Business

Descriptif de Service
Flexible Engine

Table des matières

1 Définitions

En complément des définitions des Conditions Générales et des Conditions Spécifiques Cloud, les définitions spécifiques suivantes s'appliquent à ce Descriptif de Service.

Conditions Générales désigne les conditions générales relatives aux Services du Prestataire.

Conditions Spécifiques Cloud désigne les conditions spécifiques relatives aux Services de Cloud du Prestataire.

Console Flexible Engine désigne l'interface web permettant d'administrer les Services Flexible Engine.

Fonctionnalité désigne un élément du Service « Flexible Engine ».

Interruption désigne la ou les période(s) pendant laquelle un incident provoque un dysfonctionnement significatif du Service ou de la Fonctionnalité concernée affectant l'ensemble des Utilisateurs. Le calcul de la durée d'indisponibilité se fait selon des critères propres à chaque Service ou Fonctionnalité.

Région désigne une zone géographique où le Service est disponible sur une ou plusieurs Zone(s) de Disponibilité. Les Régions sont listées dans le Descriptif de Service.

Région Multi-AZ désigne une Région disposant de plusieurs Zones de Disponibilité.

Service désigne le service « Flexible Engine » fourni pour un Tenant. Chaque Tenant constitue un Service distinct.

Tenant désigne un espace privé virtuel de ressources sur le cloud Flexible Engine auquel seuls les Utilisateurs authentifiés par login et mot de passe peuvent avoir accès. Les actions de création, destruction, modification, listage de ces ressources et des Fonctionnalités associés sont limitées à ces seuls Utilisateurs.

Machine Virtuelle (ou VM pour Virtual Machine) désigne un ordinateur logiciel qui, à l'instar d'un ordinateur physique, exécute un système d'exploitation et des applications. La machine virtuelle se compose d'un ensemble de fichiers de spécification et de configuration ; elle est secondée par les ressources physiques d'un hôte. Chaque machine virtuelle a des périphériques virtuels qui fournissent la même fonction que le matériel physique.

Zone de Disponibilité désigne un centre de données isolé ou suffisamment éloigné des éventuels autres centres de données de la Région pour permettre la mise en œuvre d'une résilience locale. Les Zones de Disponibilité de chaque Région sont listées dans le Descriptif de Service.

2 Objet

Le présent descriptif de service a pour objet de définir les conditions dans lesquelles le Prestataire fournit le service «Flexible Engine» (ci-après le « Service ») au Client.

Le présent descriptif est rattaché aux Conditions Spécifiques Cloud.

3 Présentation du Service

3.1 Aperçu du Service

Flexible Engine est une solution d'Infrastructure as a Service globale. L'offre Flexible Engine propose un riche portfolio de services Cloud accessibles à la demande. La roadmap de la solution est évolutive.

3.2 Implantation géographique

Les services Flexible Engine sont disponibles dans plusieurs Régions à travers le monde afin de permettre au Client de déployer ses services sur un Territoire mondial. La console Flexible Engine permet de gérer les instances sur n'importe quel data center. Le Client détermine, lorsqu'il paramètre son Service, la ou les Région(s) dans lesquelles ses données seront traitées et stockées. Le Prestataire ne déplace pas les données du Client dans une autre Région que celle(s) choisie(s) par le Client.

La solution propose des Régions opérées par le Prestataire et des Régions opérées par les partenaires du Prestataire. Les régions opérées par le Prestataire sont les suivantes :

- Paris (eu-west-0) qui comprend trois datacenters dans la Région de Paris en Europe de l'Ouest
- Amsterdam (eu-west-1) qui comprend trois datacenters à Amsterdam en Europe de l'Ouest
- SAP Hana Paris (eu-westxvp-28) qui comprend un datacenter dans la région de Paris

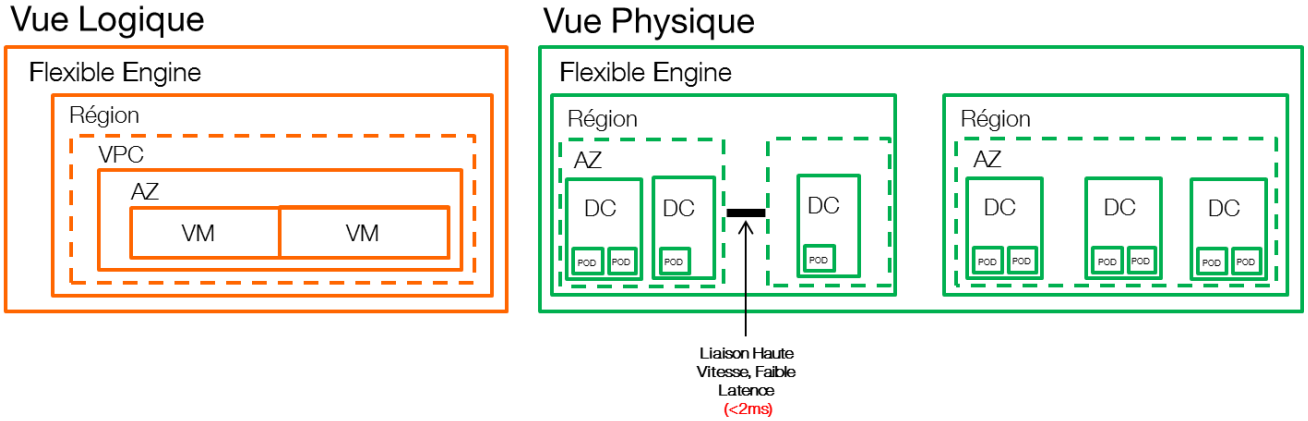
Les Régions partenaires sont visibles sur l'Espace Client.

La disponibilité des Fonctionnalités peut varier d'une Région à l'autre et est précisée dans la Fiche Tarifaire et/ou dans la Console Flexible Engine et/ou sur les sites partenaires. La Région SAP Hana Paris est accessible uniquement dans le cadre de projets SAP Hana, en mode managé (offre Managed Applications)

3.2.1 Concept de Région et de Zone de Disponibilité (AZ)

L'offre Flexible Engine s'appuie sur une architecture conçue pour être déployée à l'échelle mondiale. Elle implémente une résilience progressive de l'ensemble des zones et des composants, selon un découpage simple à appréhender.

Figure n° 1: *Vue Logique / Vue Physique*



De manière simplifiée :

- à l'échelle mondiale : différentes Régions isolées les unes des autres permettent d'adresser des usages répartis ou de mettre en place une résilience mondiale
- à l'échelle d'une Région : différentes Zones de Disponibilité [AZ] isolées entre elle. Chaque Zone de Disponibilité est implémentée dans un centre de données distinct, suffisamment éloigné pour imaginer une résilience locale, et suffisamment proche pour implémenter des répartitions de charges (moins de 2 ms de latences entre 2 AZ).
- à l'échelle d'une Zone de Disponibilité (AZ) : différentes zones de services isolées entre elles, implémentant des composants d'infrastructures tous redondés :
    - accès internet local porté par différents transitaires
    - équipements de sécurité et d'interconnexion redondés
    - infrastructure IaaS bâtie sur des équipements proposant de la haute disponibilité

Le Prestataire a imaginé une résilience de ses services en dissociant clairement :

- la couche de collecte du trafic et de gestion de la sécurité via des points de présence [POP] indépendants de l'infrastructure, localisés dans chaque Zone de Disponibilité
- la couche de fourniture des services du catalogue IaaS via les Centres de Données
- l'interconnexion entre les deux couches se fait localement à chaque Zone de Disponibilité.

3.3 Certification HDS

Flexible Engine utilisé conjointement avec le niveau de support Business ou supérieur est certifié Hébergement de Données de Santé (HDS) pour les prestataires de services de santé en France afin de gérer les données de santé sensibles des patients.

4 Conditions d'utilisation

4.1 Prix

Les prix du Service sont révisables dans les conditions prévues aux Conditions Générales, à l'exception des instances réservées dont le prix est fixé pour la durée d'engagement au moment de la réservation.

Les prix du Service sont révisables dans les conditions prévues aux Conditions Générales et aux Conditions Spécifiques Cloud, et peuvent être mis à jour mensuellement. Les nouveaux prix s'appliquent aux Contrats en cours. Le Client sera informé des nouveaux tarifs par publication sur les Interfaces Utilisateurs ou par tout autre moyen, au plus tard à la date d'entrée en vigueur des nouveaux tarifs. En cas de hausse des prix d'une Fonctionnalité existante, le Client en sera informé par courrier électronique ou par tout autre moyen au plus tard 30 jours avant l'entrée en vigueur des nouveaux tarifs. Les prix en vigueur à la Date de Mise en Service pourront être différents de ceux communiqués au moment de la souscription.

Les tarifs sont définis par Région. Le Client désigne dans la Commande une Région de rattachement sur laquelle porteront les frais qui ne sont pas liés à une Région spécifique.

Pour les Régions partenaires, seuls les prix catalogue disponibles sur le site partenaire, en dollars US, font foi.

4.2 Licences

Le Client s'engage à utiliser les Logiciels, notamment les systèmes d'exploitation, dans le respect de l'article « Propriété Intellectuelle » des Conditions Générales.

Les systèmes d'exploitation fournis dans le cadre du Service sont listés au chapitre « Service de gestion des images (IMS) ».

4.2.1 Produits Microsoft

Le Client peut soit souscrire les licences des Logiciels Microsoft auprès du Prestataire en mode locatif soit apporter des licences souscrites par lui directement auprès de Microsoft ou d'un revendeur tiers en mode mobilité, selon les conditions d'utilisation applicables à chaque Logiciel, disponibles à l'adresse suivante :

https://www.microsoft.com/fr-fr/Licensing/product-licensing/products.aspx

L'usage par le Client des Logiciels Microsoft doit respecter les conditions d'utilisation associées au contrat SPLA (Service Provider License Agreement) de Microsoft. Le client est seul responsable vis-à-vis de Microsoft des éventuelles non-conformités d'utilisation des logiciels Microsoft et il est redevable auprès du Prestataire des éventuelles conséquences imposées par Microsoft.

