

Annexe 3 : descriptif des environnements

Extrait du dossier d'architecture physique et infrastructure

SOMMAIRE

Table des matières

• I. Contexte.....	4
• II. Exigences.....	4
1. Exigences de sécurité	4
2. Plan de reprise d'activité.....	4
3. Haute disponibilité (HA)	4
4. Stockage des données	4
5. Sensibilité des données.....	4
6. Sauvegardes	5
a. Clusters VMware	5
b. Base de données managées.....	5
c. Sauvegarde DUMP pour PostgreSQL.....	5
d. Sauvegarde Elasticsearch	5
e. Mise à disposition des données anonymisées	5
7. Supervision	5
a. Centreon : offre du prestataire actuel	5
b. ELK Monitoring packagé avec les applications.....	6
8. Puits de logs.....	6
a. Puit de logs : récupération des logs de l'infra	6
b. Logs des bases de données managées par OVHCloud	6
• III. Infrastructure OVHCloud	6
1. Offre OVHCloud.....	6
2. Services managés OVHCloud.....	7
3. Clusters VMware Hosted Private Cloud HDS.....	7
a. Certification HDS	7
b. SLA.....	7
c. Dimensionnement des clusters.....	7
d. Site de PRODUCTION.....	8
e. Sites HORS PRODUCTION	9
4. NSX-T	10
a. Load balancer NSX-T.....	10
5. Backup Veeam.....	11
a. Proxy Backup Veeam.....	11
6. Cloud Public OVH Cloud	11

a. Certification HDS	11
b. SLA OVHCloud	11
c. DataPlaform	11
7. Bases de données managées PostgreSQL	12
a. Cloud Public.....	12
b. Sélection des offres par environnement.....	12
c. SLA OVH Cloud	12
8. Bases de données managées Opensearch	13
a. Besoin.....	13
b. Dimensionnement.....	13
c. Configuration.....	13
9. IPLB – Load balancer régional	13
a. Avantages.....	13
b. SLA OVH Cloud	13
c. Description	13
10.Réseau vRack.....	13
11.Schéma global OVHCloud.....	14
• IV. Architecture technique	14
1. Contexte système	14
2. Environnements	15
a. Environnements applicatifs.....	15
b. Environnements techniques ou de service	15
3. Application SI SIAO	16
4. Messagerie SaaS Alinto	17
5. DNS public	17
6. Accès via VPN	17

I. Contexte

Le SI SIAO est le système d'information de l'Etat en charge de l'orientation de personnes recherchant un hébergement d'urgence, un logement et/ou un accompagnement social.

Il comporte une application hébergée sur une infrastructure OVH pour le compte du Ministère de la Transition écologique et de la Cohésion des territoires (MTECT).

II. Exigences

1. Exigences de sécurité

L'hébergement des données doit avoir la certification HDS.

2. Plan de reprise d'activité



Il sera à définir dans la convention de service.

3. Haute disponibilité (HA)

L'infrastructure doit respecter la disponibilité en cas de panne d'un composant que cela soit au niveau des clusters VMware ou des services hébergés dans OVHCloud.

4. Stockage des données

Les données nécessaires au fonctionnement de l'application SI SIAO sont centralisées dans une base de données PostgreSQL qui est gérée par OVHCloud.

Un cluster ElasticSearch contient des données qui sont indexées à partir de la base PostgreSQL pour faciliter les recherches.

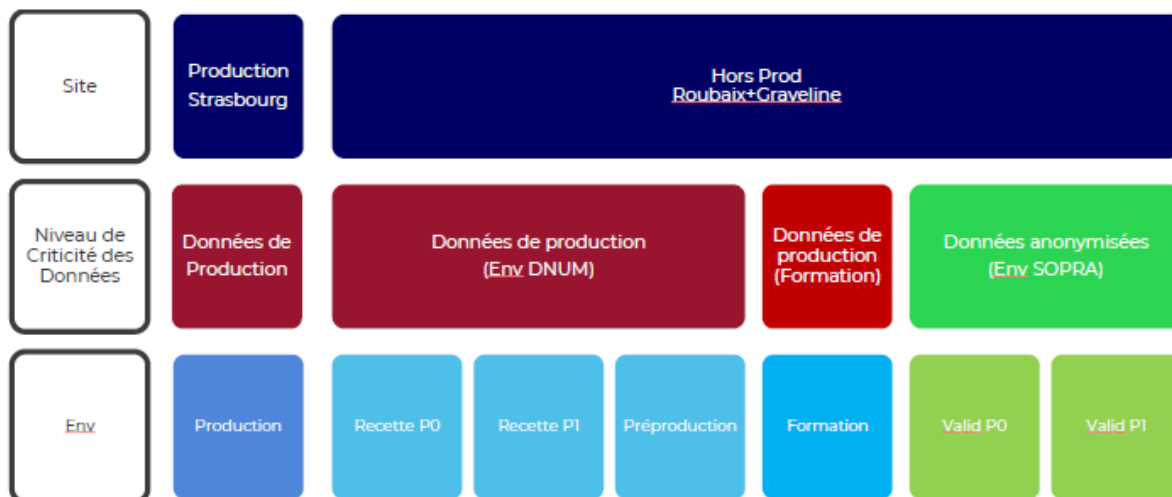
5. Sensibilité des données

Il existe 2 types identifiés de données : données de production et données anonymisées.

Données anonymisées : elles sont utilisées sur les environnements du prestataire de TMA.

En plus de la production, les données hors production PREPROD et RECETTE sont des données de production à une date donnée.

L'environnement de FORMATION possède sa propre base de données indépendante.



