Connaître les fonctionnalités Flexible Engine

Juin 2020

orange™ Business Services

1.1 Les services de puissance informatique

1.1.1 Elastic Cloud Server (ECS)

Les Serveurs Cloud Elastiques (ECS) sont des Machines Virtuelles (VM) informatiques. Ce service, disponible sur l'ensemble des Zones de Disponibilité, propose des machines virtuelles en self-service. L'Utilisateur peut démarrer, arrêter, redimensionner les VM en utilisant la Console Flexible Engine ou bien en utilisant l'API ECS.

Les Serveurs Cloud utilisent un disque système basé sur le service de volume élastique EVS, et pour certains gabarits un disque local est également inclus. L'ECS est facturé :

- lorsqu'il est allumé pour les gabarits n'incluant pas de disque local,
- y compris lorsqu'il est éteint et jusqu'à sa suppression totale pour les gabarits incluant un disque local.

Les caractéristiques techniques de chaque gabarit sont disponibles dans la Console Flexible Engine.

Les principes de facturation sont précisés dans la Fiche Tarifaire.

1.1.2 Serveurs Bare Metal (BMS)

Un BMS (Bare Metal Server) est un serveur physique qu'il est possible de souscrire et de lancer depuis la console Flexible Engine. Ce serveur est entièrement dédié au Client afin d'installer des applications clés ou pour optimiser des licences de base de données Oracle par exemple. Le client peut associer à ce server physique d'autres services Flexible Engine comme un cloud privé virtuel (VPC), des images OS (IMS), du stockage ou de réseau. Disposant d'une double carte réseau (Multi-NIC), le BMS peut se connecter à deux réseaux.

1.1.3 Auto-scaling

L'auto-scaling utilise des politiques d'auto-scaling prédéfinies pour mettre automatiquement à l'échelle les ressources du service en fonction des besoins remontés par le monitoring par ajout de VM ou destruction de VM dans un groupe.

L'auto-scaling fonctionne entre-autre avec l'Elastic Load Balancer (ELB) pour ajuster automatiquement le nombre d'ECS membres du Load Balancer nécessaires pour traiter la charge et la répartir.

Le Client peut configurer des tâches de mise à l'échelle programmées et périodiques, assurer le suivi des politiques, et définir des limitations de capacité avec des groupes d'auto-scaling afin de permettre à la fonction d'auto-scaling d'augmenter ou de réduire automatiquement le nombre d'instances de serveur cloud élastique (ECS).

1.1.1 Auto-récupération de VM (VM Auto-recovery)

Lorsque la Fonctionnalité auto-récupération de VM est activée, le système migre automatiquement les VM vers un autre serveur lorsque le serveur physique sous-jacent tombe en panne ou redémarre de façon anormale. La nouvelle VM est un clone de la VM défectueuse.

L'activation de la Fonctionnalité se fait au moyen de la console de monitoring Cloud Eye Services (CES), et est limitée aux gabarits compatibles.

1.1.2 Service de gestion des images (IMS)

Une image est utilisée pour créer des ECS avec un système d'exploitation (OS) et des applications préinstallés ou bien inversement pour sauvegarder un ECS sous forme d'image.

IMS fournit une console de gestion Web flexible afin de gérer les images IMS. Le Client peut créer des images personnalisées afin de déployer rapidement ses applications et modifier les sauvegardes.

IMS permet au Client :

- d'utiliser des images publiques avec des systèmes d'exploitation installés.
- de créer des ECS en utilisant des images disponibles dans une Région.
- de créer une image privée à partir d'un ECS existant.
- d'afficher des détails sur une image privée.

- de supprimer une image privée existante.
- de télécharger un fichier image et l'enregistrer comme image privée.
- d'exporter une image privée dans un format spécifique.
- de partager une image privée avec d'autres Utilisateurs.

Flexible Engine est pré-approvisionné d'images publiques disponibles via IMS. Orange Business Services met à jour ces images de manière régulière avec les dernières versions stables. La liste est disponible sur la console et pourra évoluer régulièrement.

IMS supporte aussi l'importation d'images privées avec la compatibilité de système d'exploitation suivant. La liste est disponible sur la console et pourra évoluer régulièrement. L'importation et l'utilisation est sous la responsabilité de l'Utilisateur.

Le Client peut importer une image privée vers le Cloud public. L'image est alors disponible dans le service IMS de votre Tenant.

De plus, les instantanés d'ECS sous forme d'image servent de sauvegarde, ce qui permet de récupérer rapidement les ECS si l'infrastructure locale du Client fait l'objet d'une défaillance.

Les images privées pouvant être exportées comprennent celles que le Client a téléchargées sur le système ou établies à partir des ECS créés à partir des images publiques gratuites.

Les images exportées peuvent être au format VMDK, QCOW2, VHD ou ZVHD.

Les images publiques peuvent porter des licences d'éditeurs tiers (Windows, Redhat, Suse). Ces licences font l'objet d'une facturation.

1.1.3 Container as a Service (CCE)

L'offre de Conteneurs as a Service est un service de conteneurs déployables en haute disponibilité et de façon élastique.. S'appuyant sur l'orchestrateur Kubernetes pour déployer et manager les applications Docker, le service CCE (Container Cloud Engine) met également à disposition un outil d'orchestration graphique permettant de créer et déployer des applications. Le service supporte uniquement les applications Docker dites 'stateless'.

Fonctionnalités du service :

- **Gestion des applications :** permet aux utilisateurs de créer, mettre à jour, supprimer et demander des applications de conteneurs Docker. Il permet également le management des modèles d'applications et de composants.
- **Orchestration graphique** : Permet de définir la topologie et le déploiement de l'application par simple glisser/déposer.
- **Gestion d'images privées** : Permet aux Utilisateurs d'uploader, de mettre à jour et de supprimer leurs images privées.
- **Management de cluster** : Permet de créer, mettre à jour et supprimer les clusters de conteneurs et d'ajuster leur taille en ajoutant des nœuds en fonction des besoins.
- **Elasticité automatique** : Permet de faire évoluer la taille des clusters en fonction de règles définies sur la charge applicative.
- **Monitoring et gestion des logs** : Possibilité de monitorer les applications sous forme de graphiques (charge CPU, utilisation mémoire) et de gérer ou télécharger ses logs.

Pour chaque conteneur Docker, le Client peut configurer la taille de la mémoire et caractéristiques de la CPU

Le nombre total de nœuds pouvant être créés sur les clusters de chaque Utilisateur est aussi limité par le quota de ressources (ECS, VPC etc.) de l'Utilisateur.