4.2.1.1 Mode locatif

Les licences Microsoft proposées par le Prestataire sont en mode locatif, le Client ne doit pas utiliser les licences correspondantes pour un usage autre que le Service souscrit auprès du Prestataire.

4.2.1.2 Mode mobilité

La mobilité de licence Microsoft, pour des logiciels précédemment acquis, est possible conformément aux avenants « License Mobility» ou « Qualified Multitenant Hoster » (QMTH) du contrat SPLA, selon les Logiciels concernés.

Entre autres conditions, le Client a la responsabilité des opérations suivantes :

- avoir souscrit auprès de Microsoft, lorsque c'est requis par Microsoft, la "Software Assurance" (SA) qui est un complément de licence pour permettre sa mobilité ;
- pour License Mobility, déclarer la mobilité à Microsoft, en indiquant les références d'ORANGE en tant que partenaire de mobilité, via un formulaire spécifique édité par Microsoft et fourni au Client par le Prestataire sur demande du Client ;
- pour QMTH, déclarer au Prestataire le nombre d'Utilisateurs pour chaque Logiciel concerné.

La mobilité de licence Microsoft de type SPLA et SPLA Academics est également possible. Un « Outsourcing Company Agreement » devra être signé spécifiquement entre le Client et le Prestataire comme indiqué dans le §7 du contrat SPLA du Client.

4.3 Réversibilité

Dans le cadre de l'offre Flexible Engine, le Client peut effectuer des sauvegardes de ses machines virtuelles ECS et de ses volumes EVS. Dans la mesure où il s'agit d'une plateforme en ligne à l'usage, le Client est autonome pour récupérer, en utilisant nominalement les APIs de Flexible Engine au travers de la connexion qu'il utilise, par exemple Internet ou une Connection Directe, les sauvegardes ainsi effectuées ainsi que les données stockées sur son Stockage Objet OBS. Le Prestataire n'intervient pas.

De manière optionnelle, des prestations de Service peuvent être envisagées sur devis.

4.4 Récupération et suppression des données HDS

Les données HDS issues des sauvegardes des machines virtuelles ECS et des volumes EBS peuvent être récupérées par le Client en mode autonome ou en mode accompagné.

Mode autonome :

Dans la mesure où il s'agit d'une plateforme d'utilisation en ligne, le Client est autonome pour récupérer, en utilisant nominativement les API de Flexible Engine HDS via la connexion qu'il utilise, par exemple Internet ou une Connexion Directe, les sauvegardes ainsi effectuées ainsi que les données stockées sur son Stockage Objet. Le Prestataire n'intervient pas. Les données appartenant au Client sont automatiquement supprimées des Datacenters dans un délai maximum de deux (2) mois à compter de la date de fin contractuelle du Service. Le Client peut décider de supprimer manuellement l'ensemble de ses données avant la fin du service depuis la console HDS de Flexible Engine.

Mode accompagné :

De manière optionnelle, des prestations de service peuvent être proposées sur devis.

Une fois transférées, les données appartenant au Client, ainsi que l'ensemble de leurs sauvegardes, sont supprimées du Datacenter dans un délai maximum de deux (2) mois à compter de la signature du procès-verbal d'acceptation du plan de réversibilité et, en tout état de cause, au plus tard deux (2) mois à compter de la date de fin contractuelle du Service. A la demande du Client, le Fournisseur peut certifier par un document écrit que les données du Client ont été supprimées.

5 Accès au Service

5.1 Portails

Après acceptation de la Commande par le Prestataire, le Client recevra un courrier électronique de confirmation de son inscription et de demande d'initialisation de son mot de passe lui permettant d'accéder au portail appelé Espace Client, à la Console Flexible Engine et d'administrer les Services dans le Tenant créé pour lui.

Le Client peut inviter des Utilisateurs avec les droits d'usage des Services dans ses Tenants. Les Utilisateurs à qui le Client a donné les droits le permettant peuvent eux-mêmes inviter d'autres Utilisateurs.

5.1.1 Le portail cloud Orange Business

Le portail cloud Orange Business est le site internet du Prestataire où sont présentées nos offres de service. On y trouve un certain nombre d'informations générales sur Flexible Engine. Le site est accessible à l'url suivante : http://cloud.orange-business.com/.

5.1.2 L'Espace Client Cloud

L'Espace Client Cloud est un espace réservé à l'Utilisateur, lui permettant de gérer son compte Flexible Engine. Il est créé à la création de son compte Flexible Engine.

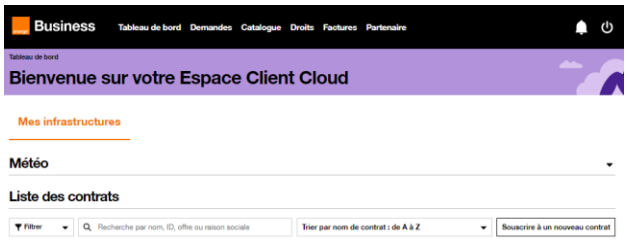


Figure n° 2: *L'Espace Client Cloud*

A partir de l'Espace Client Cloud, le Client peut gérer l'ensemble des services Flexible Engine pour ses Utilisateurs, notamment grâce aux sections suivantes :

- **Tableau de bord** : cette section permet de visualiser les informations générales du compte, d'accéder à la console
- **Demandes** : cette section permet de visualiser l'historique des demandes passées sur l'Espace Client cloud, et leur statut
- **Catalogue** : cette section permet d'accéder à un catalogue de services de l'offre Flexible Engine et de les commander : commande d'Instances Réservées, réservation de ressources dédiées, renommage de contrat, activation de Régions partenaire etc.
- **Droits** : cette section permet de gérer les droits des utilisateurs de Flexible Engine sur l'Espace Client Cloud et de leur donner accès à la Console Technique
- **Factures :** permet de consulter l'ensemble des factures en ligne, et les autres fichiers liés : facturation détaillée, simulation de facture en cours de mois… Cette section propose aussi une gestion budgétaire (alertes)
- **Abonnements :** depuis le tableau de bord cette section permet de consulter la liste des Instances Réservées et Instances Réservées Flexibles avec leur statut et date de fin d'engagement
- **Besoin d'aide :** depuis le tableau de bord cette section permet d'accéder à l'ensemble de l'aide en ligne et de créer des demandes / tickets de support
- **Partenaire :** cette section est accessible uniquement avec un « login partenaire » délivré au Client par le Prestataire à sa demande, elle permet :
    - au Client de créer ses Tenants supplémentaires – les usages de ces Tenants sont les usages du Client, ils sont agrégés à sa facture
    - au Client de gérer ses différents Tenants sur l'Espace Client Cloud depuis un login unique – accès aux différentes sections mentionnées ci-dessus,

Cette section ne permet pas de gérer les droits des utilisateurs de Flexible Engine ni d'accéder à la Console Technique de Flexible Engine.

L'Espace Client Cloud propose aussi un service d'API reposant sur les droits des utilisateurs de l'Espace Client Cloud aux différents tenants Flexible Engine.

Cette API permet au Client, si le login Espace Client Cloud utilisé dispose des droits suffisants de :

- accéder aux fichiers de facturation des Tenants,
- créer des Tenants Flexible Engine supplémentaires,
- donner des accès à aux Tenants Flexible Engine, à des utilisateurs existants ou nouveaux.

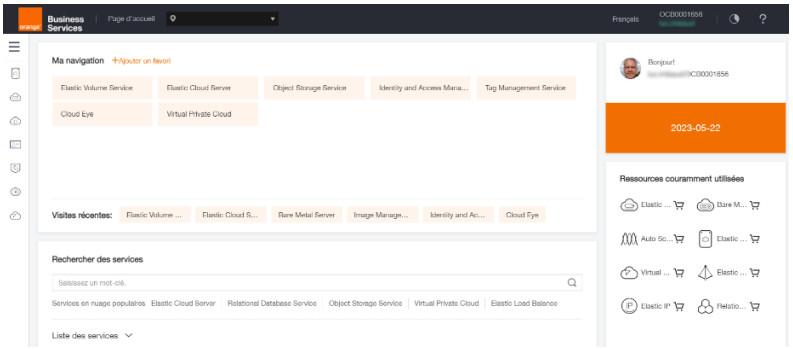
5.1.3 La Console Flexible Engine

La Console Flexible Engine est le portail web de gestion des services Flexible Engine. Il permet la gestion et le déploiement des ressources d'infrastructure IaaS.

Elle est accessible à l'url suivante : https://console.prod-cloud-ocb.orange-business.com/console/#/home

L'utilisateur retrouve ainsi l'ensemble des services et Régions de l'offre Flexible Engine.

Figure n° 3: *Console Flexible Engine*



5.1.4 Les sites partenaires

Pour les Régions partenaires, le Client dispose d'un accès au site partenaire, au moyen d'un login/mot de passe spécifique pour les fonctionnalités nécessitant une connexion, lui donnant accès à :

- des informations techniques sur la solution disponible dans les Régions partenaire
- les prix publics applicables dans le cadre du Service
- l'espace client partenaire, uniquement pour les rapports d'usage (les rapports d'usage ne valent pas facture)
- la console technique partenaire, pour le paramétrage du Service

Ne sont pas applicables au Service les autres éléments présents sur le site partenaire, notamment :

- les documents contractuels présentés par le partenaire.
- le parcours de commande, renouvellement ou résiliation offert par le partenaire (en dehors de la console technique). L'utilisation de ce parcours n'a pas d'impact sur le Service et n'engage en aucun cas le Prestataire.
- la modalité de facturation « prépayé » (« prepaid ») proposée par le partenaire.
- les promotions partenaire.
- l'accès au support partenaire. Les modalités d'accès au support du Service sont exclusivement celles décrites au chapitre 7 du présent document.

5.2 Réseau

La connexion au Service s'effectue via le réseau Internet.

Les services Flexible Engine n'incluent pas l'interconnexion réseau entre l'entreprise du Client et les infrastructures du Prestataire. Selon les besoins du Client, des offres d'interconnexion réseau peuvent être souscrites séparément auprès du Prestataire.

6 Contenu du Service

6.1 Les services de puissance informatique

6.1.1 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.

6.1.2 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.