6. Sauvegardes

Les méthodes de sauvegarde sont définies en fonction des différents composants et services associés.

a. Clusters VMware

Le service managé « Veeam Managed Backup » est utilisé pour les sauvegardes des VMs.

b. Base de données managées

Les bases de données PostgreSQL OVHCloud effectuent des sauvegardes en continu via la technologie « Point In Time Recovery » (PITR).

La durée de rétention des sauvegardes dépend de l'offre choisie.

c. Sauvegarde DUMP pour PostgreSQL

Des sauvegardes dump sont effectuées 1 fois par jour sur l'environnement de PRODUCTION pour alimenter en données les restaurations des environnements de RECETTE et PREPRODUCTION.

Une sauvegarde annuelle du dump de la base de données de production devra être archivée durant toute la durée du marché.

d. Sauvegarde Elasticsearch

PRODUCTION : sauvegarde toutes les heures ; durée de rétention 15 jours

FORMATION : sauvegarde toutes les heures ; durée de rétention 15 jours.

e. Mise à disposition des données anonymisées

Les données anonymisées sont générées et mises à disposition une fois par semaine ou sur demande du prestataire de TMA.

7. Supervision

a. Centreon : offre du prestataire actuel

Dans chaque région OVHCloud, un satellite de supervision Centreon est installé afin de collecter les données des serveurs et de les remonter aux serveurs centraux de la solution de supervision du prestataire actuel, par le biais de tunnels site à site.

Les satellites de supervision sont utilisés pour envoyer les alertes d'indisponibilité, d'avertissements (warning) et alertes critiques à l'outil de ticketing centralisé du prestataire actuel.

Une solution de ce type sera à mettre en œuvre par le nouveau titulaire du marché.

b. ELK Monitoring packagé avec les applications

Dans chaque environnement, une VM ELK Monitoring est installée et utilisée pour superviser les VMs (CPU / RAM / IO) et les composants applicatifs.

Les agents filebeat sont installés sur toutes les VMs applicatives.

Les composants VMs, et agents sont déployés via les scripts Ansible.

8. Puits de logs

a. Puit de logs : récupération des logs de l'infra

Dans chaque région OVHCloud, un serveur de logs est installé afin de collecter les logs des serveurs à l'exception des VMs monitorées par les ELK Monitoring (qui sont exclus de ce puit de log)

Les agents Filebeat et logstash sont installés sur chaque VM et remontent les logs sur les serveurs de logs.

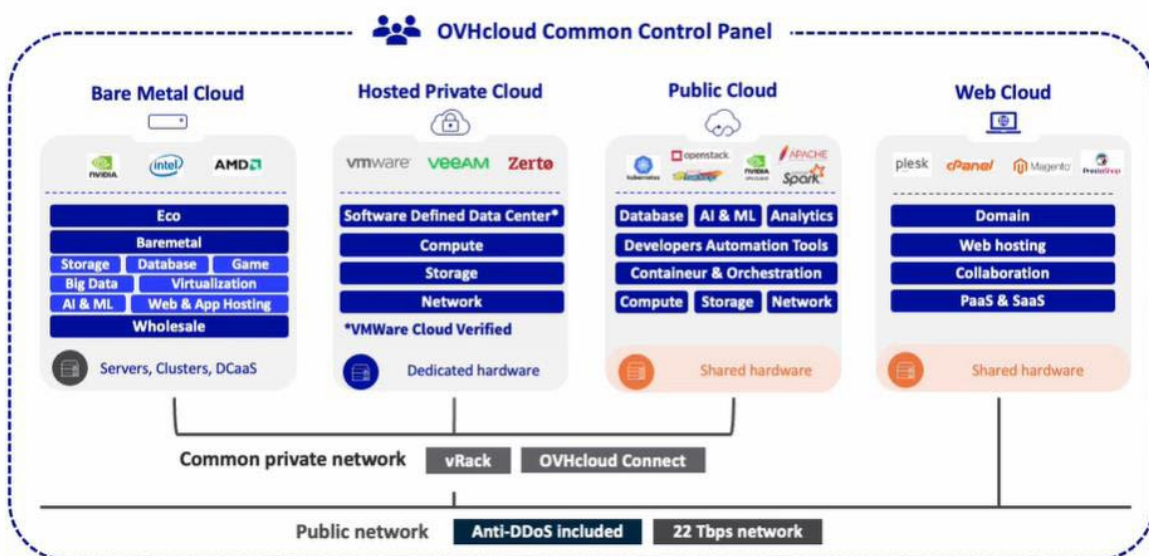
b. Logs des bases de données managées par OVHCloud

Les logs des bases de données managées doivent être accessibles et consultables par la DNUM.

III. Infrastructure OVHCloud

1. Offre OVHCloud

OVHcloud offers 4 product universes depending on your needs



Les services utilisés sur le projet sont :

- Hosted Private Cloud
 - VMware on OVHCloud
 - NSX-T
 - Backup Veeam, sauvegardes pour VMware
 - IPLB (load Balancer IP, multi régions)
- Public cloud
 - Bases de données PostgreSQL
 - Object Storage
 - DataPlatform
- Réseau
 - vRack
 - NSX-T

2. Services managés OVHCloud

Les services managés utilisés actuellement sur le projet sont :

- Backup Veeam, utilisé pour les sauvegardes VMware
- IPLB (loadbalancer IP, multi régions)
- Bases de données PostgreSQL
- DataPlatform

3. Clusters VMware Hosted Private Cloud HDS

a. Certification HDS

Les clusters sont certifiés HDS.

b. SLA

Le SLA OVHCloud pour les clusters VMware est de 99.95%.

c. Dimensionnement des clusters

i. Nombre minimum de hosts

Le cluster ElasticSearch est composé de 3 VMs (hors recette/formation). Si une VM est mise hors service, le cluster ElasticSearch continue de fonctionner.

