Figure 10 - VM BD

4.5.7 Base de données Atway-HISTO

La base de données « Atway-HISTO » stocke l'historique des événements SAGT. La base est alimentée par batch toutes les nuits à partir de la base de données Atway-BD.

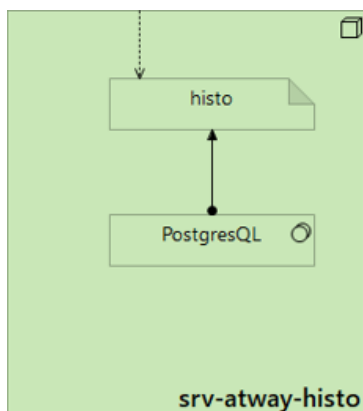


Figure 11 - VM BdD HISTO

5 ARCHITECTURE TECHNIQUE DE PRODUCTION

Ce chapitre décrit l'infrastructure système et réseau mise en place sur les DIRs.

Sur chaque DIR est installé un cluster VMware dédié à la production. Le chapitre ci-dessous décrit les éléments d'architecture définissant l'infrastructure détaillée du cluster VMware.

5.1 Description du cluster VMware

L'architecture physique SAGT repose sur deux serveurs VMware ESX partageant une baie de stockage partagée.

Le SAGT est relié aux frontaux et aux postes opérateurs par le réseau métier. Les serveurs sont reliés à la baie de stockage par un réseau iSCSI dédié.

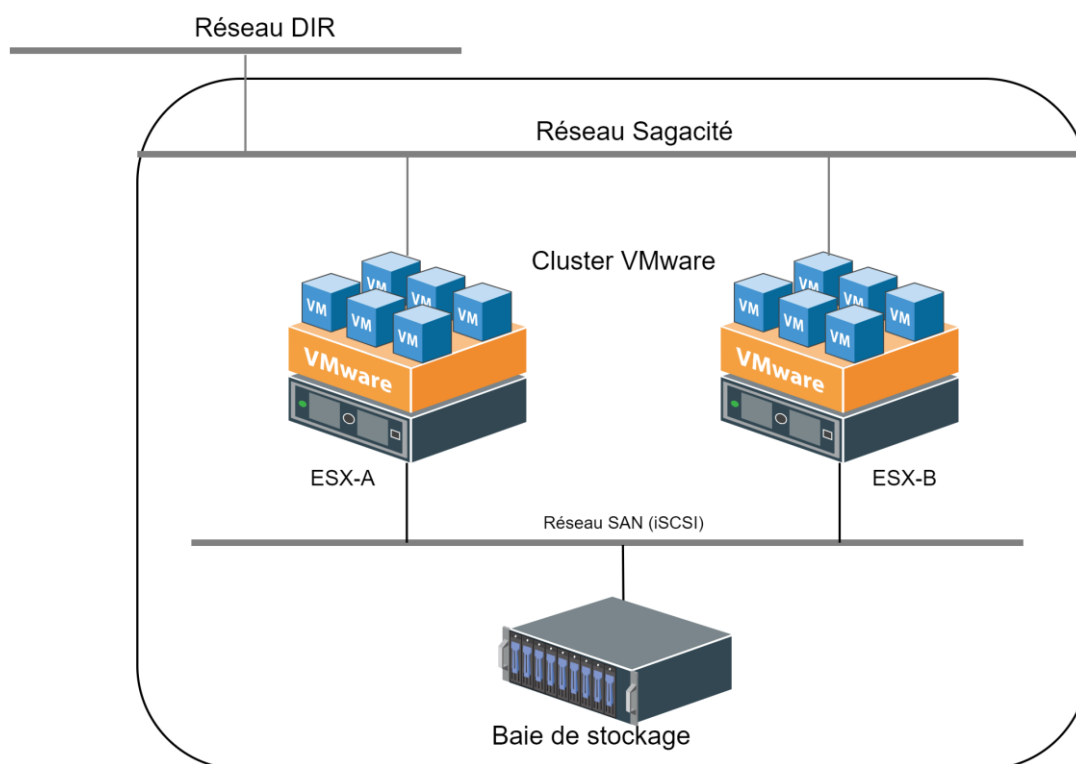


Figure 12 - Cluster VMWare SAGACITE

5.2 Description détaillée des équipements matériel

5.2.1 Schéma de câblage du cluster VMware

- Le schéma ci-dessous décrit la matrice de câblage entre les switches LAN & SAN et les 2 serveurs ESX.

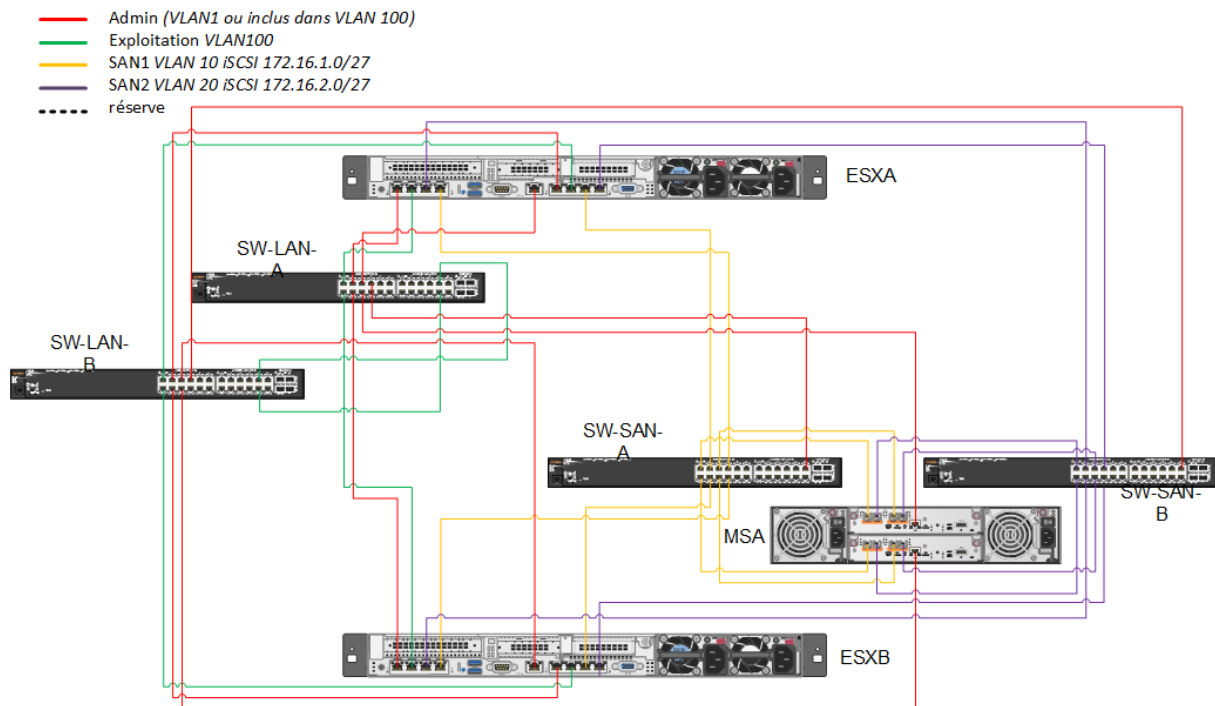


Figure 13 - Schéma de câblage

5.2.2 Connexion réseaux des switches SAN

Les switches SAN doivent respecter l'affectation des interfaces suivantes :