1.1.4 Service de Cloud dédié (DEC)

Le service de "Cloud Dédié" permet de provisionner un pool d'hyperviseurs isolés dans le Cloud public. De cette manière, le Client bénéficie au sein de son Tenant de serveurs physiques dédiés pour construire ses propres groupes de ressources virtuelles, connectées au stockage distribué et à ses réseaux virtuels.

Le Client peut connecter son « Cloud dédié » à des réseaux virtuels, à des ressources de stockage également dédiées ou des ressources de stockage distribuées (EV, OBS) et utiliser les autres services Flexible Engine pour créer des ECS, charger des images OS publiques ou privées (IMS)…, établir des sauvegardes (VBS)…

1.2 Les services de stockage

1.2.1 Le Stockage Bloc Elastique (EVS)

Stockage bloc dit « persistant » hautement disponible. Il est utilisé comme disque système pour les serveurs cloud mais également comme disques de données additionnels ajustables par l'Utilisateur.

Orange Business Services propose différentes classes de stockage, I/O standard et I/O performant laissant au Client le choix en fonction de ses besoins. Le Client dispose de la possibilité d'étendre la taille de ses volumes à sa convenance. Ces volumes bénéficient également du service de sauvegarde (VBS) permettant de sauvegarder les données du Client directement sur le stockage objet d'Orange Business Services.

Les volumes sont hautement disponibles et sont utilisés comme partition de démarrage des serveurs ou encore comme des périphériques de stockage de données additionnelles.

Les volumes blocs sont disponibles en deux gammes de performance :

- gamme standard utilisant des disques SATA
- gamme high I/O utilisant des disques SSD

1.2.1.1 Description

EVS fournit un stockage en bloc permanent, très performant. Le Client crée des disques EVS et les rattache aux ECS pour que les ECS puissent accéder et utiliser les disques.

EVS :

- supporte différents types de disque EVS, comprenant les disques EVS I/O ultra-performants et I/O classiques.
- permet d'étendre la capacité du disque EVS de manière élastique pour répondre aux besoins croissants en capacité de stockage.
- fonctionne avec Volume Backup Service (VBS) pour fournir le service de sauvegarde.
- fournit un disque système d'une capacité comprise entre 1 Go et 32To, et un disque de données d'une capacité comprise entre 10 Go et 32 To.

1.2.1.2 Caractéristiques

Elément	I/O classique	I/O ultra-performant
Capacité maximale d'un disque unique	32 To	32 To
IOPS max. par disque EVS	1000	20 000
Sortie max. par disque EVS	40 Mo/s.	320 à 350 Mo/s.
Délai de réponse moyen	entre 10 ms et 15 ms	entre 1 ms et 3 ms

Le service de stockage bloc EVS est facturé à l'usage.

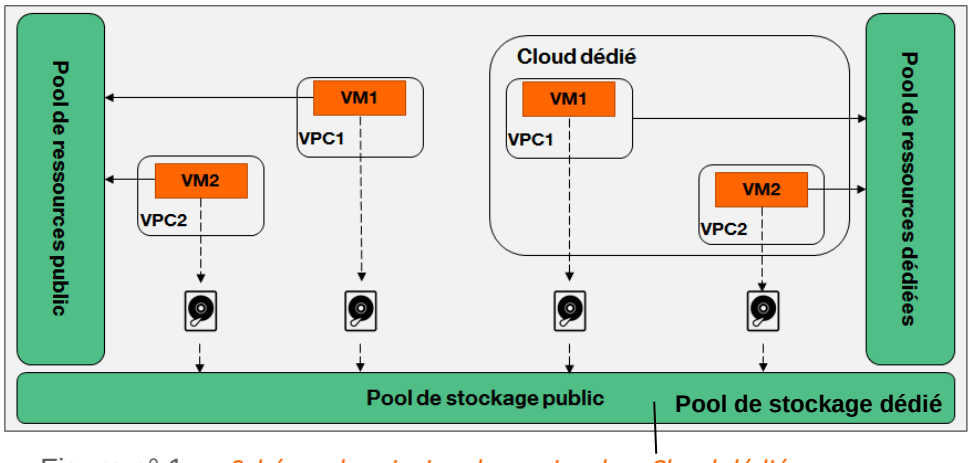


Figure n° 1: *Schéma de principe du service de « Cloud dédié »*

1.2.2 Le Stockage Objet (OBS)

Stockage objet accessible sur Internet en https via requêtes APIs REST OBS et compatible Amazon Simple Storage (S3), utilisé pour du stockage à long terme de gros volumes de données.

L'architecture mise en place est conçue pour être résistante aux pannes :

- maintien de l'intégrité des données par vérification des checksums
- autoréparation des défaillances à partir d'au moins une des réplications de données
- remplacement, suppression et ajout de disques et serveurs à chaud
- mise à jour, patches et montées de version sans interruption de service

De nombreuses solutions de partage, sauvegarde, archivage sont d'ores et déjà disponibles en plug-n'-play avec l'API RESTFul Amazon S3. Aussi, les sauvegardes des instances, appelées « instantanés », et les images d'OS cloud importées dans les projets seront sauvegardées dans le stockage objet.

OBS offre trois classes de stockage : standard, chaud et froid. OBS Standard se caractérise par une latence d'accès faible et un débit élevé. OBS Warm convient au stockage de données rarement consultées, mais qui nécessitent un accès rapide. OBS Cold est orienté vers l'archivage de données et la sauvegarde à long terme avec un accès rare aux données.

La facturation du service OBS est basée sur l'utilisation du stockage et les requêtes exécutées, en fonction des classes de stockage.

1.2.3 Le stockage local aux Serveurs Cloud

Le Stockage local des Serveurs Cloud optimisés pour le Big Data (gamme 'd') est destiné aux usages intensifs haute performance du Big Data.

Qualifié de disque « éphémère » parce qu'il a la caractéristique d'être localisé sur les disques internes de l'hyperviseur où le Client crée le serveur, il est détruit à la destruction de la VM. Ce comportement doit donc être géré au niveau de l'applicatif.

Il est particulièrement adapté aux clusters Big Data et aux bases de données No SQL dont les applicatifs tirent pleinement profit de son temps d'accès réduit, de la possibilité de parallélisations et de sa large bande passante. Il est ainsi possible de configurer jusqu'à 24 volumes de 1,8 To locaux pour les besoins de clusters Big Data distribués.

1.2.4 Sauvegarde et restauration (VBS)

Le service de backup de volume (VBS) permet aux Utilisateurs de sauvegarder, grâce à des snapshots, leurs instances virtuelles (ECS) hébergées sur des volumes élastiques (EVS). Le Client peut via la console réaliser la sauvegarde et la restauration de disques système ou de données. Ce service permet également de faire des snapshots d'instance afin de créer une image de celles-ci et de pouvoir les redéployer.