Il est donc nécessaire d'avoir 3 hosts minimum pour héberger chaque VM ElasticSearch de manière isolée sur un nœud dédié.

ii. Dimensionnement en cas de défaillance d'un host

Le dimensionnement du cluster VMware (nombre de nœuds, dimensionnement CPU/RAM) doit prendre en compte les ressources disponibles après la défaillance d'un nœud.

Par exemple, la mémoire disponible sur 2 nœuds doit être suffisante pour héberger l'ensemble des VMs après redémarrage des VMs hébergées précédemment sur le nœud défaillant.

Pour la production, en nominal, le ratio vCPU/pCores (pcores = nombre de cores physiques) doit être aux environs de 3 (recommandation VMware pour la production).

iii. Dimensionnement au « plus juste »

Le coût d'un Host n'étant pas négligeable, il est nécessaire de ne pas surdimensionner les Hosts.

iv. Tableau des consommations théoriques du cluster de PRODUCTION

Le tableau ci-dessous décrit les besoins en ressources CPU/RAM des Vms hébergées sur le cluster de production en fonction de leur profil.

Nb VMs	24
Nb RAM (Go)	222
Nb vCPU	82

Dimensionnement du cluster :

Nb Hosts	Dimensionnement d'un nœud	Panne d'un host : 2 nœuds	Nominal : 3 nœuds
CPU	12	24	36
RAM	96	192	288
vCPU / pCore	N/A	3.42	2.28
%RAM réservé théorique	N/A	116 %	77 %

v. Tableau des consommations théoriques du cluster HORS PRODUCTION

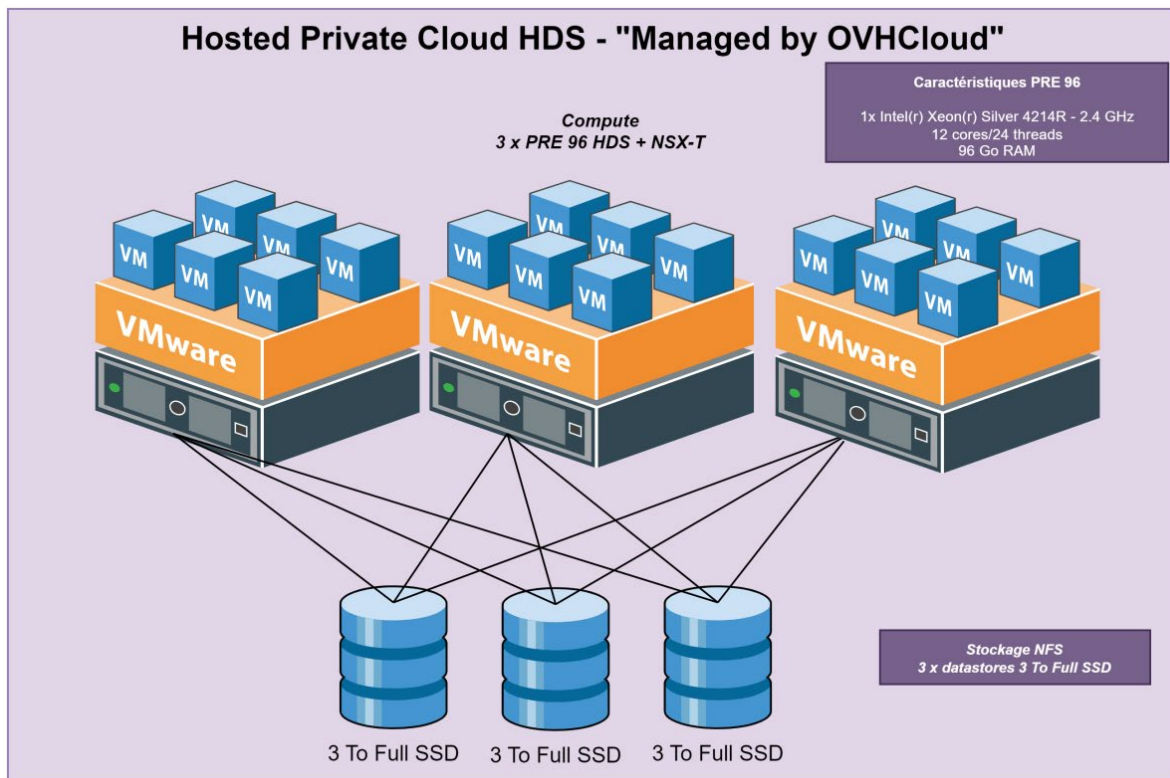
Nb VMs	77
Nb RAM (Go)	578
Nb vCPU	246

Dimensionnement du cluster :

Nb Hosts	Dimensionnement d'un nœud	Panne d'un host : 2 nœuds	Nominal : 3 nœuds
CPU	32	64	96
RAM	384	768	1152
vCPU / pCore	N/A	3.84	2.56
%RAM réservé théorique	N/A	75 %	50 %