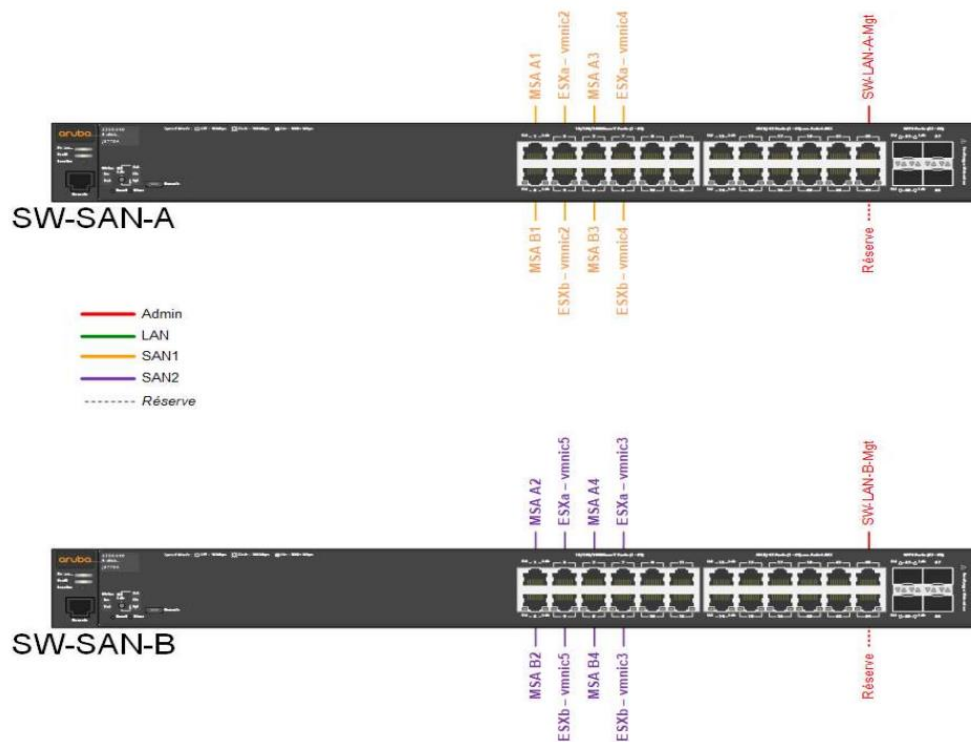


Figure 14 - Switches SAN

Chaque switch contient un VLAN Métier et un VLAN iSCSI :

- VLAN Métier : à spécifier en fonction du réseau métier, sert uniquement pour administrer les switches
- VLAN SAN1 iSCSI : 10
- VLAN SAN2 iSCSI : 20
- Les jumbo frames doivent être activées sur ces VLAN.

5.2.3 Connexions réseaux des switches LAN

Les switches LAN doivent respecter l'affectation des interfaces suivantes :



Figure 15 - Switches métier

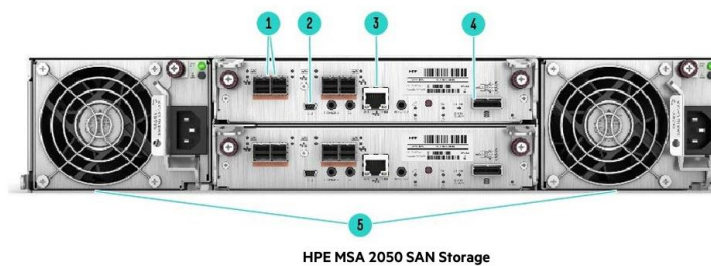
5.2.4 Baie de stockage

5.2.4.1 Modèle HPE MSA 2050 ou 2060

La plupart des DIR utilisent le modèle MSA 2050

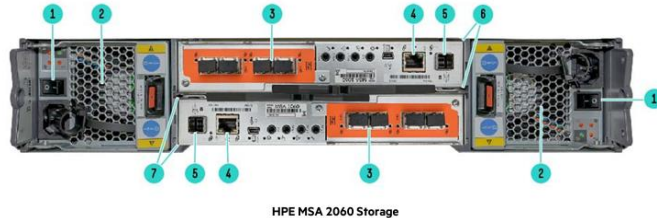


Figure 16 - 5.2.4.1.1. Vue frontale MSA 2050



- HPE MSA 2050 SAN Storage**
- 1. Host connection ports*
 - 2. CLI port (mini-USB)
 - 3. Management Ethernet port
 - 4. Expansion port
 - 5. AC or DC power supplies
- Notes:** *8 and/or 16Gb FC, 1 and/or 10GbE iSCSI or 12Gb SAS

Figure 17 - Vue arrière MSA 2050



- HPE MSA 2060 Storage**
- | Item | Description |
|------|---|
| 1. | Power Switch |
| 2. | Redundant Power and Cooling Module (AC or DC) |
| 3. | Host connection ports (8/16Gb FC, 10/25GbE iSCSI, 10GbBase-T iSCSI, or 12Gb SAS depending on model) |
| 4. | Ethernet management port |
| 5. | 12Gb SAS expansion port |
| 6. | Controller A (Inverted) |
| 7. | Controller B |

Figure 18 - Vue arrière MSA 2060

5.2.4.2 Connexion des interfaces réseaux

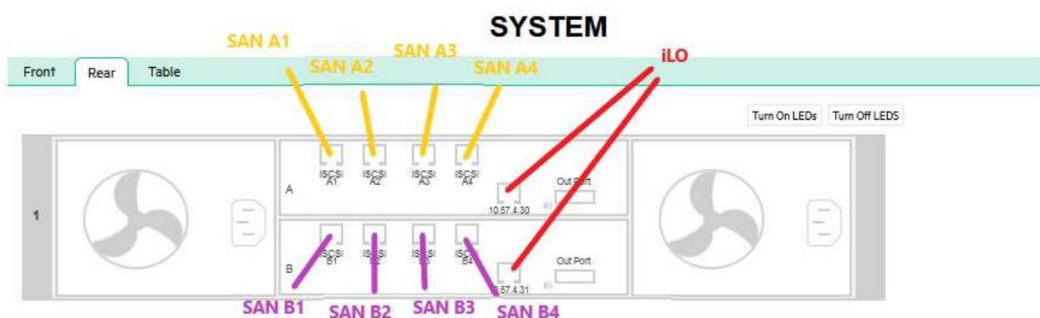


Figure 19 - Connexions réseau BAIE MSA 2050

- **Contrôleur A :**
 - VLAN SAN 1: A1 et A3
 - VLAN SAN 2: A2 et A4
- **Contrôleur B :**
 - VLAN SAN 1: B1 et B3
 - VLAN SAN 2: B2 et B4

5.2.4.3 Configuration des volumes

Par défaut 4 volumes différents sont créés sur la baie MSA

- Vol-VMFS-A1
- Vol-VMFS-A2
- Vol-VMFS-B1
- Vol-VMFS-B2

PS : Les tailles et nombre des volumes (Datastore) peuvent différer en fonction des DIRs.