Fonctionnalités mises à disposition:

- Sauvegarde complète ou incrémentale des disques EVS

- Sauvegarde manuelle ou politiques de sauvegarde automatisée
- Suivi de l'état des tâches de sauvegarde
- Restauration ou création de disques EVS à partir d'une sauvegarde
- Copies multiples des sauvegardes et répartition sur différentes Zone de Disponibilité (AZ)

Restauration de disques Elastic Volume Service d'une Zone de Disponibilité à l'autre. Le service de VBS est facturé à l'usage.

1.2.4.1 Limites de la fonctionnalité d'automatisation de la sauvegarde

- Maximum de 360 sauvegardes pour chaque Tenant.
- Chaque disque EVS d'un Tenant peut avoir jusqu'à 20 sauvegardes
- 200To au total pour chaque Tenant;
- 5 opérations de sauvegarde VBS au maximum s'exécutant à la fois, incluant la création et la suppression de sauvegarde et la restauration. Des opérations plus importantes seront suspendues.

1.2.5 Cloud Server Backup Service (CSBS)

Cloud Server Backup Service (CSBS) offre un service de protection de sauvegarde pour les Elastic Cloud Servers (ECS) vers l'Object Storage Service (OBS). Il fonctionne sur la base de la technologie de snapshots cohérent pour les disques Elastic Volume Service (EVS). Les sauvegardes de tous les disques EVS d'un ECS sont générées au même moment.

Par défaut, seule la première sauvegarde est pleine et les suivantes sont incrémentales. CSBS remplit les fonctions suivantes : sauvegarde manuelle, sauvegarde automatique et restauration.

Le service CSBS est facturé sur la base de l'utilisation d'OBS plus une redevance mensuelle fixe pour chaque VM sauvegardée.

1.2.5.1 Limitations

- Les applications et les systèmes de fichiers sur l'ECS ne sont pas suspendus avant la sauvegarde, et les données de mémoire ne sont pas sauvegardées.
- Chaque ECS ne peut être associé qu'à une seule politique de sauvegarde.
- Un maximum de cinq créations et/ou de suppressions de sauvegarde sur disque EVS peuvent être exécutées simultanément pour chaque Tenant.
- La création ou la suppression de sauvegarde sont appliquées à l'ensemble du système ECS, y compris tous leurs disques EVS.

1.2.6 Storage Disaster Recovery Service (sDRS)

Storage Disaster Recovery Service (sDRS) permet au Client de reprendre son activité informatique sur une autre AZ de Flexible Engine. Ainsi, sDRS permet au Client de mettre en place un PRA (Plan de Reprise d'Activité) adapté aux pannes ou désastres affectant ses applications ou les infrastructures nominales sur lesquelles tournent ces applications.

Le Client est autonome et seul responsable du maintien en conditions opérationnelles et de l'activation de la protection de son activité. sDRS lui permet de sélectionner les VM à protéger ; de tester la reprise de son activité sur le site de secours ; de basculer son activité vers le site de secours ; de rétablir son activité sur le site nominal.

sDRS est fondé sur une réplication des VM, avec les applications et données associées. Cette réplication se fait entre deux AZ d'une même Région de Flexible Engine.

Le tableau suivant présente les coûts supportés par le Client dans le cadre de la mise en place d'un PRA :

En phase de : **Coûts supportés**	**Protection**	**Test**	**Reprise**	
Le nombre de VM protégées (en VM/mois)	X	X	X	Coûts propres à sDRS
Le volume de données transférées entre l'AZ nominale et celle de reprise (en Go)	X	X	X	
Le stockage, sur l'AZ de secours, des données de protection (en Go/mois)	X	X		Coûts complémentaires sur Flexible Engine à prendre en compte
L'activité CPU/RAM/Stockage des VM de test ou de production sur le site de reprise		X	X	

1.2.6.1 Limitations

- sDRS ne constitue pas un PRA (Plan de Reprise d'Activité), mais seulement une solution pour que le Client en mette un en place.
- Le site nominal et le site de reprise doivent être 2 AZ d'une même Région de Flexible Engine.
- Sur la Région Paris, l'AZ de reprise doit être EU_West-0a (PA3).
- Orange Business Services ne prend aucun engagement sur la fraîcheur des données (Recovery Point Objective) et la rapidité de reprise (Recovery Time Objective)

1.2.7 Scalable File Service (SFS)

Scalable File Service (SFS) fournit un système de fichiers partagés à la demande, évolutif et performant, accessible à tous les Elastic Cloud Servers (ECS) d'un Virtual Private Cloud (VPC) donné à travers les AZ d'une Région.

Le SFS est facturé en fonction du volume de stockage utilisé.

1.2.7.1 Limitations

- Scalable File Service supporte uniquement le protocole NFSv3.
- SFS ne permet pas de modifier le nom, AZ et VPC des systèmes de fichiers existants.

1.2.8 Dedicated Distributed Storage Service (DSS)

DSS (Dedicated Distributed Storage Service) fournit des ressources de stockage physiques dédiées. Il peut s'interconnecter avec divers services de puissance informatique, tels qu'ECS, BMS et DCC. Il prend en charge le partage de disque, le chiffrement de disque, la sauvegarde de disque et les snapshots.

1.3 Les services de mise en réseaux

1.3.1 Cloud Privé Virtuel (VPC)

Le Cloud Privé Virtuel (VPC) permet à l'Utilisateur de fournir un environnement réseau virtuel isolé, configurable et gérable, améliorant la sécurité des ressources d'une Région et en simplifiant le déploiement réseau.

Le service VPC permet au Tenant d'avoir un contrôle total sur les environnements réseau virtuels, incluant la création de réseau et la configuration DHCP (protocole de configuration dynamique des hôtes). Les Tenants peuvent utiliser des groupes de sécurité pour améliorer la sécurité de leurs environnements réseau. Ils peuvent également assigner des adresses IP élastiques (EIP) à leurs VPCs pour connecter les VPCs au réseau public. Les Tenants peuvent aussi connecter des VPCs aux data centers physiques en utilisant un réseau privé virtuel (VPN) ou en utilisant une connexion directe.