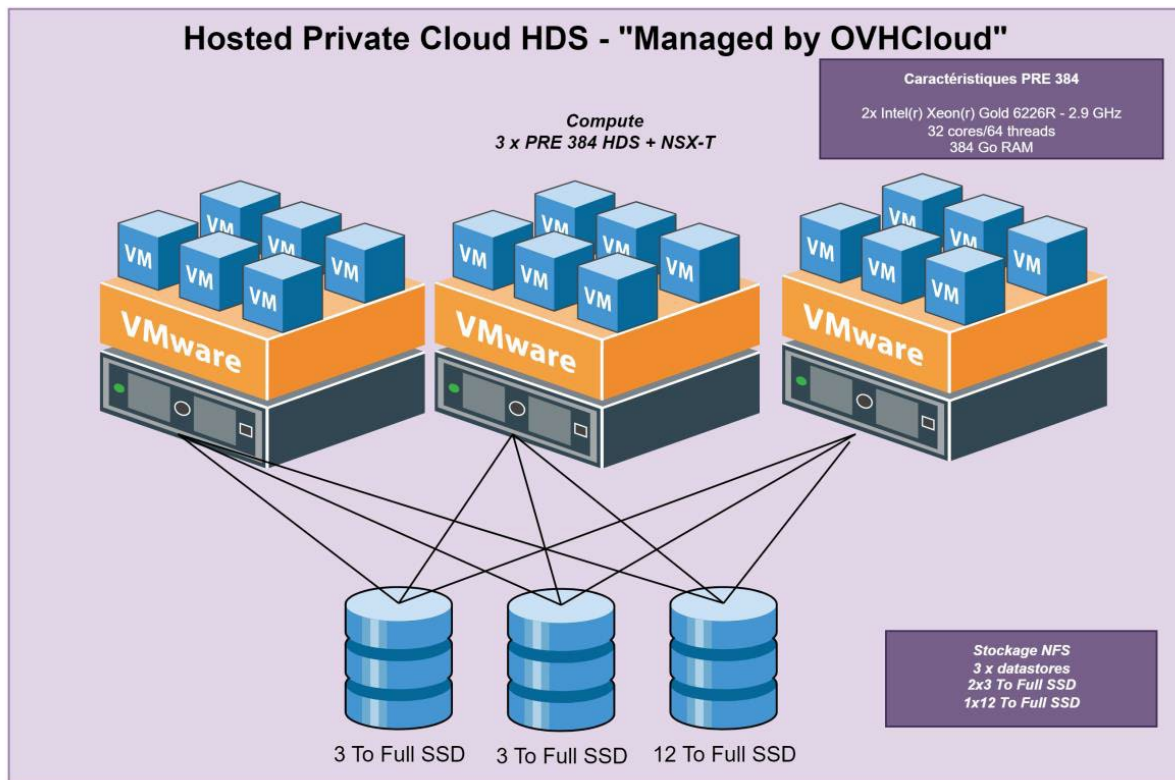
d. Site de PRODUCTION

Le cluster est constitué de 3 nœuds ESX PRE96 et de 3 datastores de 3 To chacun.



e. Sites HORS PRODUCTION

Le cluster HORS PRODUCTION est constitué de 3 nœuds PRE 384 HDS et de 3 datastores NFS (2x 3To et 1x12 To).



4. NSX-T

NSX est une solution de gestion de réseau logicielle Software Defined Networking (SDN) fournie par VMware. OVH Cloud propose ce service en remplacement de NSX-v dans son offre VMware on OVHCloud. Deux hôtes sont déployés avec, sur chacun d'eux, une machine virtuelle dédiée à NSX, ce qui permet une redondance en cas de défaillance d'un des hôtes.

Le cœur de réseau de l'application du SI SIAO est géré par la couche NSX-T hébergée dans chacun des deux clusters VMware.

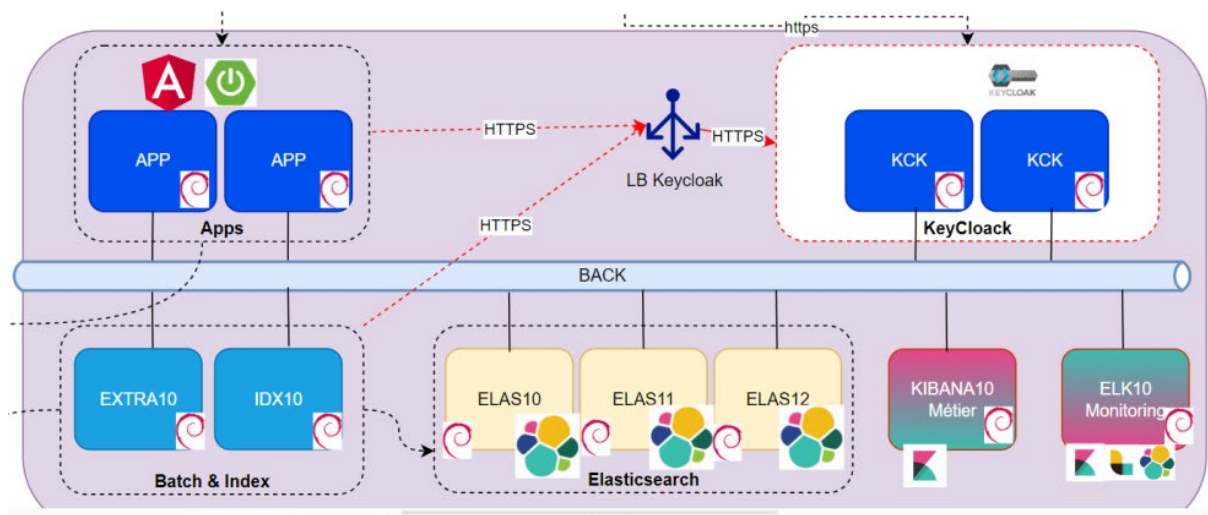
Plusieurs services d'OVHCloud sont utilisés en mode PaaS tels que le load balancer régional et les bases de données PostgreSQL managées. Il est nécessaire que la couche réseau NSX-T puisse faire communiquer ces composants avec les VMs applicatives ou d'infrastructure. Les réseaux sont donc de type VLAN et non de type segment (NSX-T) pour s'assurer de l'interfaçage avec les services du Cloud Public d'OVHCloud.

a. Load balancer NSX-T

Dans chaque cluster VMware un LB de NSX-T est utilisé en interne pour permettre aux applications SI SIAO de communiquer aux VMs Keycloak.