5.2.5 Hyperviseurs ESX

5.2.5.1 Modèle de serveur

Le modèle de serveur (sauf exception) utilisé pour SAGACITE comme nœud ESX est :

- **HPE ProLiant DL360 Gen10** (Processeur : Intel Xeon®)



Figure 20 - Vue frontale ProLiant DL360

5.2.5.2 Connexion des interfaces réseaux

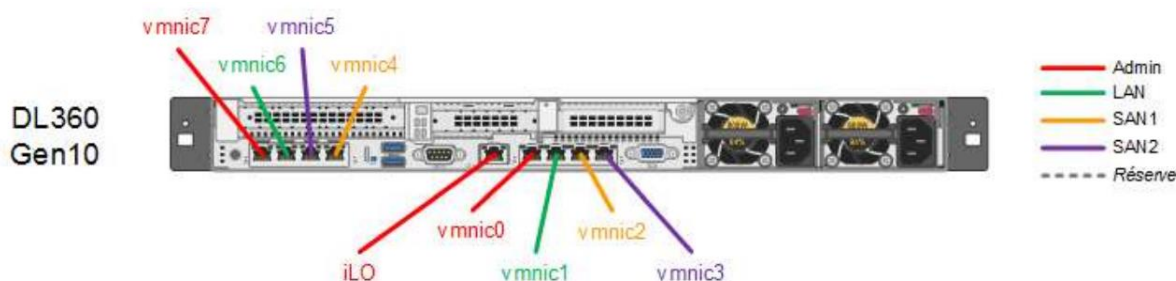


Figure 21 - Schéma de connexion réseau DL360

- Administration : Vmnic 0 et 7
- Management serveur : iLO
- Réseau Métier : Vmnic 1 et 6

- VLAN SAN 1: Vmnic 2 et 4
- VLAN SAN 2: Vmnic 3 et 5

5.2.5.3 Carte iLO

La carte iLo est une interface de management du serveur qui permet de configurer des paramètres matériels au niveau du Hardware de la machine de manière indépendante de la machine elle-même.

5.2.5.4 Configuration RAID1



Figure 22 - Configuration système RAID1

Les serveurs disposent de 2 disques durs configurés en RAID1. Ce volume contient le système d'exploitation de l'hyperviseur ESXi.

5.3 Infrastructure Production par DIR

Les informations de chapitres suivants sont traitées dans les Annexes DAT spécifiques à chaque DIR.

5.3.1 Sites de production

Se référer au chapitre « 4.2 Répartition géographique du périmètre » page 10.

Les conditions d'hébergement (sécurité physique, redondance électrique, etc) ne sont pas connues par OPEN et ne peuvent donc être décrites dans ce document

5.3.2 Liste des serveurs physiques

Voir les Annexes donnant le détail de ces informations pour chaque instance de production

5.3.3 Plan des baies

Voir les Annexes donnant le détail de ces informations pour chaque instance de production



5.3.4 Matrice de câblage

Voir les Annexes donnant le détail de ces informations pour chaque instance de production

5.3.5 Schéma d'infrastructure

Voir les Annexes donnant le détail de ces informations pour chaque instance de production

5.4 Plateforme système

Les informations de chapitres suivants sont traitées dans les annexes « DAT » spécifiques à chaque DIR.

5.4.1 Socle de virtualisation

L'ensemble des DIR utilise la solution VMware vSphere 7.x

5.4.1.1 vCenter

Voir les Annexes donnant le détail de ces informations pour chaque instance de production

5.4.1.2 Hyperviseurs

Voir les Annexes donnant le détail de ces informations pour chaque instance de production

5.4.1.3 Datastores

Voir les Annexes donnant le détail de ces informations pour chaque instance de production

5.4.2 Machines virtuelles

5.4.2.1 Liste des machines

Voir les Annexes donnant le détail de ces informations pour chaque instance de production

5.4.2.2 Profil type de dimensionnement des ressources CPU/RAM

Profil VM	OS	vCPU	RAM (Go)	Disque (Go)
AUTH	Debian 11	2	4	64
BD	Debian 11	2	4	154
CARTO1	Debian 11	2	6	84
CARTO2	Debian 11	2	6	84
CONFIG	Debian 11	4	32	218
MW1	Debian 11	2	4	54
MW2	Debian 11	2	4	54
SVC1	Debian 11	4	24	54
SVC2	Debian 11	4	24	54
REPOS-DEBIAN	Debian 11	1	2	170
TELEMETRY	Debian 11	2	8	140



VCENTER	N/A	2	24	585
DEPLOY	Debian 11	4	8	100

NB: Les nouvelles DIR sont déployés en OS Debian 12

5.4.3 Rôles, services et fonctionnalités

5.4.3.1 Authentification

5.4.3.1.1 Sagacité

- Keycloak est utilisé comme interface d'authentification pour Sagacité mais n'est pas utilisé pour l'authentification des administrateurs de l'infrastructure.

5.4.3.1.2 Systèmes Linux

- Les comptes locaux linux sont utilisés pour identifier les intervenants :
 - Des comptes partagés à destination de chaque DIR ont été créés
 - Un compte partagé « admin-open » à destination des admin OPEN (en cours de remplacement)
 - Comptes nominatifs (en remplacement de admin-open)

Préconisation : Mise en place d'une solution LDAP en remplacement des comptes locaux.

5.4.3.2 Accès root

- Les accès root direct sont interdits.
- Les accès privilégiés (root) doivent être permis uniquement au travers des commandes su ou sudo.

5.4.3.3 DNS

Voir les Annexes donnant le détail de ces informations pour chaque instance de production.

5.4.3.4 NTP

Voir les Annexes donnant le détail de ces informations pour chaque instance de production.

5.4.3.5 Proxy Web

L'ensemble des DIR est susceptible d'utiliser le réseau RIE pour sortir sur Internet pour certains flux. Certains sites disposent d'une sortie Internet dédiée et donc peuvent également l'utiliser directement pour sortir sur Internet.