6.1.3 Instances réservées

La Fonctionnalité « Instances réservées » permet à l'Utilisateur de bénéficier d'une grille tarifaire spécifique en fonction de sa durée d'engagement (1, 2, 3 ans ou 5 ans) et du paiement ou non de frais initiaux. Avec cette Fonctionnalité, l'ECS, Workspace, BMS, ou CSS ne sont plus facturés à l'usage mais selon un abonnement mensuel.

Elles s'appliquent à des ressources provisionnées via la console utilisateur ou des APIs. La souscription aux « Instances réservées » se fait via l'Espace Client Cloud. Elles ne garantissent pas la disponibilité de ressources associées au moment de la souscription. Avant de souscrire à une Instance Réservée, il est indispensable de vérifier la disponibilité de la ressource cloud dans la Console Flexible Engine qui va les allouer physiquement.

Les « Instances réservées » existent en deux modèles :

- Sans frais initiaux : l'utilisateur paye tous les mois un montant défini, quel que soit son utilisation.
- Avec frais initiaux : l'utilisateur sera facturé un montant initial (qui correspond à une partie du cout total de l'instance réservée durant la période de souscription) en plus d'un montant mensuel défini, quel que soit son utilisation.

Le Client peut faire cohabiter dans son Tenant des VM ECS à l'usage et des VM ECS en instances réservées. Les instances réservées sont souscrites pour un gabarit et une Région donnés. Chaque mois, la VM correspondant au gabarit réservé ayant la plus grosse consommation dans la Région concernée sera prise en charge par l'abonnement, tandis que les autres resteront facturées à l'usage. L'instance réservée s'applique à partir du premier jour du mois calendaire suivant la souscription. Ainsi, le premier mois d'utilisation sera facturé selon le mode « paiement à l'usage ».

A l'issue de la durée d'engagement, la facturation à l'usage reprend.

Le parcours de souscription à une Instance Réservée est décrit dans un document spécifique accessible dans via le lien suivant : https://cloud.orange-business.com/wp-content/uploads/2021/05/Page-dexplication-RI.pdf

6.1.4 Instances réservées Flexibles

Les « Instances réservées flexibles » permettent à l'utilisateur de bénéficier de la possibilité de modifier son abonnement au cours de la période de souscription. Les « Instances réservées flexibles » sont soumises aux mêmes conditions d'accès et d'utilisation que les « Instances réservées ». Les différentes possibilités quant à la modification des « Instances réservées flexibles » sont décrites dans un document spécifique accessible via le lien suivant : https://cloud.orange-business.com/wp-content/uploads/2020/11/Page-dexplication-FRI.pdf

6.1.5 Résiliation des Instances Réservées et Instances Réservées Flexibles

Il est possible d'annuler une Instance Réservée ou une Instance Réservée Flexible avant la fin de l'engagement. En contrepartie des frais de résiliation s'élevant à 12% du montant dû sur la période d'abonnement initiale seront appliqués. Les modalités de résiliation des Instances Réservées et Instances Réservées Flexible sont décrites dans un document spécifique accessible ici : https://cloud.orange-business.com/wp-content/uploads/2021/03/Page-dexplication-des-penalites-de-resiliation-anticipee.pdf

6.1.6 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.

6.1.7 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).

6.1.8 Service de gestion des images (IMS)

Une image est utilisée pour créer des ECS avec un système d'exploitation (OS) et des applications préinstallées 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. Le Prestataire 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.

6.1.9 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 tailleen 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.

6.1.10 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)…

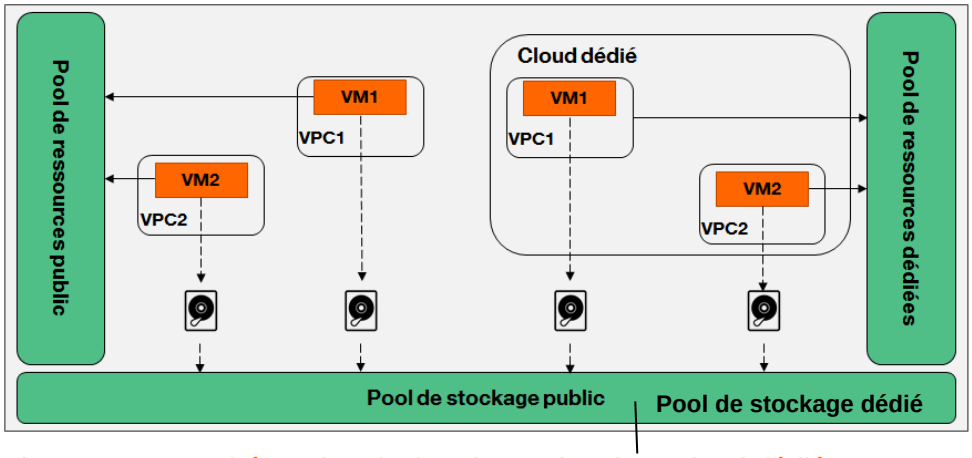


Figure n° 4: *Schéma de principe du service de « Cloud dédié »*

Les serveurs disponibles et le principe de facturation sont précisés dans la Fiche Tarifaire.

6.1.11 Flexible Engine Stack

A l'aide de Flexible Engine Stack, le Client peut utiliser les services Flexible Engine sur une infrastructure privée. Le Client peut utiliser la même interface utilisateur que celle de Flexible Engine pour contrôler son cloud, public et privé, ou des API automatisées.

6.1.12 Dedicated Host

Le service d'hôte dédié (DeH) est un service qui fournit des serveurs physiques dédiés à l'usage du Client, sur lesquels il peut créer ou migrer des machines virtuelles ECS (Elastic Cloud Server). DeH permet d'améliorer l'isolation, la sécurité et les performances de ses ECS. Lorsque le Client migre des serveurs vers un DeH, il peut continuer à utiliser les licences logicielles de son ancien serveur. En d'autres termes, le Client peut utiliser la fonction Bring Your Own License (BYOL) sur le DeH et gérer ses ECS sur DeH de manière indépendante.

6.1.13 FunctionGraph

FunctionGraph est un service informatique qui fournit des capacités d'exécution de fonctions sans serveur. Il s'adapte automatiquement aux fluctuations de la demande de ressources pendant les périodes de forte activité, tout en ne nécessitant aucune réservation de serveur ou de capacité. Les utilisateurs de Flexible Engine peuvent écrire leur propre code et spécifier des conditions d'exécution.

FunctionGraph est compatible à la fois avec Log Tank Service (LTS), qui permet aux utilisateurs de visualiser les journaux d'exécution des fonctions sans avoir à les configurer, et avec Cloud Eye, qui permet aux utilisateurs de visualiser les métriques de monitoring des fonctions sans avoir à les configurer.

6.1.14 Server Migration Service (SMS)

Le service de migration de serveurs (SMS) offre des services de migration Private to Virtual (P2V) et Virtual to Virtual (V2V) pour aider le Client à déplacer des données et des applications depuis des serveurs locaux x86 physiques ou des machines virtuelles sur des clouds privés (Flexible Engine Stack, Dedicated Cloud) ou cloud publics vers des machines virtuelles ECS sur des pools de ressources mutualisées (Elastic Cloud Server) ou dédiées (Dedicated Host).

6.1.15 Image Management Service (IMS)

Image Management Service (IMS) offre un libre-service flexible et des capacités complètes de gestion d'images. Lors de la création d'un ECS (Elastic Cloud Server) ou plusieurs ECS par lot vous pouvez utiliser une image publique ou créer une image privée.

Une image est un serveur en cloud ou un modèle de disque qui contient un système d'exploitation (OS), des données de service ou les logiciels nécessaires.

Image Management Service (IMS) vous permet de gérer l'ensemble du cycle de vie de vos images. Vous pouvez créer des ECS ou des BMS à partir d'images publiques, privées ou partagées. Vous pouvez également créer une image privée à partir d'un serveur en cloud ou d'un fichier image externe pour faciliter la migration des workloads vers le cloud.

6.1.16 Dedicated Storage Service (DSS)

Le Dedicated Storage Service (DSS) vous fournit des pools de stockage dédiés qui sont physiquement isolés des autres pools afin de garantir une sécurité élevée. Grâce à la redondance des données et aux technologies d'accélération du cache, DSS peut fournir des ressources de stockage hautement fiables, durables et à faible latence. En s'interconnectant de manière flexible avec différents services informatiques, tels que Dedicated Host (DeH), Elastic Cloud Server (ECS) et Bare Metal Server (BMS), DSS est parfait pour différents scénarios, tels que le calcul haute performance (HPC), le traitement analytique en ligne (OLAP) et les charges hybrides.

6.1.17 Cloud Bastion Host

Cloud Bastion Host (CBH) est une plateforme unifiée de gestion et de contrôle de la sécurité. Elle fournit des services de gestion des comptes, des autorisations, de l'authentification et de l'audit, qui vous permettent de gérer de manière centralisée les ressources de l'informatique en cloud.

Un système CBH comporte divers modules fonctionnels, tels que des modules de département, d'utilisateur, de ressource, de politique, d'opération et d'audit. Il intègre des fonctions telles que l'authentification unique (SSO), la gestion unifiée des actifs, les protocoles d'accès multi-terminaux, le transfert de fichiers, et la collaboration de session. Avec le portail de connexion O&M unifié, les technologies de protocole et les technologies d'isolation de l'accès à distance, CBH permet une gestion centralisée, simplifiée et sécurisée ainsi qu'un audit de la maintenance pour les ressources en cloud telles que les serveurs, les hôtes en cloud, les bases de données et les systèmes d'application.

6.1.18 Identity and Access Management

La gestion des identités et des accès (IAM) permet la gestion des identités et le contrôle d'accès des utilisateurs. Vous pouvez utiliser IAM pour gérer les comptes d'utilisateur (tels que les comptes d'employé, de système ou de programme d'application) et contrôler les autorisations d'exploitation de ces comptes d'utilisateur sur vos ressources (telles que les ressources informatiques, de stockage et réseau). De cette façon, IAM empêche ces comptes de partager votre mot de passe ou votre clé d'accès avec d'autres utilisateurs. IAM assure également la sécurité des comptes utilisateurs et réduit les risques de sécurité pour les informations de votre entreprise en vous permettant de définir des politiques de vérification de connexion, des politiques de mot de passe et une liste de contrôle d'accès (ACL).