Par défaut, chaque « environnement SISIAO » possède :

- Sa propre IP associée au LB 192.168.0.XXX (le dernier octet XXX correspond au numéro de VLAN du réseau BACK SI SIAO)
- Son propre Pool de serveurs SI SIAO
- Un routage et des règles firewall autorisant les flux HTTPS (Niveau 4) de communiquer entre les différents composants (LB sur le T1 et entre les VMs).



5. Backup Veeam

a. Proxy Backup Veeam

Pour prévenir les blocages de VMs pendant les sauvegardes, il est nécessaire de prendre certaines mesures.

Ces blocages sont dus au fait qu'un seul serveur de sauvegarde doit gérer plusieurs VMs avec des tâches de sauvegarde.

Il est donc suggéré d'ajouter suffisamment de BackupProxies pour répartir la charge de travail lors de l'exécution des tâches de sauvegarde.

Il est également recommandé d'avoir une instance de serveur de sauvegarde/backup proxy pour chaque hôte de l'infrastructure VMware.

Ces procédures ne sont pas documentées. Il est indispensable d'utiliser les API pour augmenter le nombre de BackupProxies, une opération qui peut prendre plusieurs heures.

En fonction du site, le niveau de service est différent :

PRODUCTION : Offre Advanced

HORS PRODUCTION : Offre Standard

6. Cloud Public OVH Cloud

a. Certification HDS

L'offre Public Cloud est certifiée HDS.

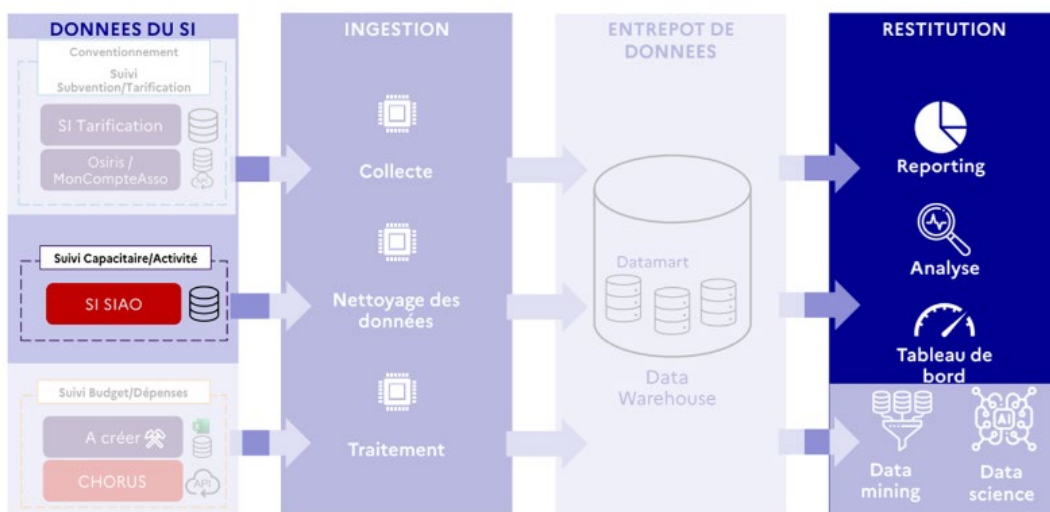
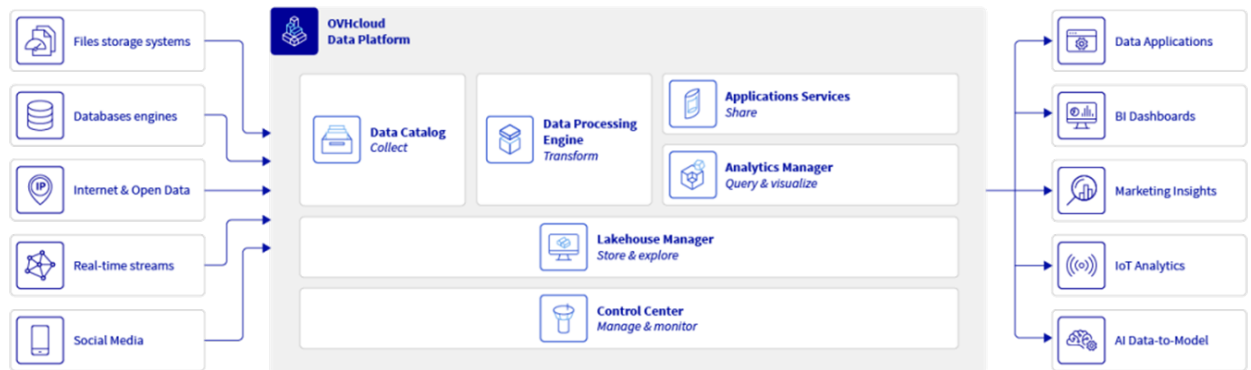
b. SLA OVHCloud

Les SLA sont définis en fonction du lien suivant : [Public Cloud Service Level Agreement](https://www.ovhcloud.com/fr/public-cloud/service-level-agreement) (ovhcloud.com).

Pour des services comme l'IPLB ou les Bases de données managées il faut se référer à leur propre SLA.

c. DataPlaform

La plateforme de DataViz du SI SIAO est basée sur la solution DataPlaform OVH Cloud.



7. Bases de données managées PostgreSQL

a. Cloud Public

L'offre de service « Bases de données managées » fait partie intégrante de l'offre Cloud Public.