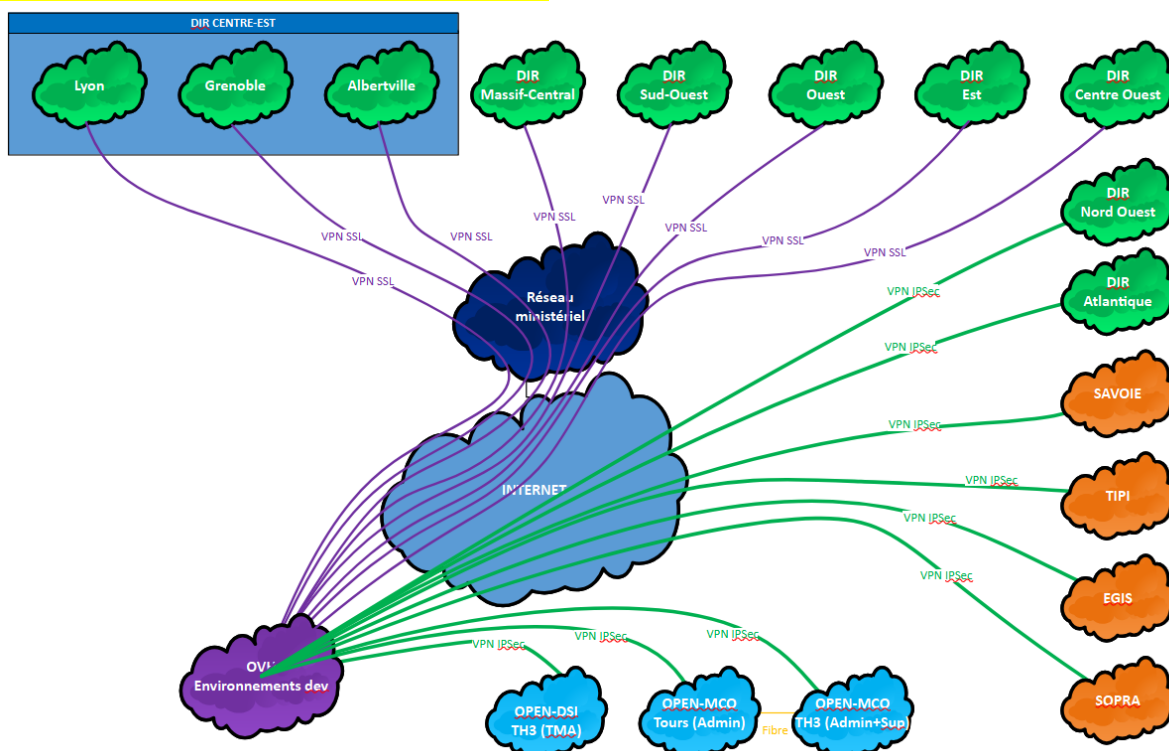
Voir les Annexes donnant le détail de ces informations pour chaque instance de production

5.5 Architecture réseau et sécurité

5.5.1 Schéma global (vue macro)

La topologie réseau retenue est la suivante :

Figure 23 - Vue globale des accès réseaux



Les interconnexions retenues sont associées aux enjeux suivants :

- Accès des administrateurs/développeurs OPEN aux infrastructures DIR depuis les sites de Tours et de Rennes en passant par OVH
- Solution de supervision OPEN hébergée sur le datacenter de Telehouse 3 (TH3) et dont un satellite global est hébergé sur OVH et récupère les informations depuis les satellites déployés sur chaque DIR.
- Accès depuis les DIR vers OVH pour réaliser des phases de tests applicatives
- Les DIR seront joignables via le RIE (à leur demande pour des raisons pratiques) qui interconnecte tous les sites distants

5.5.2 Périmètre

Le MCO des infrastructures réseaux des DIR n'est pas à la charge d'OPEN. Par conséquent, les informations qui sont exposées dans cette partie peuvent être incomplètes, ou être amenés à être modifiés sans que nous en ayons connaissance.

Les informations explicitées sont basées sur les documents fournis par les clients et par les différentes actions de recensement initiées par OPEN.

5.5.3 Plan d'adressage IP

Voir les Annexes donnant le détail de ces informations pour chaque instance de production

5.5.4 Interconnexions VPN

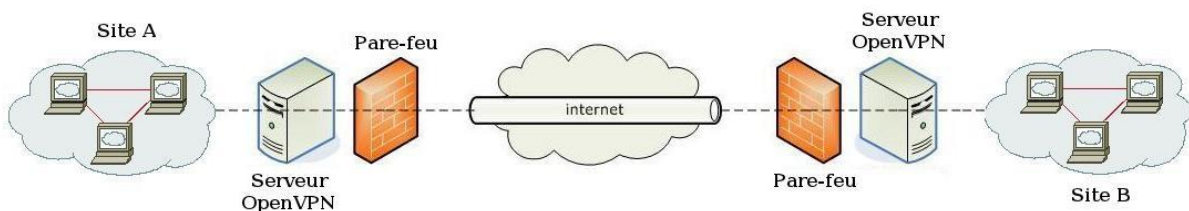
5.5.4.1 Présentation OpenVPN

OpenVPN est un protocole et solution logicielle VPN open-source permettant d'établir des interconnexions distantes sécurisées en point à point ou site à site, ainsi que des connexions nomades. Cette solution s'appuie sur un mécanisme client/serveur.

OpenVPN permet plusieurs types de topologies réseaux :

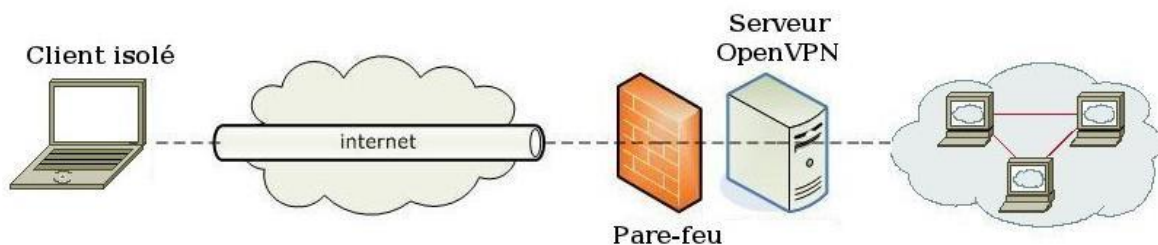
- La topologie « site à site » permet d'étendre et d'interconnecter deux sites distants.
- La topologie « nomade » permet à un utilisateur de se connecter de manière sécurisée à un site distant via son pc portable.

5.5.4.2 Topologie VPN site-à-site



Source : <https://wiki.debian-fr.xyz/>

5.5.4.3 Topologie VPN nomade



Source : <https://wiki.debian-fr.xyz/>

5.5.5 Architecture OpenVPN Sagacité

5.5.5.1 Contraintes

Les accès nécessaires, pour permettre la MCO, l'administration et la supervision des serveurs de production Sagacité ainsi que le socle d'infrastructure système, sont les suivants :

- Accès permanent des administrateurs OPEN (MCO + TMA)
- Accès permanent de la solution de supervision CENTREON
- Accès permanent de la solution de récupération des informations serveurs (OCS) pour peuplement de la CMDB
- Accès permanent de la solution de récupération de logs

Les administrateurs OPEN se connectent préalablement au serveur de rebond OVH avant de passer par le serveur de rebond spécifique à la DIR.