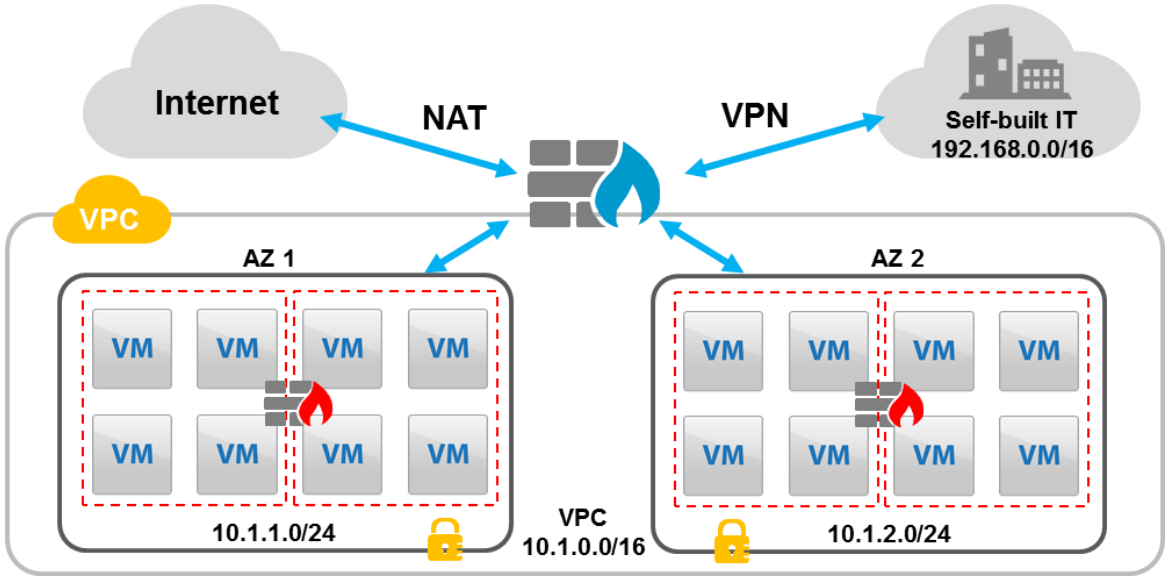


Figure n° 2: *VPC au sein d'une Région multi-AZ*

1.3.1.1 Spécifications VPC

- Plage d'adresses IP (RFC1918): 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16
- Plage de bande-passante pour EIPs: de 1 Mbit/s à 1Gbps
- Sous-réseaux VPN: 1000

Les quotas techniques par Tenant sont disponibles sur la console de Flexible Engine.

1.3.2 Adresses IP Publiques Elastiques (EIP)

Une adresse IP publique élastique (EIP) est une adresse statique IPv4 joignable sur Internet et conçue pour un environnement informatique dynamique. Une EIP est associée au Tenant de Flexible Engine et le Client est responsable pour attacher une EIP à un ECS pour permettre la communication avec Internet.

Une EIP peut avoir trois états :

- Allouée : réservée à un tenant
- Attachée : attachée à un serveur cloud

Lorsqu'un ECS est détruit, les EIP attachées restent allouées au Tenant et peuvent être attachées à un autre ECS. When an ECS is deleted, bound EIPs remain allocated to the Tenant and may be bound to another ECS.

L'adresse IP publique allouée est facturée à l'usage horaire (modèle pay-as-you-go).

1.3.3 VPN as a Service

La fonctionnalité de VPN as a Service du VPC permet de créer à la demande des VPN IPSec sur Internet pour encrypter le trafic depuis le VPC de l'Utilisateur vers le End Point IPsec de son choix. L'utilisateur peut ainsi établir des connexions sécurisées entre ses propres infrastructures et Flexible Engine.

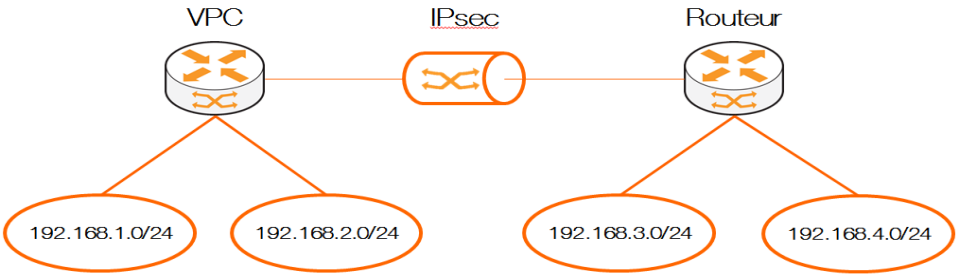


Figure n° 3: *Schéma de principe VPN IPsec*

Le service de VPN as a Service est facturé à l'usage.

1.3.4 Groupes de sécurité

Un groupe de sécurité agit comme un pare-feu virtuel à l'ECS afin de contrôler le trafic entrant et sortant. L'Utilisateur peut attacher un ECS à plusieurs groupes de sécurité. Le groupe de sécurité agit au niveau du gabarit. Ainsi, chaque ECS dans un sous-réseau du VPC pourrait être attribué à un ensemble différent de groupe de sécurité. Si l'Utilisateur ne spécifie pas de groupe de sécurité au lancement d'un ECS, l'ECS est automatiquement attribué par défaut au groupe de sécurité « default » du VPC.. Chaque groupe de sécurité offre la possibilité de créer et d'éditer des règles par rapport à des protocoles (tcp, udp, icmp), ports, adresse source et destination.

Les groupes de sécurité ne sont pas facturables.

1.3.5 Répartiteurs de charge (ELB)

Le répartiteur de charge élastique (ELB) est un service qui permet de distribuer automatiquement le trafic réseau vers de multiples Elastic Cloud Servers (ECSs) pour équilibrer la charge de service.

Fonctionnellement, ce service:

- permet la répartition de charge sur les flux HTTP / HTTPS / TCP à destination d'un pool de serveurs
- supporte les terminaisons SSL
- permet la répartition de charge inter-AZ
- permet l'Autoscaling en fonction du trafic
- assure une capacité d'extension linéaire (élimination des SPOFs)
- supporte le monitoring de métriques : trafic entrant et sortant, nouvelles requêtes, requêtes simultanées, paquets de données entrants et sortants, nombre de connexion, connexions inactives.
- permet la configuration de Health Check sur les instances

Le service de répartition de charge (ELB) est facturé à l'usage.

1.3.6 Répartiteur de charge de réseau privé

Cette fonctionnalité permet de répartir la charge à l'intérieur d'un Cloud Privé Virtuel, sans passer par internet. Le répartiteur de charge de réseau privé permet de répartir la charge entre les différents serveurs du Cloud Privé Virtuel, à l'intérieur d'une Zone de Disponibilité ou entre les Zones de Disponibilité d'une même Région.

Il est possible de faire cohabiter dans une même architecture des répartiteurs de charge de réseau privé (par exemple pour les serveurs de base de données) et des répartiteurs de charge web (pour les serveurs web).