6.1.19 Database Security Service

Database Security Service (DBSS) est un service intelligent de sécurité des bases de données. Basé sur le mécanisme d'apprentissage automatique et les technologies d'analyse des données de masse, il peut auditer vos bases de données, détecter les attaques par injection SQL et identifier les opérations à haut risque.

L'audit de base de données s'applique sur les services suivants :

- Instances RDS
- Bases de données construites sur ECS
- Bases de données construites sur BMS

Voici les différents caractéristiques des services :

- Sauvegarder et restaurer les journaux d'audit de la base de données et respecter les exigences de conservation des données d'audit.
- Surveiller les risques, les sessions, la distribution des sessions et la distribution SQL en temps réel.
- Signaler les alarmes en cas de comportements à risque et d'attaques et répondre aux attaques de bases de données en temps réel.
- Localiser les violations internes et les opérations inappropriées et protéger les actifs de données.

(Il est à noter que l'audit de base de données peut effectuer un audit flexible sur la base de données sans affecter les services utilisateur).

- Surveiller la connexion à la base de données, le type d'opération (définition des données, opération, contrôle) et l'objet d'opération en fonction des opérations à risque pour auditer efficacement la base de données.
- Analyser les risques, les sessions et l'injection SQL pour vous aider à maîtriser la situation de la base de données en temps opportun.

● Fournir une bibliothèque de modèles de rapport pour générer des rapports d'audit quotidiens, hebdomadaires ou mensuels en fonction de vos configurations.

● Envoyer des notifications d'alarme en temps réel pour vous aider à obtenir des rapports d'audit en temps opportun.

6.2 Les services de stockage

6.2.1 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.

Le Prestataire 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 du Prestataire.

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 trois gammes de performance :

- gamme standard
- gamme high I/O utilisant des disques SSD
- gamme ultra high/IO utilisant des disques SSD

6.2.1.1 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.

6.2.1.2 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.

6.2.2 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, tiède 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.

6.2.3 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.

6.2.4 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.

6.2.4.1 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.

6.2.5 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.

6.2.5.1 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 peut être exécuté 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.

6.2.6 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 :

Coûts supportés / **En phase de :**	**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	

6.2.6.1 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).
- Le Prestataire ne prend aucun engagement sur la fraîcheur des données (Recovery Point Objective) et la rapidité de reprise (Recovery Time Objective)

6.2.7 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.

6.2.7.1 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.

6.2.8 Scalable File Service Turbo (SFS Turbo)

SFS Turbo répond aux scénarios de service de type NAS, fournissant des services de fichiers avec une faible latence et des IOPS élevés.

- Interconnexion flexible : prend en charge l'interconnexion ECS et EVS, à déployer selon les besoins.
- Isolation : Chaque service SFS Turbo est dédié à son domaine et n'est pas partagé avec d'autres ECS ou EVS.

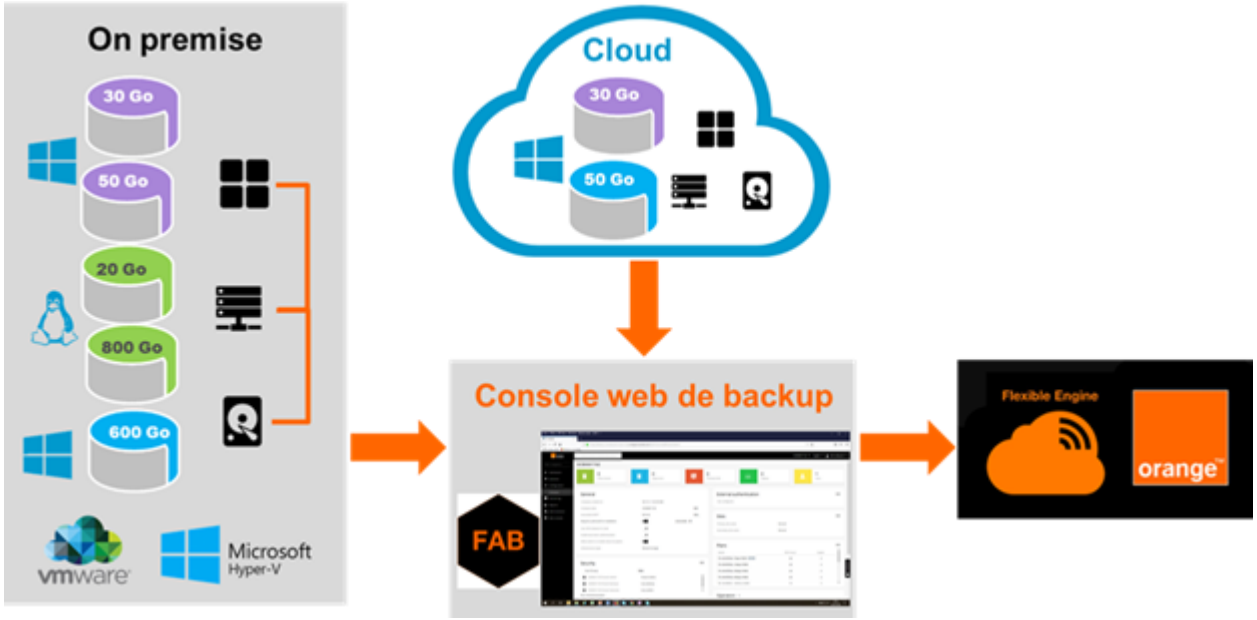
- Haute performance : supporte une latence de 1 à 2 ms et un IOPS maximum de 20 000.
- Prise en charge du protocole NFS standard, ainsi que le chiffrement, la sauvegarde et la restauration des données de fichiers.
- L'instance SFS Turbo offre une haute disponibilité au sein d'un AZ

6.2.9 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.

6.2.10 File and Application Backup

File & Application Backup (FAB) est un service de sauvegarde de Fichiers et d'Applications dans le Cloud du Prestataire en libre-service. Il permet de faire la sauvegarde des ressources hébergées dans des environnements on-premise ou Cloud comme présenté dans le schéma ci-dessous.



Fonctionnalités

Les sauvegardes supportées sont :

- Les fichiers, pour les serveurs Windows et Linux.
    - Disponible pour Windows et Linux, elle permet :
    - de protéger l'ensemble des données par défaut, ou de choisir certains répertoires ou fichiers unitaires,
    - d'utiliser des mécanismes de filtre pour exclure des fichiers de la sauvegarde (par nom, par type)
- Les bases de données
    - Disponible pour SQL Server, Oracle et MySql. Elle permet une sauvegarde consistante de vos bases de données. La restauration à la transaction près est disponible, selon le modèle de récupération de données défini sur vos bases de données.
- Infrastructure Exchange
- Office 365 (Exchange online)

  Cette fonctionnalité permet de sauvegarder vos boites mail Office 365 5exchange Online) qui s'appuient sur les annuaires Azure et permet de restaurer les données d'une manière granulaire.

Caractéristiques
FAB dispose des caractéristiques suivantes pour la protection de vos données :

- Interface web sécurisée afin d'accéder à votre outil de sauvegarde
- Protection de données au travers de tunnels chiffrés bout en bout
- Optimisation de votre bande passante en bénéficiant de mécanismes internes préconfigurés de compression et déduplication des données protégées
- Stockage Cloud intégré à la solution (stockage Objet Flexible Engine)
- Configuration prédéfinie des sauvegardes (1 sauvegarde chaque jour de la semaine entre 8h et 20h + 1 le week-end) tout en gardant le choix de la rétention des données protégées
- Sauvegardes à la demande selon vos besoins pour protéger vos données ponctuellement
- Navigation dans le temps pour la restauration de vos données à la date de leur sauvegarde
- Restauration de vos données sur leur source ou vers une destination de votre choix
- Gestion fine des éléments à protéger / restaurer (granularité au fichier)
- Gestion des versions (nombre de versions sauvegardées, délai de rétention).
- Gestion illimitée des accès à votre interface de sauvegarde pour définir vous-mêmes, sans contrainte, les administrateurs de votre sauvegarde
- Sécurisation de vos données par réplication de la sauvegarde vers une autre région Flexible Engine
- Tableaux de bord et rapports d'activité préconfigurés pour faciliter le suivi du service.

Accès au service
File and Application backup est disponible pour tout utilisateur disposant d'un domaine Flexible Engine. La demande d'accès et l'accès à la console utilisateur spécifique File and Application Backup se fait via l'Espace Client Cloud.

6.2.11 Cloud Backup and Recovery

Cloud Backup and Recovery (CBR) permet aux utilisateurs de sauvegarder leurs instances ECS et disques EVS et SFS Turbo... La politique de rétention (nombre et durée des sauvegardes) est paramétrable par l'utilisateur.

6.2.11.1 Cloud Disk Backup :

CBR permet de sauvegarder un ou plusieurs EVS du domaine du Client (disque système ou de données)

6.2.11.2 Cloud Server backup :

CBR permet au Client de sauvegarder un serveur entier sur la base d'instantanés pour les ECS et BMS. Il est conseillé d'utiliser la sauvegarde de serveur en nuage (Cloud Server Backup) dans les scénarios qui nécessitent une cohérence élevée des données, tels que les clusters RAID.

6.2.11.3 File System Backup :

CBR permet de sauvegarder les systèmes de fichiers SFS Turbo, puis d'utiliser les sauvegardes pour créer de nouveaux systèmes de fichiers SFS Turbo, afin d'éviter la perte de données importantes.

6.2.12 Data Express Service (DES)

Data Express Service (DES) est un service de transmission de données à l'échelle du téraoctet. Ce service utilise des supports de stockage physiques (Serveur NAS) pour envoyer des quantités importantes de données des centres de données d'entreprise vers le cloud. Il a pour objectif de résoudre les problèmes liés au transfert de données à grande échelle, tels que les coûts de réseau élevés et les temps de transfert prolongés.