5.5.5.2 Principe d'interconnexion OpenVPN site à site

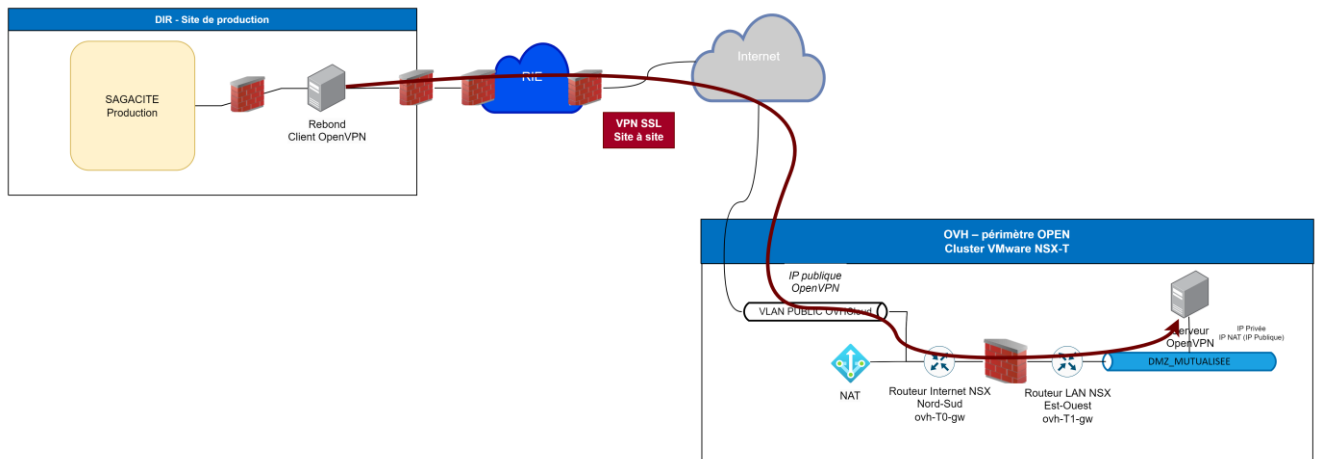


Figure 24 - Schéma OpenVPN site-à-site

Sur le schéma sont illustrées deux parties interconnectées :

- **En haut à gauche** : une DIR à interconnecter avec OVH, qui utilise le réseau RIE (SNUM)
- **En bas à droite** : l'infrastructure OVH infogérée par OPEN
- Pour initier la connexion, le client OpenVPN coté DIR initie la connexion vers le serveur OpenVPN coté OVH

Remarque : Certaines DIR ont un accès direct vers OVH sans passer par le RIE

5.5.5.3 Autres usages des VMs OpenVPN DIR & OVH

- **Côté OPEN/OVH** : le serveur OpenVPN est également utilisé comme PKI pour signer les certificats fournis
- **Côté DIR** : le client OpenVPN est également utilisé comme serveur de rebond pour OPEN

5.5.5.4 Connexion réseau (tunnel, port, protocole, proxy, routes)

Le mode tunnel est utilisé pour créer l'interconnexion VPN site à site. Un réseau d'interconnexion est spécifiquement défini et seul le serveur peut communiquer avec tous les clients (et chaque client/DIR ne peut communiquer qu'avec le serveur OpenVPN).

- **La connexion utilise le protocole TCP et s'établit sur le port 443.**

Ce choix a été suggéré par le SNUM du fait que l'accès en sortie des DIR vers le ministère sur ce port soit déjà autorisé et ne nécessite pas de demande dérogation complémentaire auprès du SNUM pour autoriser un nouveau port personnalisé.



• Proxy http pour les accès Internet

Les DIR utilisent un proxy en sortie pour joindre Internet et c'est donc ce dernier qui est renseigné dans la configuration cliente OpenVPN avant de sortir sur le réseau du SNUM. L'intégralité des informations de routage spécifiques au tunnel site à site est configurée au niveau du serveur OpenVPN, qui propage les routes sur le client OpenVPN.

• Génération de certificats

Une PKI est configurée sur le serveur OpenVPN qui joue le rôle d'autorité de certification. La configuration associée est incluse dans le fichier de configuration client OpenVPN pour simplifier le déploiement.

5.5.5.5 Liste prérequis par DIR

- Création d'un réseau dédié à l'infogérance OPEN sur l'infrastructure de la DIR
- Création et configuration d'un serveur Linux constituant à la fois le serveur de rebond OPEN et le client OpenVPN
- Configuration des routes permettant aux réseaux DIR de passer par le client OpenVPN pour joindre l'infrastructure OVH
- Implémentation des règles de filtrage selon la matrice de flux validée par les deux parties (accès serveurs Sagacité et socle système)

5.5.5.6 Modèle de matrice de flux pour chaque DIR :

Source	Destination	Service	action	comments
Serveur de rebond DIR	Socle système	ICMP, SSH (TCP/22), HTTPS (TCP/443)	accept	Accès administration
Serveur de rebond DIR	Serveurs production Sagacité	ICMP SSH (TCP/22)	accept	Accès administration + copie de fichiers (SCP)

5.5.6 Matrices de flux

Les matrices de flux étant en lien avec les adhésions de l'environnement OVH sont dans le SharePoint à l'emplacement suivante : [TMA SAGACITE > Documents Client > 05 – Documentation > 04 – DAT > Matrices de flux](#)

Le périmètre MCO du réseau des DIR étant hors-périmètre, nous ne disposons pas les informations des règles de filtrage implémentées sur les firewalls des clients.

5.5.7 Inventaire équipements réseaux

Le périmètre MCO du réseau des DIR étant hors-périmètre, nous ne disposons pas des informations

5.5.8 Informations liaisons opérateurs

Le périmètre MCO du réseau des DIR étant hors-périmètre, nous ne disposons pas des informations

5.6 Services mutualisés OPEN

5.6.1 Serveurs de Rebond

Pour permettre à OPEN d'accéder à distance aux environnements de production, une infrastructure composée de plusieurs serveurs de rebond a été mise en place. Elle comprend :

- Un serveur de rebond situé dans le réseau mutualisé OPEN d'OVH
- Un serveur de rebond présent dans chaque DIR

Cette infrastructure, appelée « bastion », renforce la sécurité en limitant les accès à un seul point d'administration pour OVH et un seul par DIR.

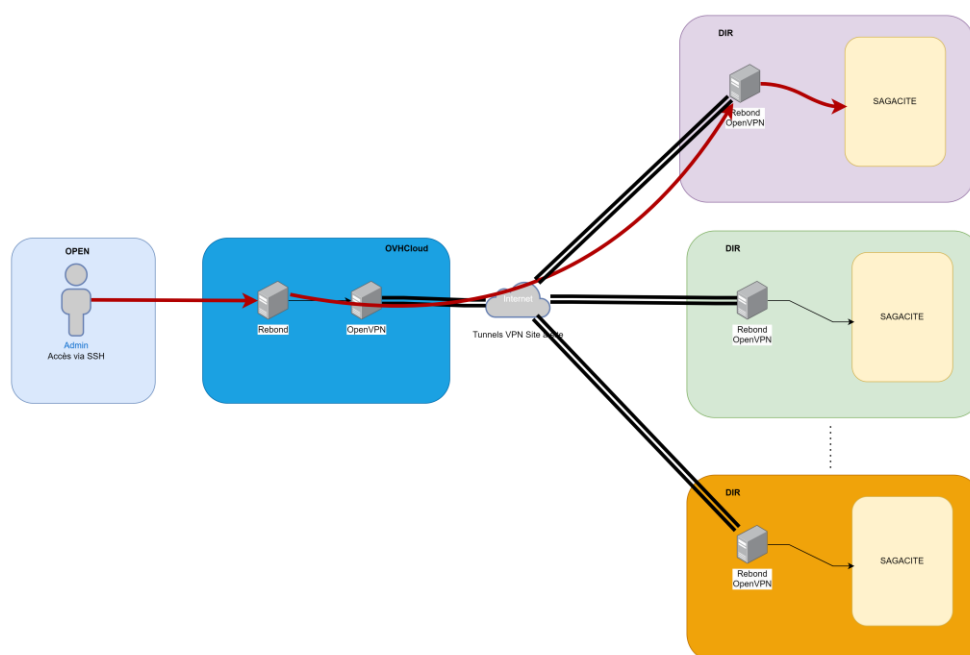


Figure 25 - Connexion admin OPEN vers les DIR

5.6.1.1 VMs

- **OpenVPN OVH**
 - Hostname: DCEVPNVP01
 - Nat: 162.19.2.211
 - IP: 10.201.1.15



- **Rebond OVH**
 - Hostname: DCERBFEVD01
 - IP: 10.201.1.3
- Les VMs de rebond des DIR sont répertoriés dans le fichier d'inventaire des VM.