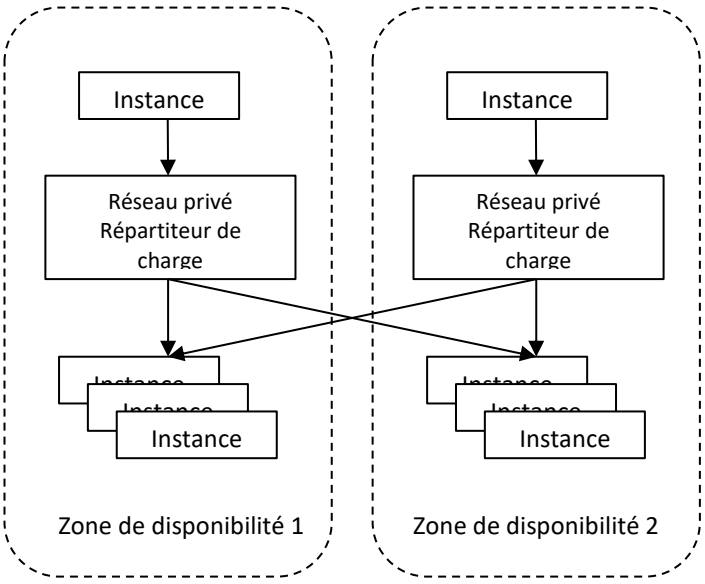


Figure n° 4: *Répartiteur de charge de réseau privé*

Limitation :

ECS peut seulement accéder au répartiteur de charge de réseau dans la même zone de disponibilité. L'ELB privé est facturé à l'usage.

1.3.7 Connexion à Internet

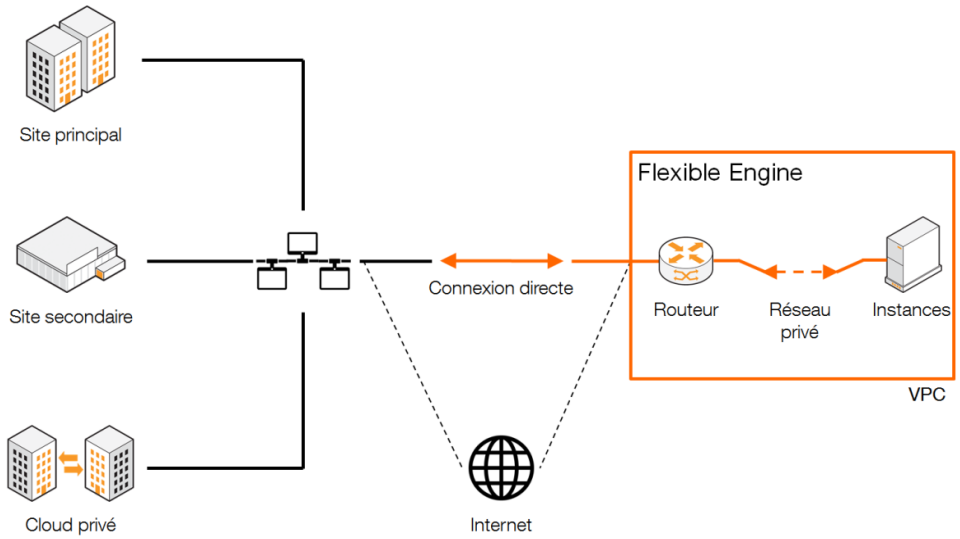
L'utilisation de la plateforme Flexible Engine par la Console ou par les API des Services est par défaut disponible à travers Internet et nécessite une authentification par login et mot de passe.

L'Utilisateur peut configurer les VPC, les EIP et les groupes de sécurité pour que les ECS accèdent à Internet.

Le trafic sortant vers Internet est facturé.

1.3.8 Connexion Directe

La Connexion Directe Flexible Engine est une solution pour connecter directement un réseau Client au Cloud Privé Virtuel FE (VPC) sans utiliser Internet.



Les ressources Client (ECS) sont contenues dans un Cloud Privé Virtuel (VPC) et externalisées vers l'entreprise à travers une connexion directe qui peut être un répartiteur appelé Port Dédié FE ou à travers un réseau partenaire. La capacité disponible pour chaque solution est indiquée dans le tableau ci-dessous.

La facturation de la connexion directe s'effectue sur une base mensuelle de bande passante souscrite. Les frais de transport pour les partenaires et les frais de déploiement et de connexion des routeurs clients vers la connexion directe FE ne sont pas inclus.

Capacité de la connexion directe	Port dédié FE	via un réseau partenaire	
		Business VPN Galerie	Equinix Cloud Exchange
2 Mbps		X	
5 Mbps		X	X
10 Mbps		X	X
30 Mbps		X	X
40 Mbps		X	X
50 Mbps		X	X
100 Mbps		X	X
200 Mbps		X	X
300 Mbps		X	X
500 Mbps		X	X
1 Gbps	X	X	X
2 Gbps			X
3 Gbps			X
4 Gpbs			X
5 Gbps			X
6 Gbps			X
7 Gbps			X
8 Gbps			X
9 Gbps			X
10 Gbps	X		X

1.3.8.1 La Connexion Directe via le Port Dédié Flexible Engine

Le Client peut directement accéder à des ports de 1 Gbps ou 10 Gbps sur les routeurs FE.

Pour les ports dédiés (1Gbps et 10 Gbps), le Client est responsable de la location d'espace de colocation pour déployer ses propres routeurs dans le PoP Flexible Engine, pour interconnecter ces routeurs vers le réseau interne et pour acheter les circuits pour connecter ces routeurs au port dédié FE.

1.3.8.2 La Connexion Directe via un réseau partenaire

Les partenaires actuels sont : Orange Business Service (Business VPN Galerie) et Equinix (Equinix Cloud Exchange).

La connexion directe FE via le Business VPN Galerie fournit de la connectivité Cloud privée MPLS sécurisée entre Flexible Engine et le Business VPN du client. Cela permet d'étendre la connectivité Réseau d'Entreprise Privée de bout-en-bout basée sur la technologie MPLS vers son VPC Flexible Engine, qui est vu comme un autre site.

Le Client peut utiliser Equinix Cloud Exchange pour connecter son réseau privé à Flexible Engine. Dans ce cas, le Client doit souscrire à Equinix Cloud Exchange. La Connexion Directe FE via Equinix Cloud Exchange est disponible à Paris et sera déployée à Singapour et Atlanta selon la roadmap.

Afin de bénéficier d'une solution réseau MPLS de bout-en-bout, le Client a besoin d'un côté d'activer l'option facturable de Connexion Directe FE et d'un autre d'acheter le service du partenaire choisi.

1.3.9 Service de Noms de Domaine

Le Service Nom de Domaines (DNS) fournit un moyen pour les utilisateurs et les développeurs de traduire un nom de domaine (tel que www.example.com) en une adresse IP (telle que 192.0.2.2.1) afin que les ordinateurs puissent accéder aux applications. Avec ce service, les utilisateurs de Flexible Engine peuvent configurer le DNS sur la console technique FE ou via l'API. Le service DNS peut être utilisé pour les zones publiques et privées.