Le service consiste à envoyer un serveur NAS sécurisé au centre de données du Client ainsi qu'un logiciel client (DES Client) qui doit être installé sur un système d'exploitation Linux. DES Client permet aux utilisateurs de choisir et de déplacer les données du site du Client vers un serveur NAS (parfois appelé "téléport") tout en les chiffrant. Les données sont ensuite déplacées vers le bucket OBS (Object Storage Service) choisi par le Client lorsque le téléport est envoyé au centre de données de Flexible Engine.

6.3 Les services de mise en réseaux

6.3.1 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.

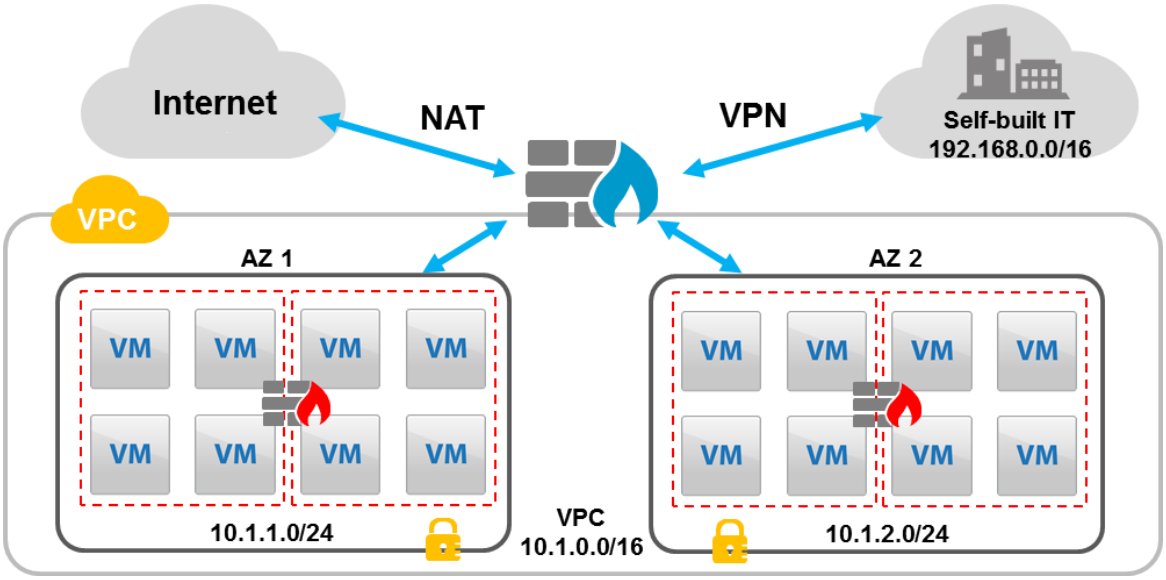


Figure n° 5: *VPC au sein d'une Région multi-AZ*

6.3.1.1 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.

6.3.2 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).

6.3.3 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.

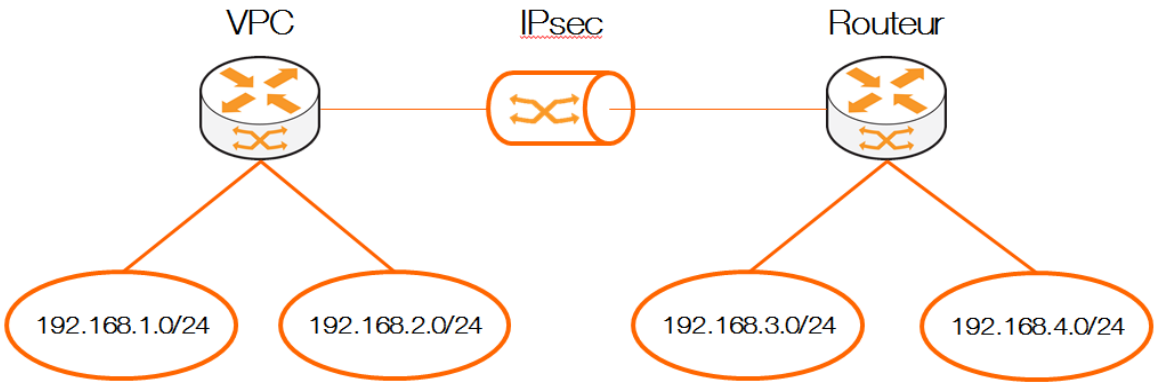


Figure n° 6: *Schéma de principe VPN IPsec*

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

6.3.4 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.

6.3.5 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.

6.3.6 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).

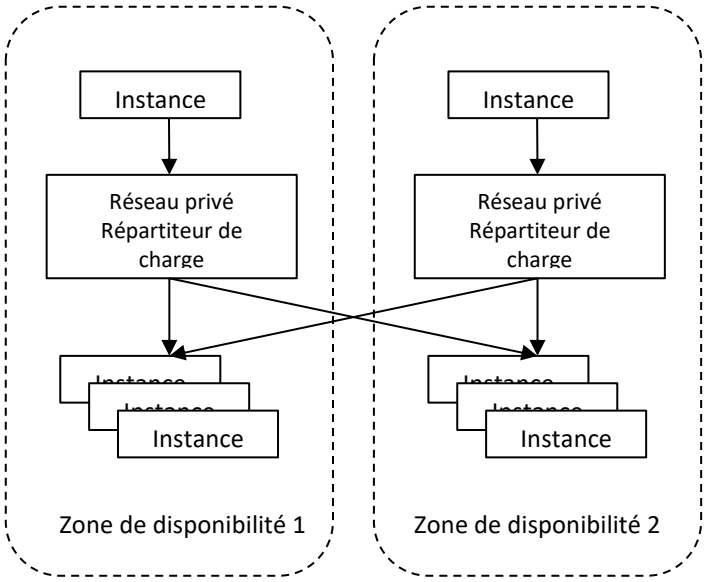


Figure n° 7: *Répartiteur de charge de réseau privé*

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.

6.3.7 Connexion à Internet

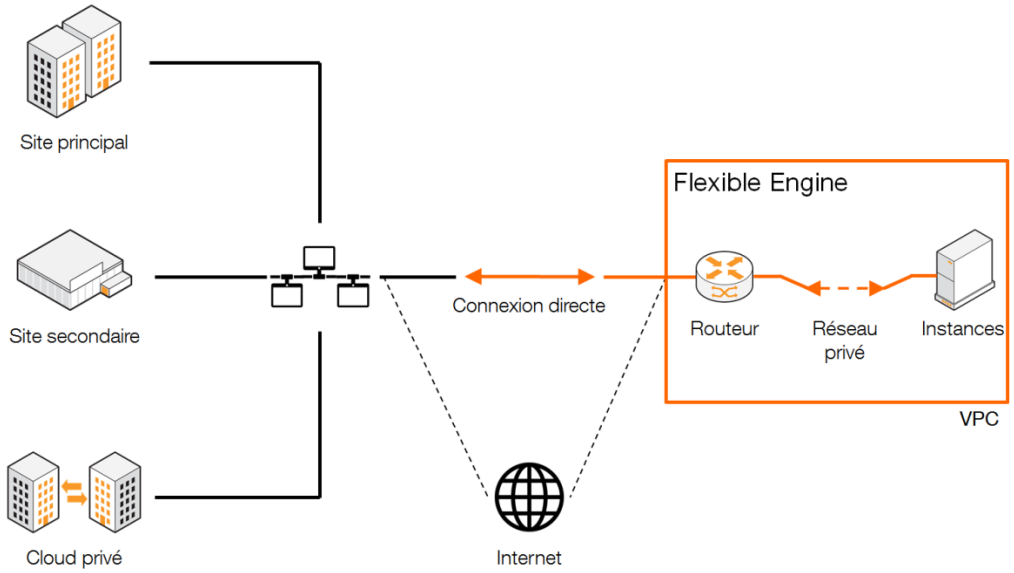
L'utilisation de la plateforme Flexible Engine par la Console ou par les API des Services est par défaut disponible à travers Internet et nécessite une authentification par login et mot de passe.

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.

6.3.8 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

6.3.8.1 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.

6.3.8.2 La Connexion Directe via un réseau partenaire

Les partenaires actuels sont : Le Prestataire (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

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.

6.3.9 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.

6.3.10 VPC Endpoint (VPCEP)

Le service VPC Endpoint (VPCEP) offre des canaux sécurisés et privés pour connecter le VPC du Client aux VPC Endpoints (services cloud sur la plateforme actuelle ou sur les services privés du Client), offrant une configuration de réseau flexible sans avoir besoin d'EIP.

6.3.11 NAT Gateway (NAT)

Le service NAT Gateway offre la fonction Network Address Translation (NAT) pour Elastic Cloud Servers (ECSs) dans un cloud privé virtuel (VPC), permettant à ces ECSs d'accéder à Internet en utilisant des adresses Elastic IP (EIPs) ou pour fournir des services à des réseaux externes.

6.3.12 Virtual Private Network

Le service Virtual Private Network (VPN) établit un tunnel de communication crypté entre un utilisateur distant et un cloud privé virtuel (VPC). Avec le service VPN, vous pouvez vous accéder aux ressources de ce VPC.

Par défaut, les ECS d'un VPC ne peuvent pas communiquer avec votre datacenter. Pour permettre les communications entre eux, il faut utiliser un VPN.

Un VPN se compose d'une passerelle VPN et d'une ou plusieurs connexions VPN. Une passerelle VPN fournit une sortie Internet pour un VPC et fonctionne avec la passerelle distante du réseau du site distant.

La connexion VPN vous permet de créer rapidement un environnement cloud hybride sécurisé.

6.3.13 Domain Name Service

Le service Domain Name Service (DNS) fournit directement la résolution de noms de domaine et des services de gestion de noms de domaine. Il traduit les noms de domaine ou les ressources applicatives en adresses IP nécessaires à la connexion réseau. Ce faisant, les demandes d'accès sont dirigées vers les ressources souhaitées.

Le service DNS assure les fonctions suivantes :

● Résolution des noms de domaines publics :

Associe les noms de domaine aux adresses IP publiques afin que les utilisateurs finaux puissent accéder à votre site Web ou à vos applications Web sur Internet.

● Résolution de noms de domaines privés :

Associe les noms de domaine privés en adresses IP privées pour faciliter l'accès aux ressources du cloud au sein des VPC.