5.6.2 Serveur OCS – CMDB

5.6.2.1 Description

OCS Inventory (Open Computer and Software Inventory) est un outil open-source utilisé pour la gestion de parc informatique

OPEN utilise le logiciel OCS Inventory, dans le but d'automatiser l'inventaire des serveurs dans les différentes infrastructures DIR.

OCS est une architecture client-serveur.

- **Serveur OCS** : Le serveur OCS hébergé sur le réseau mutualisé stocke les informations recueillies depuis les VMs.
- **Agents OCS** : les agents sont installés sur les systèmes, ils collectent les informations et les envois vers le concentrateur OCS.
- Les agents installés sur les VMs SAGACITE envoient les données sur le « Concentrateur OCS » via le port http (80/TCP).
- Le serveur GLPI (MCOGRVP03) collecte par batch les informations collectées par le Concentrateur OCS

5.6.2.2 Schéma de principe

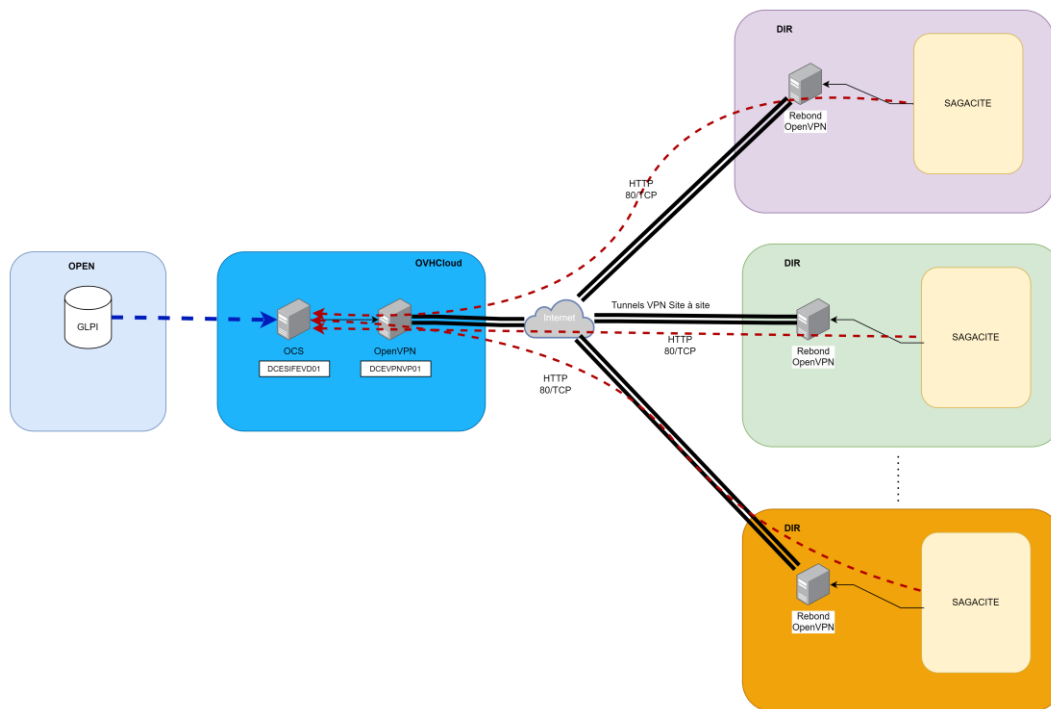


Figure 26 - Schéma de connexion vers le serveur OCS

5.6.2.3 VMs

- **Concentrateur OCS**
 - Hostname : DCESEFEVD01
 - IP : 10.201.2.9
- Les VMs des DIR sont répertoriés dans le fichier d'inventaire des VM.

5.6.3 Supervision Centreon

5.6.3.1 Schéma global

Le schéma ci-dessous est une vue des interactions entre le serveur central Centreon (concentrateur Centreon) et les différents Pollers localisés sur chaque DIR.