Le client est facturé en fonction du nombre de zones hébergées et du nombre de requêtes DNS.

1.4 Sécurité

Les différents mécanismes de sécurité génèrent des événements et des alertes, consolidés en temps réel dans une zone « événements de sécurité », non accessible par les Utilisateurs. Flexible Engine s'appuie sur les services d'un SOC pour l'exploitation courante 24/7/365 de ces événements. Le SOC assure notamment un suivi spécifique des connexions VPN échouées sur le réseau d'administration.

Concernant les traces des équipements de sécurité, Flexible Engine dispose des journaux d'accès à ses services APIs, console d'administration et tableau de bord client. Ces données ont vocation à être communiquées aux autorités judiciaires.

1.4.1 Isolation des ressources

Flexible Engine fournit des services permettant à un utilisateur de créer une infrastructure virtualisée au-dessus d'une infrastructure physique mutualisée pour l'ensemble des Utilisateurs. Les mécanismes de virtualisation mis en œuvre assurent un cloisonnement logique fort entre les ressources virtualisés des clients (un Tenant par client). L'accès aux ressources d'un Tenant passe par les API OpenStack mettant en œuvre une authentification forte (login / mot de passe / token) et sécurisée (en SSL via https).

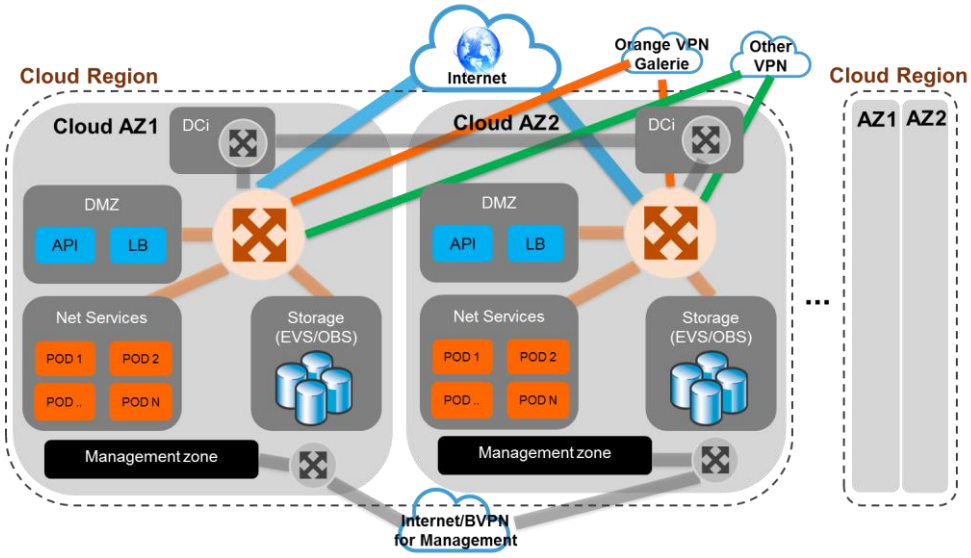


Figure n° 5: *Architecture logique / isolation des ressources*

Virtualisation système :

La plateforme de virtualisation Flexible Engine repose sur le moteur de virtualisation OpenSource XEN. Au-delà de la sécurité standard de cette solution, l'hyperviseur a été durci pour renforcer son cloisonnement :

- **Processus** : les processus de serveurs virtuels différents n'ont aucune visibilité les uns sur les autres
- **Mémoire vive** : les tests effectués par Orange Business Services montrent que les données en mémoire allouées après l'usage d'un serveur virtuel ne peuvent pas être récupérées
- **Données persistées** : pas de stockage local à l'hyperviseur (hors gabarit spécifique type BigDisk). L'accès aux serveurs virtuels déployés dans le tenant s'établit quant à lui par connexion sécurisée SSH ou RDP sur la base de la clé publique fournie au lancement de l'instance et de la clé privée dont il est le seul dépositaire.

Cette couche de virtualisation et son orchestration ont été soumis à des tests d'intrusion qui n'ont pas montré de vulnérabilité et qui n'ont pas réussi à récupérer de données persistées en mémoire ou sur les disques durs des hyperviseurs.

Virtualisation stockage :

La ségrégation d'accès aux données stockées (bloc et objet) est assurée par une couche applicative (Openstack Cinder pour le stockage block, compatible AWS S3 pour le stockage objet) qui n'autorise des accès aux données qu'aux Utilisateurs propriétaires des données ou de l'espace de stockage concerné.

Par ailleurs, les données écrites sur l'infrastructure ne sont pas récupérables une fois supprimées par le client ou lorsque l'infrastructure virtuelle correspondante est résiliée par le client. Ces mécanismes sont testés régulièrement grâce à des tests d'intrusion réalisés par Orange Cyberdefense et ses partenaires dont le savoir-faire est reconnu sur le marché. A noter que les disques physiques nécessitant d'être remplacés sont détruits par broyeuse avec un processus de traçabilité des matériels et de certification des opérations de maintenance.

Virtualisation réseau :

Les fonctionnalités de VPC porté par le composant OpenStack Neutron offrent un cloisonnement logique fiable des communications sur le réseau Utilisateurs. Toute forme de trafic réseau qui n'est pas naturellement autorisée sur le tenant du client n'est pas traitée par les équipements supportant le réseau virtuel du client, empêchant tout usage de technologies de spoofing.

1.4.2 Protection Anti-DDOS des EIP

L'Utilisateur peut protéger ses adresses IP publiques des attaques en déni de service au travers de la fonctionnalité Anti-DDOS.

Cette protection Anti-DDoS se base sur un échantillonnage du trafic et autorise la protection des infrastructures suivant plusieurs axes

- blackholing (suppression complète d'un trafic spécifique)
- throttling (limitation d'un trafic spécifique)
- cleaning (nettoyage d'un trafic spécifique)

Le service Anti-DDoS offre les fonctions suivantes :

- protection contre les attaques de trafic et attaques CC (mail) applicatives.
- personnalisation par les Utilisateurs des politiques Anti-DDoS
- sélection par les Utilisateurs des adresses IP publiques à protéger
- fourniture des rapports de suivi en temps réel.
- fourniture des rapports de sécurité hebdomadaires.

1.4.3 Gestion des identités et des accès (IAM)

La Gestion des identités et des accès (IAM) contrôle centralement les certificats de sécurité des utilisateurs et les politiques d'accès utilisateurs (qui incluent une liste de contrôle d'accès). Toutes les APIs utilisées pour les services de Flexible Engine (ainsi que l'accès à la console Flexible Engine) sont protégées par les contrôles d'authentification et d'autorisation de la fonctionnalité IAM.