● Résolution inverse :

Permet d'obtenir un nom de domaine sur la base d'une adresse IP. La résolution inversée, ou recherche DNS inversée, est généralement utilisée pour obtenir un nom de domaine à partir d'une adresse IP.

DNS, est généralement utilisée pour confirmer la crédibilité des serveurs de messagerie.

6.3.14 Direct Connect

Direct Connect est un service cloud qui vous permet d'établir une connexion réseau dédiée entre vos locaux et Flexible Engine. En utilisant Direct Connect, vous pouvez établir une connectivité privée entre Flexible Engine et votre centre de données, vos sites ou votre environnement de colocation. Vous pouvez aussi établir une connexion entre votre routeur et Flexible Engine.

Si une redondance est nécessaire, nous vous recommandons d'établir deux connexions se terminant à des emplacements différents. Une connexion consiste en une seule connexion dédiée entre les ports de votre routeur et le routeur Flexible Engine.

6.4 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.

6.4.1 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).

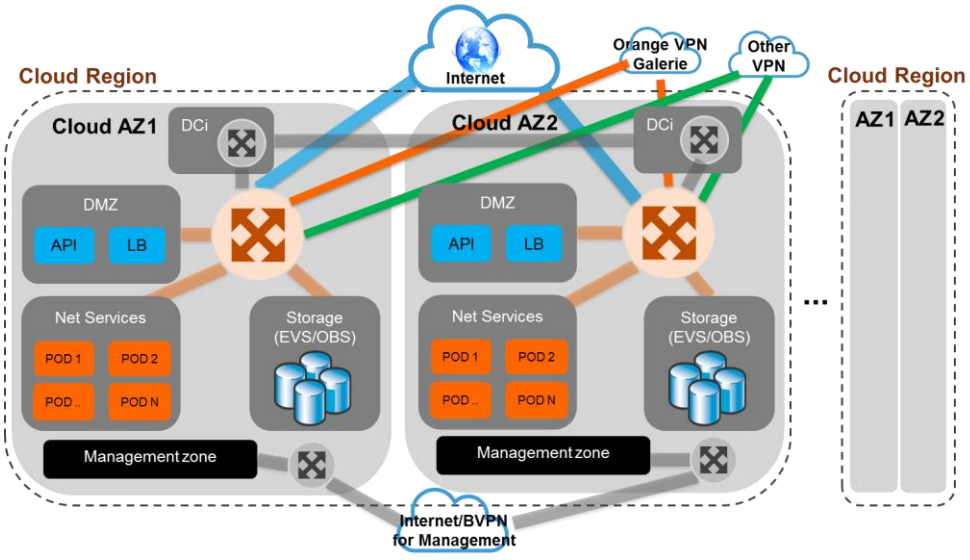


Figure n° 8: *Architecture logique / isolation des ressources*

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 le Prestataire 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.

6.4.2 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.

6.4.3 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).

6.4.4 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.

6.4.5 Web Application Firewall (WAF)

Le pare-feu d'application Web (WAF) a pour objectif d'accroître la stabilité et la sécurité des services Web ainsi que la gestion des risques afférents. Il examine toutes les requêtes HTTP et HTTPS pour détecter et bloquer les attaques suivantes : Injection de langage de requête structuré (SQL), scripts intersites (XSS), shells web, injections de

commandes et de code, inclusion de fichiers, accès aux fichiers sensibles, exploitation de vulnérabilités tierces, attaques Challenge Collapsar (CC), crawlers malveillants et falsification de requêtes intersites (CSRF).

Le WAF permet protéger des noms de domaine ou des adresses IP.

6.4.6 Host Security Service (HSS)

Host Security Service (HSS) est un gestionnaire de sécurité pour les serveurs. Il améliore la sécurité globale de l'hôte et fournit des fonctions telles que la gestion des vulnérabilités, la gestion des actifs, l'inspection de la ligne de base et la détection des intrusions afin de détecter plus rapidement les intrusions, dans l'objectif de répondre aux exigences de conformité.
Pour utiliser HSS, un agent doit être installé sur les serveurs Elastic Cloud (ECS) à protéger, ce qui permet au personnel O&M (opérations & maintenance) de gérer de manière centralisée la sécurité de l'hôte par le biais du centre de gestion de la sécurité.

6.4.6.1 Liste des ***fonctionnalités*** :

- Gestion des actifs : Gère et analyse les informations relatives aux actifs de sécurité, telles que le compte, le port ouvert, le processus, le répertoire Web et le logiciel.
- Détection des vulnérabilités : Détecte les vulnérabilités des systèmes et des logiciels (tels que Secure Shell, OpenSSL, Apache HTTP Server et MySQL) et fournit des suggestions de rectification.
- Inspection de base :Découvre les mots de passe faibles et les configurations système courantes afin d'identifier et de prévenir les risques.
- Détection des intrusions :Détecte et protège les comptes contre les attaques par force brute, les webshells, les mineurs de crypto-monnaies, les ransomwares et les chevaux de Troie.

6.5 Services d'analyse de données

6.5.1 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 entreHDFS, 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.

6.5.2 Cloud Stream Service (CS)

Cloud Stream Service est un service d'analyse de flux de données big data en temps réel fonctionnant sur le cloud public. Les clusters de calcul sont gérés par Cloud Stream. Cloud Stream Service est compatible avec les API Apache Flink, et les tâches Cloud Stream Service s'exécutent en temps réel.

Basé sur Flink et Spark Streaming, Cloud Stream intègre des fonctionnalités et une sécurité supplémentaires, et prend en charge les méthodes de traitement par flux et par lots. Cloud Stream Service est en fin de vie et la solution va évoluer vers Data Lake Insight (DLI).

6.5.3 Data Ingestion Service (DIS)

Le service d'ingestion de données (DIS) est un service de streaming en temps réel évolutif, capable de capturer et de traiter une grande quantité de données en continu pour des besoins spécifiques. Les données envoyées au DIS peuvent être stockées pour un traitement et une analyse hors ligne. Le DIS peut-être utilisé pour des scénarios existants tels que la capture de données de capteurs IoT, les clics de sites Web, les transactions boursières, les flux sociaux, l'application mobile de jeux de télémétries ou de capteurs de véhicules autonomes.

DIS est un système de service web géré Publish-Subscribe à haut débit et à messages distribués. L'utilisateur peut créer, supprimer, décrire le débit de flux via une console web.

6.5.4 Data Pipeline Service (DPS)

Data Pipeline Service (DPS) est un service web fonctionnant sur le cloud public. Il permet au Client d'automatiser le déplacement et la transformation des données entre différents services. Avec DPS, le Client peut définir un pipeline pour décrire les tâches de traitement des données, la séquence d'exécution des tâches et le plan de planification des tâches. DPS planifie et contrôle ensuite l'exécution des tâches sur la base du plan d'ordonnancement et de la relation prédéfinis, afin de réaliser le traitement et le mouvement des données entre les services. DPS est en fin de vie et évoluera vers le Data Lake Governance Center (DGC) qui sera lancé prochainement.

6.5.5 Data Warehouse Service (DWS)

Data Warehouse Service (DWS) est une base de données en ligne basée sur le cloud MPP (massively parallel processing). DWS fournit également certains outils pour l'exploitation et la maintenance de la base de données, y compris la sauvegarde et la restauration, la surveillance et la connexion à la base de données.

6.5.6 Cloud Search Service (CSS)

Cloud Search Service (CSS) est un service de recherche distribuée managé. Il est compatible avec les logiciels open source Elasticsearch et Opensearch et offre aux utilisateurs des fonctionnalités de recherche de données structurées et non structurées, de statistiques et de rapports. CSS fonctionne de la même manière qu'une base de données.

CSS peut être déployé automatiquement. CSS fournit des pratiques d'optimisation pour les moteurs de recherche et ne nécessite pas d'exploitation et de maintenance. En outre, il dispose d'un système de surveillance qui fournit des mesures clés, notamment sur les systèmes, les clusters et les performances des requêtes.

6.5.7 Data Lake Insight (DLI)

Data Lake Insight (DLI) est un service de traitement et d'analyse des données sans serveur compatible avec les SQL standard, Spark et Flink SQL. Il prend également en charge plusieurs modes d'accès, et est compatible avec les formats de données courants.

6.5.8 Data Lake Governance Center (DGC)

Data Lake Governance Center (DGC) est une plateforme unique de développement et d'exploitation de données à cycle de vie complet. Ce VPC fournit des fonctions telles que l'intégration, le développement, supporte la construction intelligente des bases de données de connaissances de l'industrie, et incorpore des fondations de données telles que le stockage, le calcul et les moteurs d'analyse de Big Data, aidant les entreprises clientes à construire des capacités d'exploitation de données.

6.5.9 Graph Engine Service (GES)

Le GES (Graph Engine Service) facilite l'interrogation et l'analyse des données de structure graphique en fonction de diverses relations. Il est particulièrement adapté aux scénarios nécessitant l'analyse de données de relations riches, notamment l'analyse des relations sociales, la recommandation marketing, les opinions publiques et l'écoute sociale, la communication d'informations et la lutte contre la fraude.

6.6 Services de base de données

6.6.1 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.

6.6.2 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.

6.6.3 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.

6.6.4 Data Replication Service (DRS)

DRS est un service cloud pour la migration et la synchronisation en ligne des bases de données en temps réel. Il simplifie les processus de migration de données et réduit les coûts de migration. Le Client peut utiliser DRS pour transmettre les données entre les bases de données dans divers scénarios.

6.6.5 Data Admin Service (DAS)

Data Admin Service (DAS) est une plateforme unique de gestion de bases de données cloud qui permet aux utilisateurs de gérer des bases de données sur une console web. Elle offre le développement de bases de données, l'exploitation et la maintenance (O&M), le diagnostic intelligent et le DevOps au niveau de l'entreprise, ce qui facilite l'utilisation et la maintenance des bases de données.

6.6.6 Distributed Database Middleware

Distributed Database Middleware (DDM) est un service middleware de base de données (désigné pour les données relationnelles distribuées) qui est compatible avec MySQL. Il utilise une architecture découplée du stockage (des ressources compute) qui facilite l'extension des ressources de calcul et de stockage pour traiter un grand nombre de demandes simultanées et de données.