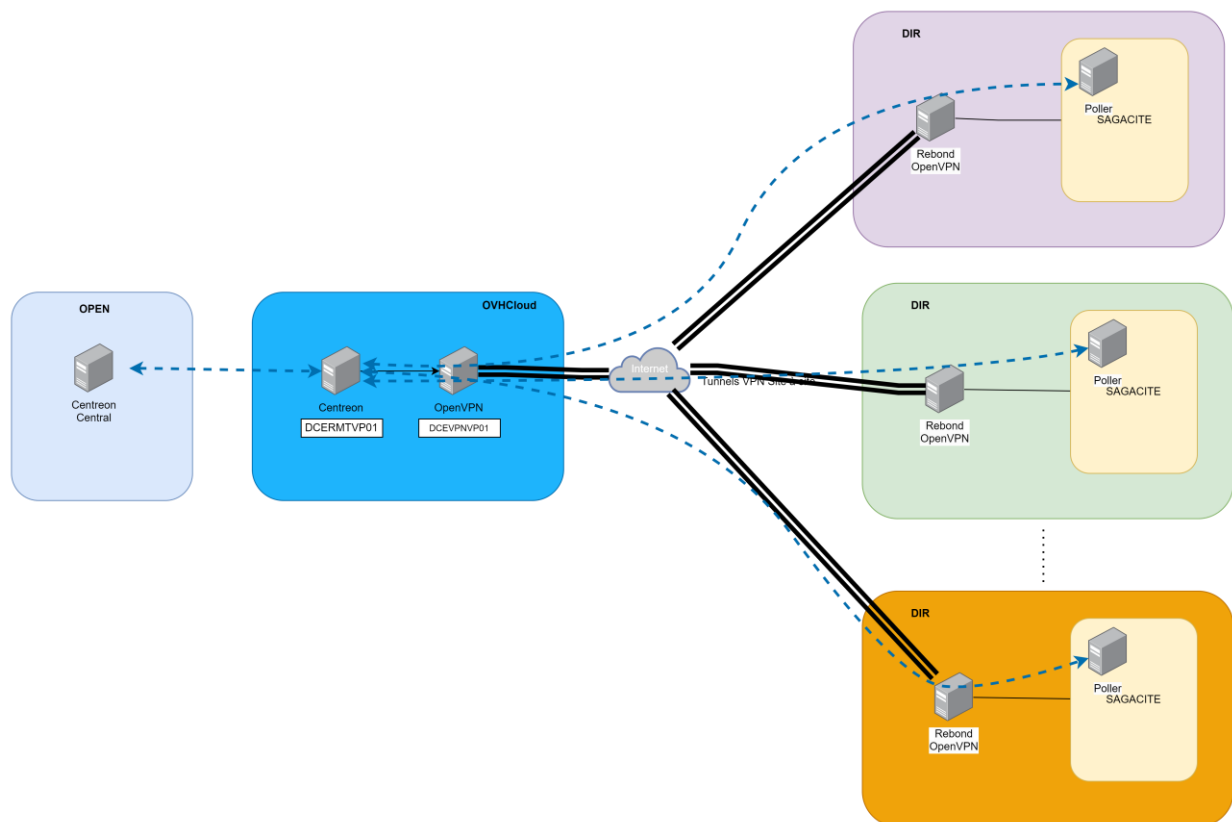


Figure 27 - Vue globale Centreon

5.6.3.2 Schéma des flux réseau (simplifié)

Le schéma ci-dessous décrit de manière générique les connexions entre les différents composants (Concentrateur Centreon, Poller, VMs et matériels).

Le schéma ne décrit pas les différentes variations possibles dans les DIR.

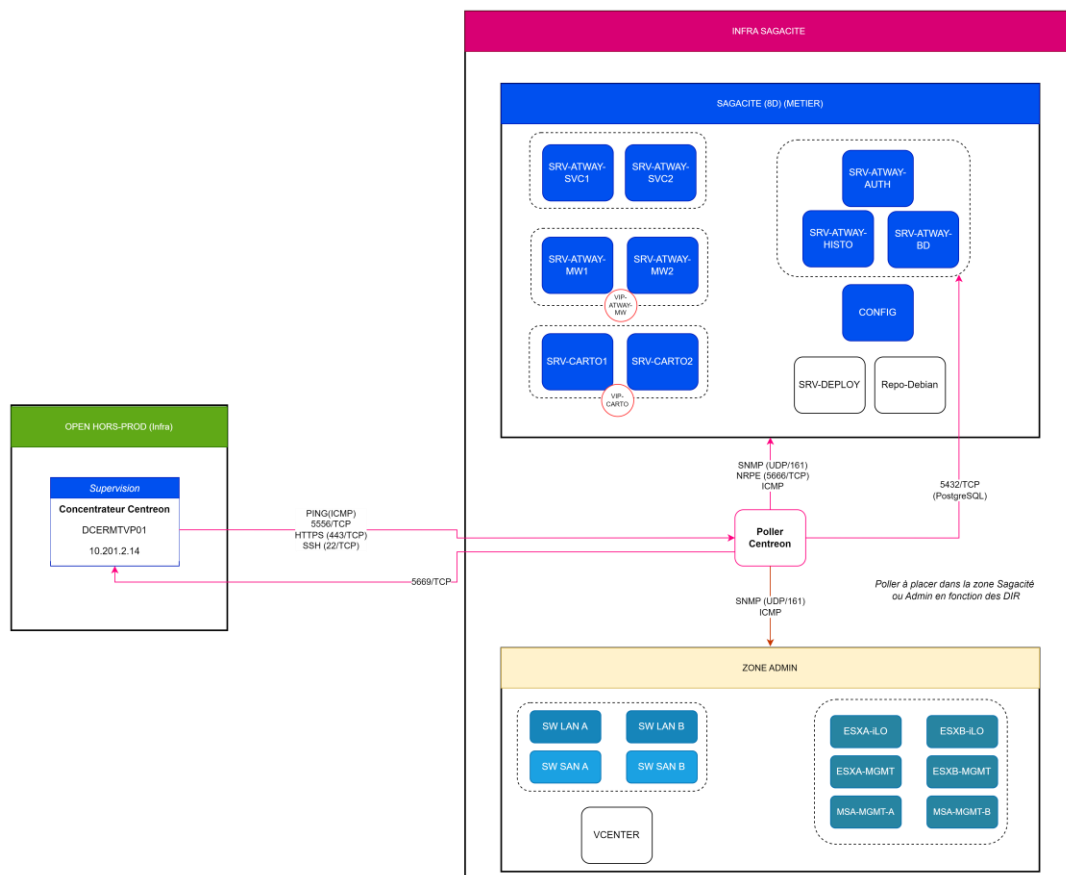


Figure 28 - Vue des flux du Poller Centreon

5.6.3.3 VMs

Centreon central

- Hostname: DCERMTVP01
- IP : 10.201.2.14
- Les Pollers des DIR sont répertoriés dans les fichiers d'inventaire des VM.