Cf. PostgreSQL : [Bases de données Open Source | OVHcloud](#)

b. Sélection des offres par environnement

Environnement	Modèle	Nb nœuds	CPU	RAM	Stockage
PRODUCTION	Business DB1 60	2	16	60	1.28 To
PREPROD-PRA	Business DB1 60	2	16	60	1.28 To
FORMATION	Essential DB1 15	1	4	15	320 Go
RECETTE P0	Essential DB1 30	1	8	30	640 Go
RECETTE P1	Essential DB1 30	1	8	30	640 Go
VALID P0	Essential DB1 30	1	8	30	640 Go
VALID P1	Essential DB1 30	1	8	30	640 Go

c. SLA OVH Cloud

Le SLA OVHCloud pour la production est de 99,9% liée à l'offre Business.

8. Bases de données managées Opensearch

a. Besoin

Les bases de données PostgreSQL ne permettent pas l'exportation et l'accès aux logs directement. Il est nécessaire de passer soit par les API pour récupérer les dernières logs, soit d'utiliser les bases de données Opensearch pour stocker leurs logs via « l'intégration de service ».

b. Dimensionnement

Le besoin d'envoyer les logs vers OpenSearch n'est pas critique, il n'est pas nécessaire d'avoir de la HA pour ce service.

Le besoin de traitement qui est uniquement limité par des requêtes sur demande sur les logs de manière ponctuelle. Il n'est pas nécessaire de prendre des machines puissantes en CPU/RAM.

L'infrastructure étant positionnée dans deux régions distinctes, une instance OpenSearch est requise par site.

c. Configuration

PRODUCTION : Essential DB1-4

HORS PRODUCTION : Essential DB1-4

9. IPLB – Load balancer régional

Le load balancer régional est utilisé pour partager la même adresse IP entre les 2 régions.

a. Avantages

Le Load-Balancer va gérer l'ensemble des URL publiques des deux régions.

« Let's Encrypt » est utilisé pour générer les certificats TLS est géré nativement.

En cas de PRA, il permettra de basculer l'URL de production vers le site de secours, (environnement de préproduction/PRA)

b. SLA OVH Cloud

Le SLA pour la production est de 99,9% (Offre Pack 2).

c. Description

Le service OVHcloud Load Balancer est composé de 4 parties élémentaires :

- les frontends,
- les fermes de serveurs et leurs serveurs,
- les routes avancées entre les Frontends et les Fermes de serveurs,
- les certificats SSL/TLS permettant de chiffrer les connexions TCP et/ou HTTP.

Un frontend est créé pour écouter sur le port 80, tandis qu'un autre écoute sur le port 443 avec un certificat SSL/TLS généré par « Let's Encrypt ». Ces frontends sont configurés pour diriger leur trafic vers une ou plusieurs fermes HTTP en fonction des règles de routages. Chaque ferme peut disposer d'un ou plusieurs serveurs, selon la configuration choisie / adaptée.

10. Réseau vRack

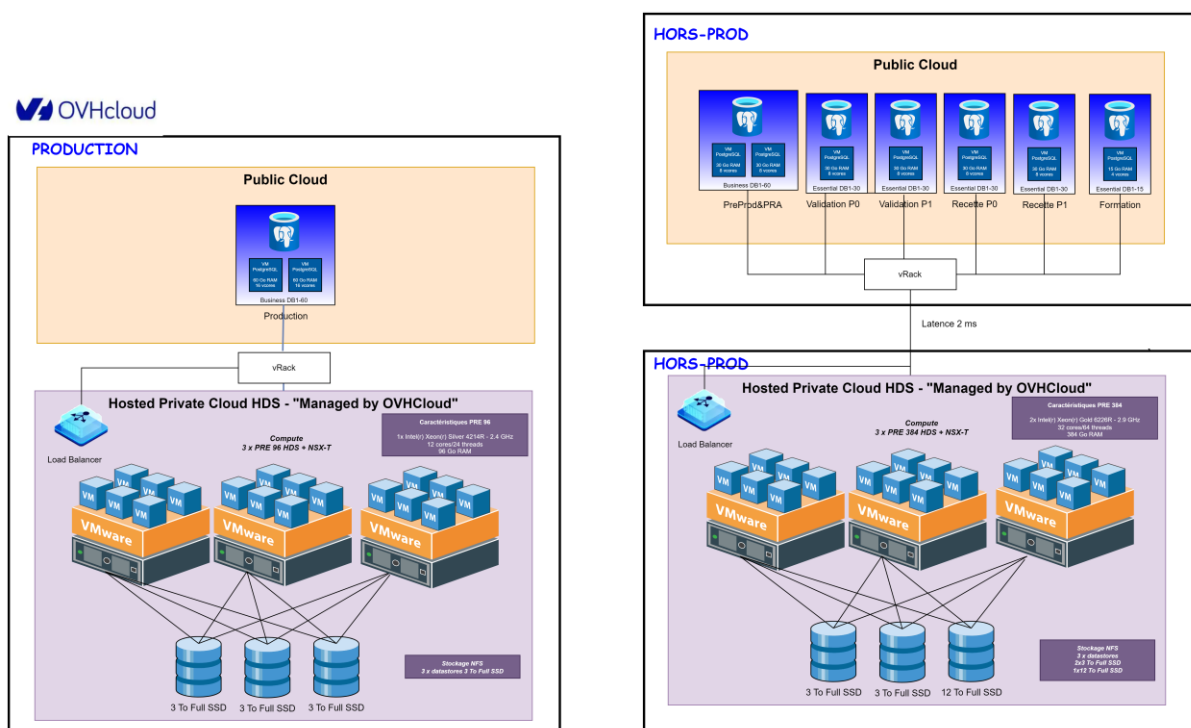
Un vRack est une infrastructure gérée par OVHCloud. Il est possible de créer jusqu'à 4000 VLAN au sein d'un même vRack. vRack utilise le niveau 2 de la couche TCPIP.