6.6.7 DDM utilise une architecture de calcul et de stockage découplée qui fournit des fonctions telles que le partitionnement de bases de données et de tables, le fractionnement (lecture/écriture), la mise à l'échelle élastique (Elastic Scaling), l'exploitation et la maintenance durables. En outre, La gestion des nœuds d'instance n'a aucun impact sur vos charges de travail. Vous pouvez effectuer des opérations d'exploitation et de maintenance sur vos bases de données, lire ainsi qu'écrire des données, depuis et vers celles-ci, sur la console DDM. Tout cela, comme si vous exploitiez une base de données MySQL à nœud unique.GaussDB NoSQL

GaussDB NoSQL est un service de base de données NoSQL distribué, multi-modèle, avec une architecture de calcul et de stockage découplée et de stockage. Cette base de données haute disponibilité est sécurisée et évolutive, elle peut être déployée, sauvegardée ou restaurée rapidement, et inclut la surveillance et la gestion des alarmes.

6.7 Applications d'entreprise

6.7.1 WorkSpace [End of life]

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.

6.7.2 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. Par défaut, deux connexions sont fournies avec chacune des licences Windows server fournie par le Prestataire.

Pour utiliser plus de deux connexions simultanées, le client doit apporter des licences RDS/SAL dont il est titulaire en mode mobilité, dans les conditions décrites dans la section "Licences / Produits Microsoft". 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.

6.7.3 Office

Office est suite logicielle bureautique. Flexible Engine ne fournit pas ce type de licences. Chaque licence Office (Standard ou Professional Plus) doit être souscrite pour un seul Utilisateur, personne physique. Ces licences ne sont pas éligibles à la mobilité.

En revanche les licences « Office 365 Professional Plus » peuvent être apportées par le Client sur Flexible Engine, sous réserve d'être déclarées au Prestataire.

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

6.7.4 oneclick™

oneclick™ est un service Virtual Desktop Infrastructure (VDI) qui permet au Client de provisionner un environnement de poste de travail pour les Utilisateurs avec des services des disques et des systèmes d'exploitation dédiés. De cette façon, les Utilisateurs sont en mesure d'accéder à distance à leurs applications bureautiques habituelles à partir des appareils dédiés et de manière efficace.

La liste des services ECS dédiés est disponible sur la Console et est sujette à des évolutions.

Le service oneclick™ peut être acheté sous forme d'abonnement mensuel ou annuel selon les modèles de licence définis sur le site du fournisseur https://cloud.orange-business.com/en/offers/infrastructure-iaas/public-cloud/appliance-catalog/oneclick/ .

Le support du logiciel oneclick™ est assuré par la société oneclick qui doit être le premier point de contact. Les détails de contacts et les instructions pour ouvrir un ticket sont disponible sur le site web de oneclick : https://help.oneclick-cloud.com/en/ . Les heures d'ouverture spécifiques, les objectifs de disponibilité du service et les délais de réponse aux tickets sont indiqués à cette adresse : https://oneclick-cloud.com/en/general-service-level-agreement/ - niveau Gold.

6.7.5 Distributed Message Service (DMS)

Distributed Message Service (DMS) est un service évolutif de mise en file d'attente de messages, DMS est hébergé sur la plate-forme computing cloud. Grâce à l'utilisation de la technologie de cluster distribué, DMS prend en charge l'accès à grande échelle et à haute concurrence. Ce service dissocie les composants d'une application cloud.

DMS fournit une console Web pour gérer les files d'attente de messages et les interfaces de programmation d'application (API) pour accéder aux messages. À l'aide de la console DMS, le Client peut créer des files d'attente et effectuer des tests de production et de consommation de messages. Les applications utilisateur peuvent alors appeler directement les API RESTful, rendant le service DMS rapidement disponible pour les applications.

Un système de surveillance et de maintenance a été mis en place pour garantir un fonctionnement fiable du DMS.

Tous les messages stockés dans une zone de service de messagerie isolée sont protégés contre les accès non autorisés.

6.7.6 Distributed Message Service for Kafka

Distributed Message Service (DMS) pour Kafka est un service de mise en file d'attente des messages basé sur Apache Kafka et plus particulièrement sur les instances Kafka premium. Les ressources de calcul, de stockage et de bande passante utilisées par une instance sont dédiées par l'utilisateur.

Apache Kafka est un middleware de messages distribués qui offre un débit élevé, la persistance des données, l'évolutivité horizontale et le traitement des données en continu. Il adopte le modèle de publication et d'abonnement et est utilisé pour la collecte de journaux, le streaming de données, l'analyse de systèmes en ligne/hors ligne et la surveillance en temps réel.

6.7.7 Distributed Message Service for RocketMQ

Distributed Message Service (DMS) pour RocketMQ est un service orienté messages qui offre une faible latence, une grande flexibilité, un débit élevé, une scaling dynamique, une gestion facilitée et de nombreuses fonctions de messagerie.

DMS pour RocketMQ présente les caractéristiques suivantes :

- Compatibilité avec les clients open-source RocketMQ.
- Nombreuses fonctions de messagerie, y compris la livraison ordonnée des messages, les messages retardés, les messages planifiés, la relance des messages, les messages de type lettre morte et les messages transactionnels, qui répondent à divers besoins dans les scénarios de commerce électronique et de finance.
- Des fonctions de surveillance et d'analyse, notamment le traçage des messages, le suivi des messages, l'analyse des traces, l'exportation des messages de type lettre morte, la surveillance et les alarmes, qui permettent au Client de surveiller ses services et de les maintenir en état de marche.

6.7.8 Simple Message Notification (SMN)

6.7.9 Simple Message Notification (SMN) est un service de notification de messages, hébergé, flexible et à grande échelle. SMN permet au Client d'envoyer des messages à des adresses e-mail et des applications HTTP/HTTPS.Dedicated API Gateway

API Gateway (APIG) est votre service d'hébergement API entièrement managé. Avec APIG, vous pouvez créer, gérer et déployer des API à n'importe quelle échelle pour regrouper vos fonctionnalités. En quelques clics seulement, vous pouvez intégrer des systèmes internes, monétiser les capacités de service et exposer de manière sélective les fonctionnalités avec des coûts et des risques minimes.

● Pour monétiser vos services et vos données, vous pouvez créer des API dans APIG. Vous pouvez ensuite fournir les API aux appelants d'API à l'aide de canaux hors ligne.

● Vous pouvez également obtenir des API ouvertes auprès d'APIG pour réduire votre temps et vos coûts de développement.

6.8 Services pour les développeurs

6.8.1 Les API de Flexible Engine

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

6.9 Outils de monitoring

6.9.1 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.

6.9.2 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.

6.9.3 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.

6.9.3.1 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.

6.9.4 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.

6.9.5 Application Operations Management (AOM)

Application Operations Management (AOM) est une plateforme multidimensionnelle de gestion O&M pour les applications cloud. Elle surveille les applications et les ressources en cloud associées en temps réel, collecte et associe les métriques des ressources, les logs et les événements pour analyser l'état de santé des applications. Elle fournit également des rapports d'alarme flexibles et une visualisation des données qui facilitent la détection des erreurs.

Plus précisément, AOM surveille et gère uniformément les serveurs, les dispositifs de stockage, les réseaux, les conteneurs web et les applications hébergées dans Docker et Kubernetes, pour prévenir les problèmes et faciliter la localisation des pannes.

6.9.6 Log Tanks Service (LTS)

Log Tank Service (LTS) collecte et stocke les logs, permettant au Client de les interroger en temps réel. Il simplifie la prise de décision, aide à effectuer des opérations de routine et améliore l'efficacité du traitement des logs.

6.10 Container

6.10.1 Application Performance Management (APM)

6.10.2 Application Performance Management (APM) est un service de cloud qui surveille et gère en temps réel les performances et les défauts des applications déployées dans le cloud. Il permet l'analyse des performances des applications distribuées pour aider les exploitant à résoudre rapidement des problèmes tels que l'analyse d'erreurs et des impacts de performances dans l'architecture distribuée et améliorer ainsi l'expérience des utilisateurs finaux.Application Service Mesh (ASM)

Application Service Mesh (ASM) est une solution non intrusive qui permet au Client de gérer le cycle de vie et le trafic des microservices. Elle est compatible avec les écosystèmes Kubernetes et Istio et héberge un large éventail de fonctionnalités telles que l'équilibrage de charge, la coupure de circuit et l'injection de fautes. En outre, elle permet diverses méthodes de déploiement de type "graysacle", "canary" ou "blue-green".

6.10.3 Intelligent EdgeFabric (IEF)

Intelligent EdgeFabric (IEF) fournit aux utilisateurs une solution de déploiement de containeur à l'edge. En exploitant la synergie edge-cloud, les utilisateurs peuvent gérer les nœuds et les applications edge à distance tout en

continuant à traiter les données à proximité. En outre, ils peuvent effectuer des opérations et de la maintenance (O&M) dans le cloud, y compris la surveillance des noeuds edge, la surveillance des applications conteneurisées à l'edge et la collecte des logs.

6.10.4 Multi-cloud Container Platform (MCP)

Multi-Cloud Container Platform (MCP) fournit des solutions conteneurisées multi-cloud et hybrides-cloud pour la gestion unifiée des clusters entre les plateformes clouds (privées ou publiques), le déploiement unifié et la distribution du trafic des applications multi-clouds. Elle vise à résoudre la problématique de haute-disponibilité multi-cloud et joue un rôle important dans divers scénarios, notamment la répartition du trafic entre diverses plateforme, la séparation des services et des données ou encore la possibilité d'avoir des plateformes de développement et une production dans des environnement distinct (ex: public et on premise)

6.10.5 Software Repository for Container (SWR)

Software Repository for Container (SWR) permet de gérer des images de conteneurs Docker tout au long de leur cycle de vie, avec possibilité de push, pull et de suppressions des images.

Le dépôt d'images privé et la gestion fine des autorisations permettent d'accorder différentes autorisations d'accès, à savoir la lecture, l'écriture et la modification, à différents utilisateurs. Chaque fois qu'une image est mise à jour, l'application déployée dans Cloud Container Engine (CCE) avec cette image peut automatiquement être mise à jour. L'option de déclenchement active la mise à jour automatique de l'application.