5.6.4 Dépôt Debian 11

5.6.4.1 Schéma de principe

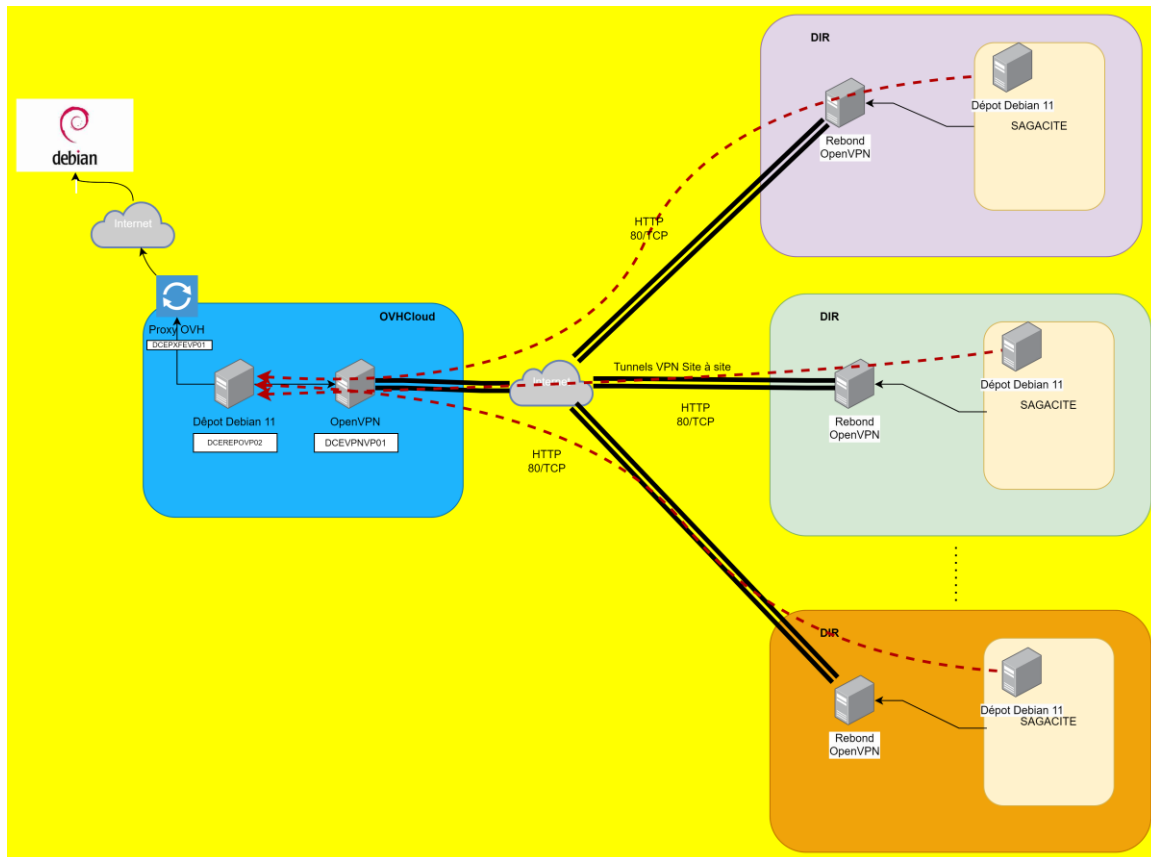


Figure 29 - Vue des flux des dépôts Debian

5.6.4.2 VMs

Dépôt Debian 11 Centralisée OVH

- Hostname: DCEREPOVP02
- IP : 10.201.2.12

Proxy Interne OVH

- Hostname: DCEPXFVP01
- IP : 10.201.2.8

- Les « Dépôts Debian » des DIR sont répertoriés dans les fichiers d'inventaire des VM.

5.6.5 Centralisation des logs de sécurité

Le projet « Centralisation des logs » en cours de définition

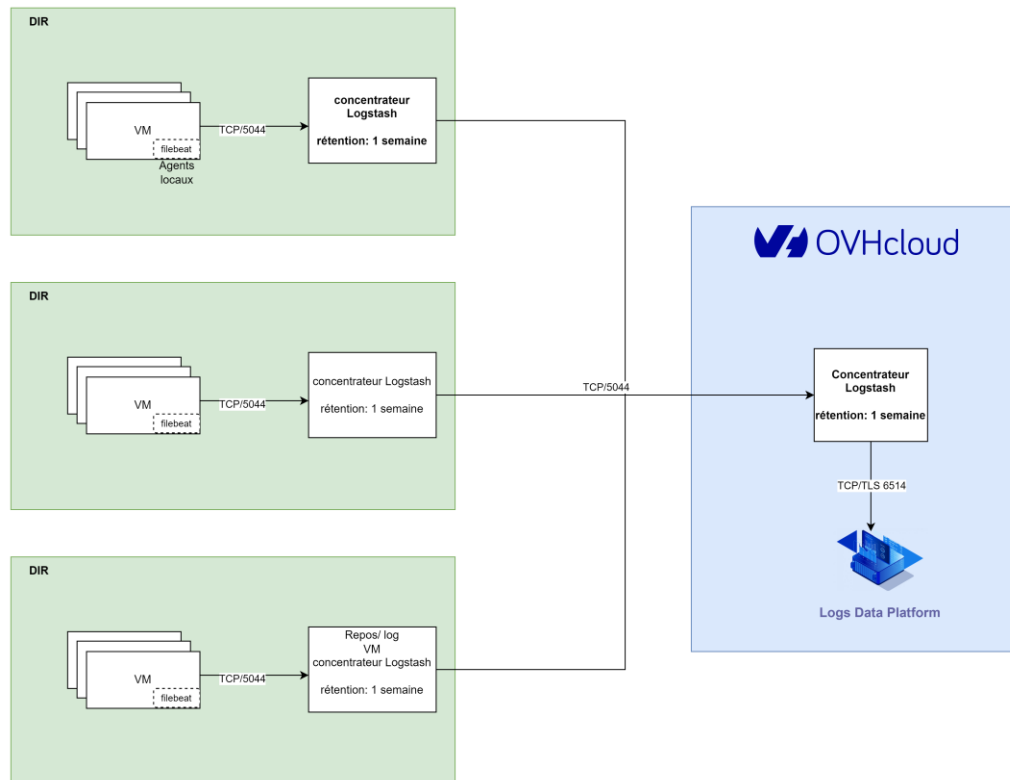


Figure 30 - Schéma de principe de la centralisation des logs

5.6.6 Sauvegarde

Le projet de sauvegarde SAGACITE (3-2-1-1-0) a été conseillé par OPEN auprès de chaque DIR en 2025. En tout état de cause une solution de sauvegarde totale à fréquence régulière est fortement conseillée pour SAGACITE. Cependant les décisions d'adopter une solution de sauvegarde appartiennent à chaque DIR.

5.6.7 Anti-Virus ESET

Il n'y a pas d'anti-virus installé sur la production.

5.6.8 Gestion de l'observabilité

- Le logiciel OpenTelemetry peut-être déployé par la TMA dans le cadre de l'observabilité. La VM « OpenTelemetry » est installé dans le même réseau SAGACITE.
- Le support et l'utilisation est à la charge de la TMA.

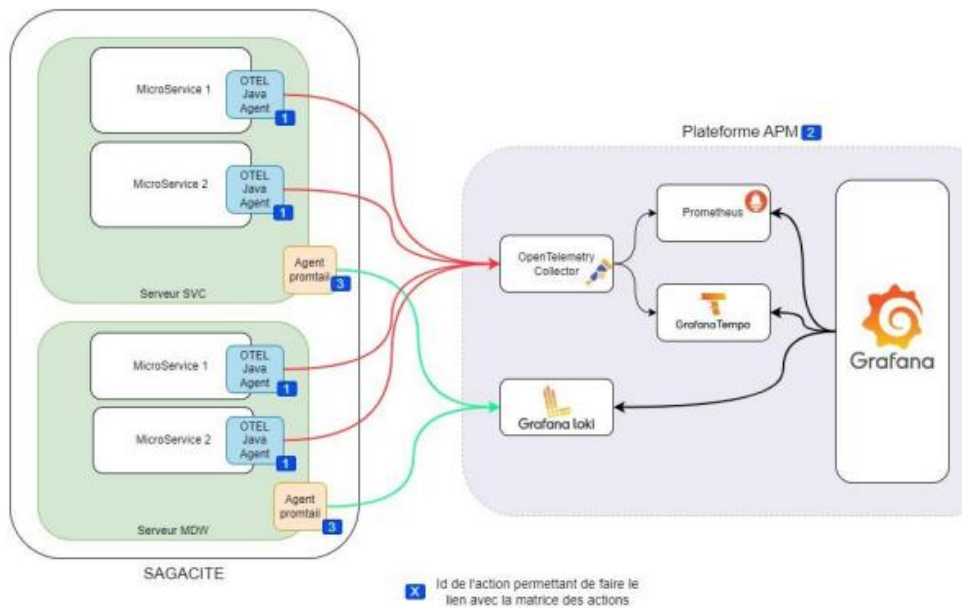


Figure 31 - Composants OpenTelemetry

5.7 Dossier d'exploitation

Se référer au dossier d'exploitation (DEX) pour les chapitres suivants :

- Ordonnancement / Automatisation
- Patch Management
- Règles d'exploitation
- Plages d'ouverture des différents services de l'application