Le vRack est utilisé via les VLANs pour permettre la communication entre les différents composants d'OVHcloud tel que les clusters VMware avec les Bases de données managées installées dans le Cloud Public ou encore avec les Load-Balancers.

vRack permet la communication entre plusieurs sites d'OVHcloud en attribuant simplement un même numéro de VLAN aux sites distant.

Un seul vRack est utilisé pour l'ensemble du projet SI SIAO.

11. Schéma global OVHcloud

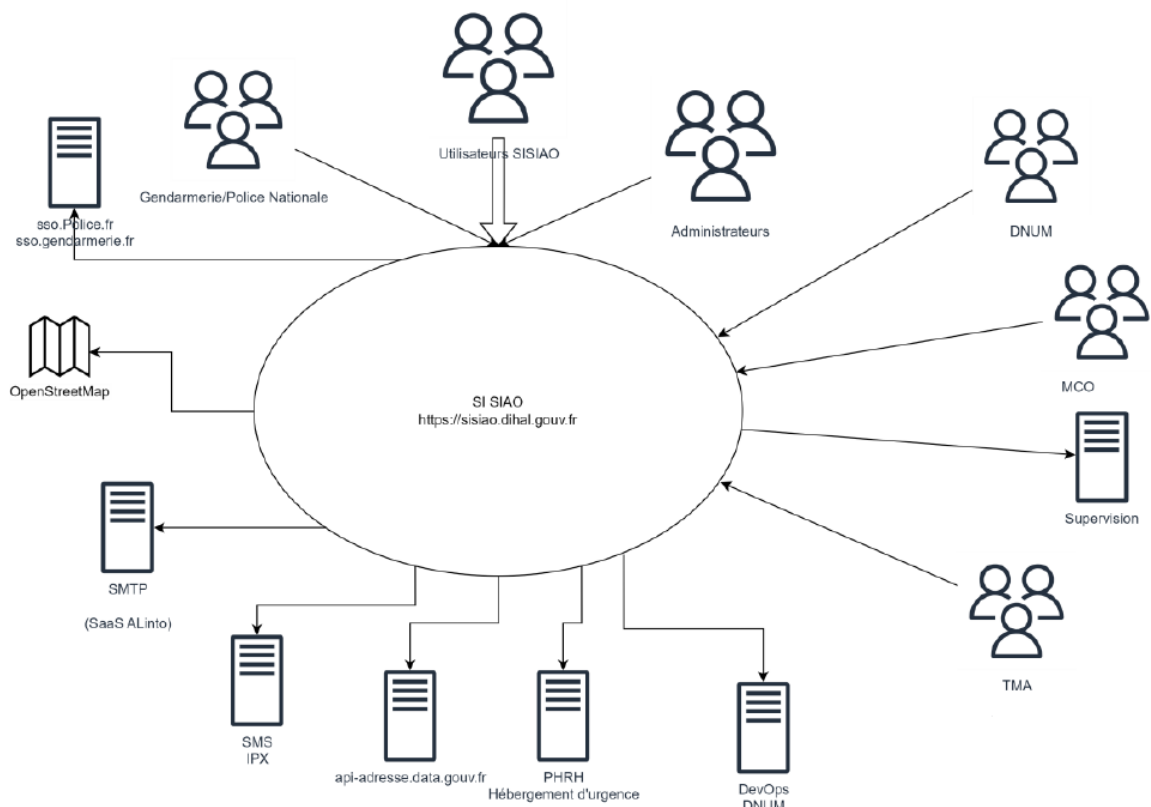


IV. Architecture technique

1. Contexte système

Le système contextuel représente l'ensemble du système en tant qu'objet ou processus unique et identifie les interfaces entre le système et les entités externes.

Le schéma ci-dessous décrit les interactions du système (ici le portail SI SIAO) avec les acteurs humains (utilisateurs, administrateurs) ou des systèmes logiques (GitLab DNUM, la supervision Infogérant, ...).



2. Environnements

a. Environnements applicatifs

8 environnements applicatifs

Environnement	Description	Données applicatives
PRODUCTION	Environnement de production	Production
PREPROD-PRA	Environnement de préproduction et PRA	Production
FORMATION	Environnement de formation permettant de réaliser les formations des futurs utilisateurs du système	Formation
RECETTE P0	Environnement de recette de la maintenance corrective	Production
RECETTE P1	Environnement de recette évolutive	Production
VALID P0	Environnement de validation TMA maintenance corrective	Anonymisée
VALID P1	Environnement de validation TMA maintenance évolutive	Anonymisée
BAC A SABLE	Environnement pour les tests d'accrochage éditeurs	Anonymisée