Le service IAM comprend également une possibilité d'authentification à facteurs multiples (MFA-Multiple Factor Authentication) ainsi qu'une Fonctionnalité de création d'accès temporaires (STS-Security Token Service).

1.4.4 Key Management Service (KMS)

Key Management Service (KMS) est un service permettant aux Utilisateurs de gérer de façon centralisée leurs clés CMK (Customer Master Key). KMS utilise des modules de sécurité matériels (HSM) pour protéger les CMK.

Une CMK est une clé de chiffrement de clé KEK (Key Encryption Key) créée par un utilisateur avec KMS. Elle est utilisée pour chiffrer et protéger les clés de chiffrement des données DEK (Data Encryption Key). Une CMK peut être utilisée pour chiffrer une ou plusieurs DEK.

1.5 Services d'analyse de données

1.5.1 Map Reduce Service (MRS)

Le service MapReduce Service (MRS) permet de déployer des clusters sécurisés fournissant des ressources de calcul et de stockage à des fins d'analyse massive de données ou de traitement en temps réel.
Les ressources utilisées pour le calcul et le stockage peuvent être créées et supprimées en fonction des traitements nécessaires afin d'optimiser les coûts.

- Les principaux composants sont les suivants :Analyse et calculs massifs de données
    - Hadoop : plate-forme distribuée utilisant MapReduce pour effectuer des traitements parallèles sur de gros volumes de données et HDFS pour le stockage
    - Spark : framework de traitements distribués capable de réduire la latence du traitement de grandes quantités de données par ses fonctionnalités d'analyses « in-memory ». Il supporte les langages Scala, Java et Python. Il intègre dans MRS, Spark SQL afin de requêter et d'analyser les données via le langage SQL standard.
    - HBase (Hadoop Database) : système de gestion de base de données non relationnelles distribuées, écrit en Java, disposant d'un stockage structuré pour les grandes tables. Il fournit ainsi une solution fiable, performante et scalable pour compléter les bases de données relationnelles dans le traitement de données massives.
    - Hive Apache : infrastructure d'entrepôt de données intégrée à Hadoop permettant l'analyse, le requétage via un langage syntaxiquement proche de SQL ainsi que la synthèse de données.
    - HDFS (stockage massif de données) : système de fichiers distribué qui donne un accès haute-performance aux données réparties dans des clusters Hadoop. Comme d'autres technologies liées à Hadoop, HDFS est devenu un outil clé pour gérer des pools de Big Data et supporter les applications analytiques. Après avoir été traités et analysées, les données sont cryptées via SSL et stockées dans le stockage objet (OBS) ou dans HDFS.
    - Kerberos : MRS utilise KrbServer pour fournir l'authentification Kerberos sur tous les composants, sécurisant ainsi les mécanismes d'authentification.
    - Hue : fournit une interface graphique (WebUI) pour les applications MRS, permettant la gestion de HDFS, de MapReduce et des bases de données, édition de HQL et SparQL.
    - CarbonData : format de données en colonne ici associé à Spark et qui permet d'accélérer les requêtes d'un ordeur de grandeur.
    - Kafka : plate-forme de streaming distribuée. Elle utilise les concepts de « publisher » et « subscriber » et permet la collecte et consommation de messages en temps réel.
    - Storm : système de traitement temps réel. Pendant de Hadoop pour le temps réel, Storm permet des flux de données à large échelle en temps réel.
    - Loader : implémentation de Sqoop, permettant de transférer des données de Hadoop vers des datastores structurés et d'utiliser de multiples datasources et des échanges entre HDFS, HASE, RDBMS, NFS, SFTP.
    - Apache Flume : logiciel destiné à la collecte et à l'analyse de fichiers de log. L'outil est conçu pour fonctionner au sein d'une architecture informatique distribuée et ainsi supporter les pics de charge.

Les types d'ECS supportés par MRS sont listés dans la Fiche Tarifaire.

Limitations d'utilisation

Les limitations suivantes doivent être prises en compte pendant l'utilisation de MRS : si des fichiers sont téléchargés via le Web, la taille du fichier ne peut pas excéder 50 Mo. Si les données sont transférées d'HDFS vers OBS, la capacité maximale

des données est de 5 Go. La largeur de bande maximale du réseau est de 5 Go/s. Pour plus de détails, cf. les limitations des caractéristiques d'ECS, VPC, EVS et OBS.

La tarification du Service MRS est fonction du choix des machines ECS utilisées au sein du Cluster MRS et s'ajoute au prix du service ECS.

1.6 Services de base de données

1.6.1 Bases de données relationnelles (RDS)

Le service de bases de données relationnelles (RDS) permet de déployer des bases de données MySQL, PostgreSQL ou Microsoft SQL Server, avec un déploiement en mode simple ou en mode actif-passif.

L'installation et le déploiement des bases de données se fait de façon automatique. Le service propose également des outils d'opération et de maintenance: PRA, sauvegarde et restauration, monitoring, migration. Le service permet de réduire la complexité et les coûts d'opération de maintenance, permettant ainsi au Client de se concentrer sur l'applicatif et le business.

Les gabarits et systèmes RDS ainsi que leur tarification sont présentés dans la Fiche Tarifaire.

1.6.2 Distributed Cache Service (DCS)

Distributed Cache Service (DCS) est un service de base de données en mémoire compatible avec Redis et IMDG. Basé sur une architecture HA, DCS supporte trois types d'instance : single-node, master/standby et cluster. Le DCS garantit des performances élevées en lecture/écriture et un accès rapide aux données.

1.6.3 Document Database Service (DDS)

Document Database Service (DDS) est un service de base de données compatible avec MongoDB qui est sécurisé, hautement disponible, fiable, évolutif et facile à utiliser. Il offre une variété de fonctions, y compris la création d'instances de base de données, la mise à l'échelle, la redondance, la sauvegarde, la restauration, la surveillance et la création de rapports d'alarme.

1.7 Applications d'entreprise

1.7.1 WorkSpace

WorkSpace est une solution de Desktop-as-a-Service (DaaS) permettant au Client de fournir aux Utilisateurs des postes de travail Microsoft Windows virtuels, hébergés sur le cloud, incluant des vCPU, des disques et des systèmes d'exploitation. De cette façon, les Utilisateurs peuvent y accéder à partir des terminaux compatibles.

La liste des gabarits est disponible sur la console et peut évoluer régulièrement.

WorkSpace peut être souscrit sous la forme d'un abonnement mensuel forfaitaire donnant droit à un usage illimité ou sous la forme d'un paiement à l'usage facturé à l'heure, assorti le cas échéant d'un abonnement mensuel.

1.7.2 Remote Desktop Services (RDS/SAL)

Le RDS permet à un Utilisateur de se connecter à distance à une application d'entreprise hébergée sur un serveur Windows. Le Client doit souscrire une licence RDS/SAL (Subscriber Access License) pour chaque Utilisateur susceptible d'avoir accès à l'application d'entreprise concernée. Les machines ne peuvent être licenciées.

Le Client peut soit souscrire les licences auprès d'Orange Business Services en mode locatif soit apporter des licences dont il est titulaire en mode mobilité, dans les conditions décrites dans la section "Licences / Produits Microsoft".

Le prix de vente, disponible dans la Fiche Tarifaire Flexible Engine, est applicable par mois calendaire complet sans prorata temporis.

1.7.3 Office

Office est suite logicielle bureautique. Flexible Engine propose la version « Standard » incluant les logiciels Word, Excel, PowerPoint, OneNote, Outlook, Publisher et la version « Professional Plus » incluant les logiciels Word, Excel, PowerPoint, OneNote, Outlook, Access, Publisher et Client Skype.

Chaque licence Office (Standard ou Professional Plus) est souscrite pour un seul Utilisateur, personne physique. Ces licences ne sont pas éligibles à la mobilité.

En revanche les licences « Office 365 Professional Plus », qui ne sont pas proposées au catalogue Flexible Engine, peuvent être apportées par le Client, sous réserve d'être déclarées à Orange Business Services.

Chaque licence Office (Standard ou Professional Plus) ou Office 365 Professional Plus doit être associée à une licence « Remote Desktop Services ».

Le prix de vente des licences Office (Standard ou Professional Plus), disponible dans le catalogue Flexible Engine, est applicable par mois calendaire complet sans prorata temporis.

1.8 Services pour les développeurs

1.8.1 Les API de Flexible Engine

Les APIs mises à disposition par Flexible Engine sont des APIs RESTful basées sur la technologie OpenStack et documentées dans le Help Center.

1.8.2 Orchestration : Resource Template Service (RTS)

Avec l'orchestrateur Heat RTS (Resource Template Service) mis à disposition via APIs, le Client peut réaliser de manière automatisée et configurable, la totalité d'un déploiement d'infrastructure virtualisée (serveurs, routeurs, réseaux, volumes, etc...) en s'appuyant sur les différentes API des modules Openstack.

Il est ainsi possible de créer des templates HOT (Heat Orchestration Template) qui permettent de spécifier la configuration, la description et les relations de l'ensemble des ressourcespour automatiser et faciliter le déploiement de la plate-forme.

1.8.3 API Gateway

API Gateway permet aux développeurs de créer, publier, sécuriser et monitorer les API de leurs applications.

La Fonctionnalité est facturée en fonction du nombre d'appels API et du trafic sortant.

1.9 Outils de monitoring

1.9.1 Supervision et monitoring (CES)

Le Cloud Eye Service (CES) est un service de monitoring ouvert qui permet de mettre en place du monitoring, de l'alerting et de la supervision pour vos ressources en temps réel.

Il permet notamment de monitorer des métriques directement sur les instances de calcul (ECS), les volumes de stockage (EVS), les Clouds Privés Virtuels (VPC), les répartiteurs de charge (ELB), les groupes d'autoscaling (AS) et les bases de données relationnelles aaS (RDS).

Il est ainsi possible pour le Client de configurer des règles d'alerting et des politiques de notifications basées sur ses métriques pour suivre dans le temps le statut et les performances des objets monitorés.

Les fonctionnalités sont les suivantes :

- **Monitoring automatique** : le monitoring débute de façon automatique lors de la création d'une instance ou d'un groupe d'autoscaling. Aucune action supplémentaire n'est nécessaire.
- **Configuration d'alarme flexible** : le Client peut configurer des règles de déclenchement d'alarme et de seuil pour l'ensemble de ses métriques. Il est également possible d'activer ou désactiver ces règles lorsque souhaité.
- **Notifications en temps réel** : fonction de notification activable afin de recevoir des notifications sur mobile ou par email ; il est également possible d'envoyer ces notifications à un serveur dédié.
- **Suivi de métriques** : la page de Tableau de Bord permet d'avoir une vue d'ensemble (sous forme de graphiques) et de créer les métriques souhaitées.

1.9.2 Cloud Trace Service

Cloud Trace Service (CTS) fournit un journal d'opérations sur les ressources de service cloud. Celui-ci permet l'interrogation, l'audit, la remontée du journal des opérations ainsi que le stockage des logs dans des containers OBS avec une grande

fiabilité. De plus, cette fonctionnalité enregistre tous les logs déclenchés par les API ouvertes et la console de chaque service cloud intégré à cette fonctionnalité. L'Utilisateur ne peut créer qu'un seul tracker pour chaque Région dans chaque Tenant. Cette fonctionnalité n'est pas facturée.

1.9.3 Simple Message Notification (SMN)

Simple Message Notification (SMN) est un service de notification de messages. Il permet aux utilisateurs d'envoyer des messages par e-mail , SMS ou HTTP/HTTPS à un groupe d'abonnés par lots.
SMN peut être intégré avec d'autres Fonctionnalités pour recevoir des notifications d'événements de leur part.

SMN est facturé en fonction du nombre d'appels API, du nombre de notifications, du nombre de SMS et de leur destination, et du volume de trafic Internet utilisé.

1.9.3.1 Limitations

- L'abonnement ne prend effet qu'après confirmation de l'abonnement par l'abonné. Les abonnés doivent être invités et confirmer leur abonnement pour recevoir des messages.
- La taille maximale des messages est limitée à 256 kB.
- Les messages sont réservés pendant 7 jours et le système les efface automatiquement par la suite.
- En cas d'échec d'un message, le système essaie d'envoyer le message 6 fois de plus. Si l'envoi échoue toujours, le système abandonne le message.

1.9.4 Tag Management Service (TMS)

Tag Management Service (TMS) est un service pour le balisage et la catégorisation des services cloud. Les utilisateurs peuvent utiliser des balises pour classer et rechercher des ressources Cloud par but, dimension, projet, environnement.... Les ressources supportées sont : ECS, OBS, VPC, VBS, EVS, EVS, AS, IMS.

2 Support

Ce chapitre a pour objet de décrire les services de support fournis par Orange Business Services dans le cadre des Services de l'offre Flexible Engine, leur organisation et les modèles de processus associés.

Ce chapitre détaille :

- les offres de support proposées au Client ;
- l'organisation de la communication entre Orange Business Services et le Client ;
- l'organisation et le périmètre des activités du support fourni par Orange Business Services ;
- les prérequis à la fourniture du support par Orange Business Services ;
- la manière de déclarer un incident ou une demande auprès du Support Technique ;
- la manière dont le Support Technique prend en compte et traite un incident ou une demande ;