b. Environnements techniques ou de service

2 environnements de service

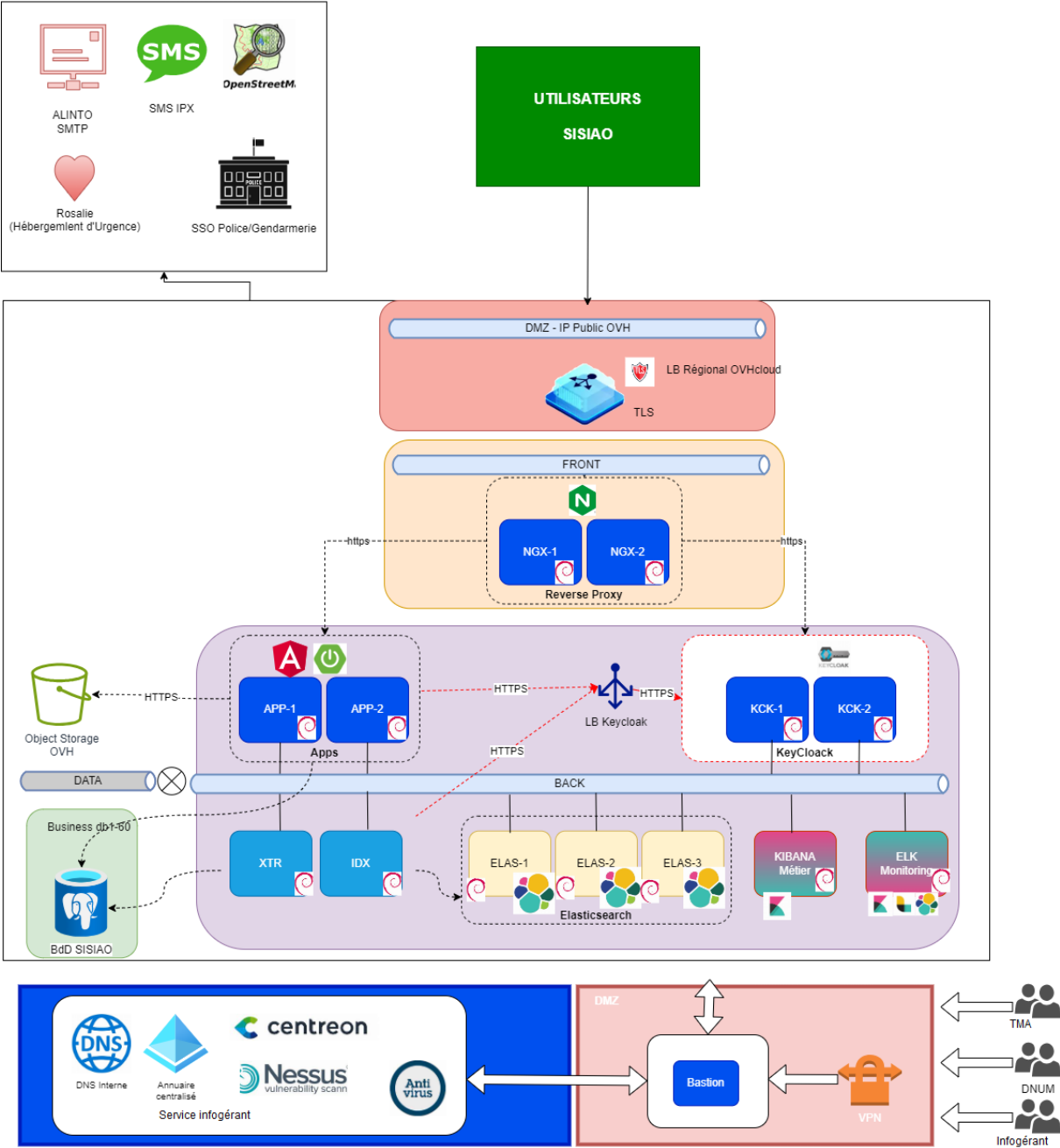
Environnement	Description	Données applicatives
---------------	-------------	----------------------

SVC-INFOGERANT	Environnement de service utilisé par l'infogérant	N/A
SVC-SISIAO	Environnement de service utilisé par le MTECT ou par la TMA	N/A

3. Application SI SIAO

Le schéma ci-dessous décrit les briques de l'architecture applicative de production. Les principaux composants d'infrastructure y sont représentés.

Les briques applicatives ne sont pas représentées ici.

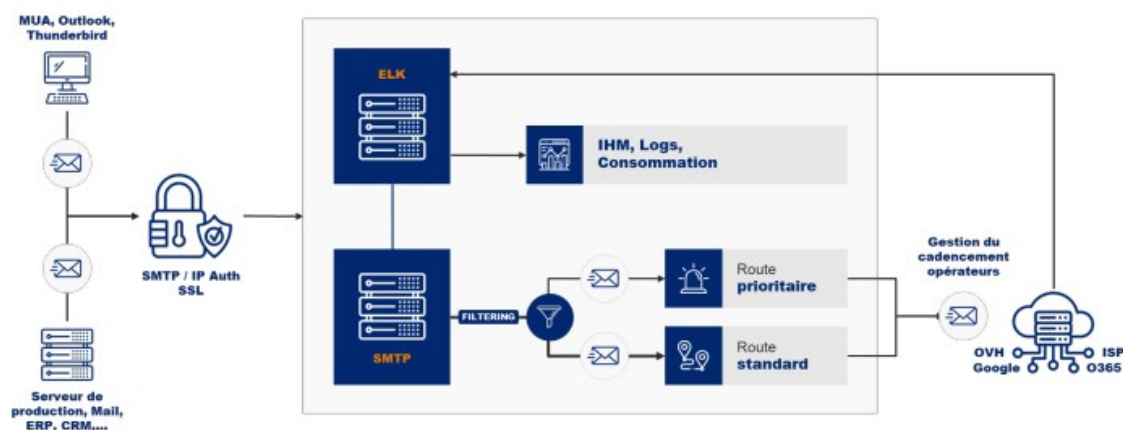


4. Messagerie SaaS Alinto

Pour les besoins métiers, il est nécessaire que la plateforme puisse émettre des courriels à destination des utilisateurs du SI SIAO.

Seul les environnements PRODUCTION, FORMATION (et PREPROD-PRA configuré en mode PRA) doivent être capables d'émettre des courriels.

Le choix d'architecture est de s'appuyer sur un service externe via la société ALINTO



5. DNS public

Le sous-domaine sisiao.dihal.gouv.fr est géré par l'infogérant et une délégation est mise en place côté des DNS par la DIHAL.

6. Accès via VPN

Les accès aux interfaces de monitoring, dashboards, outillages et accès SSH sont protégés par des VPN.