Les utilisateurs peuvent push, pull et gérer des images Docker en utilisant la console SWR, les API SWR ou la Command Line Interface (CLI) de Docker.

6.11 Certification HDS pour Flexible Engine

La certification HDS de Flexible Engine garantit aux établissements de santé en France clients de Flexible Engine HDS que les services d'infrastructure qu'ils utilisent sont conformes au Code de la Santé Publique (Article L.1111-8), qui stipule que tout établissement de santé (hôpitaux, laboratoires pharmaceutiques) en France qui gère des données médicales personnelles doit faire appel à un prestataire de services certifié HDS.

Flexible Engine doit être utilisé en conjonction avec le niveau de support Business ou supérieur afin d'être certifié HDS.

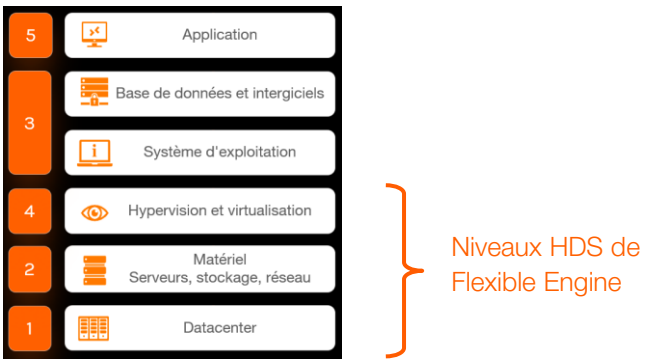
Les clients HDS de Flexible Engine ont accès à un service d'assistance francophone dont le personnel est formé à la certification HDS.

Flexible Engine HDS couvre les niveaux 1, 2 et 4 de la certification HDS. Le Prestataire n'intervient que sur ces niveaux. Il appartient au Client de s'assurer de l'applicabilité et, le cas échéant, de la conformité de la réglementation relative à l'hébergement de données de santé concernant les autres niveaux.

Niveau 1 = Centre de données

Niveau 2 = Matériel pour les serveurs, le stockage, le réseau

Niveau 4 = Infrastructures virtuelles



6.11.1 Audit

Le prestataire peut communiquer des rapports d'audit de certification aux clients qui en font la demande.

Le Prestataire fait régulièrement réaliser des audits internes en matière de sécurité de l'information. En outre, il peut faire réaliser des audits de tiers pour le compte du Client dans le respect des conditions prévues à l'article Protection des données personnelles des Conditions générales.

Dans le cadre du service Flexible Engine HDS, il est précisé qu'aucune Donnée de Santé à Caractère Personnel n'est transférée en dehors de l'Union européenne et/ou vers un pays ne disposant pas d'une législation sur le traitement des données à caractère personnel jugée adéquate par décision de la Commission européenne.

7 Support

Ce chapitre a pour objet de décrire les services de support fournis par le Prestataire 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 le Prestataire et le Client ;
- l'organisation et le périmètre des activités du support fourni par le Prestataire ;
- les prérequis à la fourniture du support par le Prestataire ;
- 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 ;

7.1 Domaine d'application

Les Fonctionnalités Béta ne donnent lieu à aucun engagement de support de la part du Prestataire.

7.2 Définitions

- **Le Catalogue** désigne le catalogue des Services tels que décrits dans le Descriptif de Services Flexible Engine
- **Un Incident** est une Interruption non prévue des Services ou une réduction de la qualité des Services.
- **Un Ticket** est un enregistrement dans l'outil de ticketing du Prestataire pour toute demande ou déclaration d'Incident sur les Services. Un Ticket est utilisé pour échanger des informations entre l'équipe Support Technique et les contacts nommés du Client lors de la gestion et du traitement d'une Demande ou d'un Incident sur les Services.
- **Un Problème** est un Incident sur les Services récurrent ou majeur qui a été résolu mais dont l'origine (sa cause) n'a pas encore été identifiée.
- **Une Erreur Connue** est un Incident sur les Services qui est déjà survenu (récurrent) et dont l'origine de la cause est connue.
- **Une Demande** est une demande du Client pour avoir une information, un conseil ou pour bénéficier d'un changement standard ou encore pour avoir accès à l'un des Services.
- **Une Perte de service** est une Interruption totale des Services causée par l'arrêt d'un ou plusieurs éléments constitutifs de la plateforme de production du Prestataire (critiques ou non critiques) et qui rend la fourniture du service concerné impossible.
- **Un Arrêt Planifié** est une période d'arrêt de la plateforme des Services qui a été planifiée et préalablement annoncée par le Prestataire. Durant cette période d'arrêt, tout ou partie des Services est indisponible.
- **Un Arrêt non-planifié** est un Incident qui survient en dehors de la période d'arrêt planifiée et duquel il résulte une perte des Services.
- **Le Help Center** désigne les pages documentaires de Flexible Engine accessible depuis la Console Flexible Engine.
- **Les Heures Ouvrées** se situent entre 09h00 et 19h00 (heure française), du lundi au vendredi, hors jours fériés français.
- **Les Services de Support** sont les services de support des Services délivrés par le Prestataire.
- **Les Offres de Support** sont les offres auxquelles le Client peut souscrire, donnant droit à différent niveaux d'engagement de Services de Support de la part du Prestataire.
- **Le Service Client** du Prestataire est le service client pour les Services de l'offre Flexible Engine.

- **Le Site Internet** désigne le site web cloud Orange Business du Prestataire dont l'url est http://cloud.orange-business.com/
- **Le Support Technique** du Prestataire est le support technique pour les Services.
- **Le point de contact unique (SPOC / Single Point Of Contact)** est l'ensemble de l'équipe Support Technique du Prestataire pour les Services du Catalogue qui est le contact dédié pour le Client en cas de Demande ou d'Incident.
- **Une Demande de Changement (RFC / Request For Change)** est une demande formelle d'amélioration ou de modification des Services, émise par le Prestataire, et qui détaille le changement requis. La description d'une RFC est indiquée dans la procédure de gestion des changements telle qu'indiquée au paragraphe « Gestion des changements » des présentes.
- **Un Contact Nommé** est un expert fonctionnel désigné par le Client ayant une bonne connaissance des Services. Seul un Contact Nommé est autorisé à émettre des Demandes ou déclarer des Incidents concernant les Services auprès du support technique du Prestataire.

7.3 Organisation des Services de Support

L'organisation des Services de Support s'articule autour de deux entités :

- le Service Client ;
- le Support Technique (International ou européen, selon le niveau de support).

Dans le cadre d'une souscription à une offre de Services de Support, le Client peut contacter le Prestataire pour:

- des Demandes de service ;
- la déclaration d'un Incident.

Le support du Prestataire a pour objectif de gérer les Demandes et Incidents, en réalisant les actions suivantes :

- prise en charge les Demandes et les Incidents, ainsi que leur traitement et résolution en suivant les procédures de gestion des Incidents et des Demandes telles que définies dans cette convention de service ;
- communication des informations appropriées et à jour au Contact Nommé du Client concernant le traitement des Incidents et des Demandes qui leur ont été dûment déclarés ;
- amélioration et mise à jour les procédures de support technique.

7.3.1 Les Offres de Support

Le Prestataire propose à ses Clients les Offres de Support suivantes :

- **Basic** : documentation, FAQ en ligne sur le Site Internet et sur le Help Center pour une consultation en autonomie pour l'ensemble des Clients des Services.
- **Standard** : offre de support conçue pour les Clients dont l'usage des Services est destiné à des développements d'applications hors production.
- **Business** : offre de support conçue pour les Clients dont l'usage des Services est destiné à des applications de production.
- **Business Europe** : offre de support conçue pour les Clients qui préfèrent que leurs données ne soient pas transférées ou accessibles depuis un pays hors Europe.
- **Premium** : offre de support conçue pour les Clients dont l'usage des Services est destiné à des applications de production exigeantes.

Les services de support sont souscrits pour un minimum de six (6) mois. Le client peut modifier sa Commande uniquement vers une offre de support plus élevée en gamme pendant la période d'engagement. Il est alors à nouveau engagé pour six (6) mois sur le nouveau niveau souscrit.

Les modifications de niveau de support prennent effet en début de mois calendaire.

Offres de support pour les services Flexible Engine	BASIC	STANDARD	BUSINESS	PREMIUM	BUSINESS EUROPE
Service Client					
Flexible Engine documentation via Help Center	Inclus	Inclus	Inclus	Inclus	Inclus
API documentation via Help Center					
Questions relatives au compte, aux souscriptions, à la facturation	Heures ouvrées	Heures ouvrées	Heures ouvrées	Heures ouvrées	Heures ouvrées
Site de support	Internati onal	International	International	International	Europe

Support Technique					
Supervision des data-centers 24h/24, 7j/7	Inclus	Inclus	Inclus	Inclus	Inclus
Moyens d'accès					
Ticket via l'Espace Client Cloud de Flexible Engine	Ticket receptionné 24h/24, 7j//7	Ticket receptionné 24h/24, 7j//7	Ticket receptionné 24h/24, 7j//7	Ticket receptionné 24h/24, 7j//7	Ticket receptionné 24h/24, 7j//7
eMail	N/A	N/A	N/A	Oui	Oui
Téléphone	N/A	N/A	Téléphone avec ticket préalable	Téléphone avec ticket préalable	Téléphone avec ticket préalable
Horaires de traitements des tickets	Jour ouvré	Jour ouvré	P1, P2: 24/7 P3: Heures ouvrées	24/7	P1, P2: 24/7 P3: Heures ouvrées
Temps de réponse (MTTI)					
MTTI sur incident p4	N/A	N/A	N/A	24 heures 5 jours ouvrés	N/A
MTTI sur incident p3	N/A	1 jour ouvré	1 jour ouvré	8 heures	12 heures ouvrées
MTTI sur incident p2	N/A	1 jour ouvré	2 heures	1 heure	2 heures
MTTI sur incident p1	N/A	12 heures ouvrées	1 heure	15 minutes	1 heure
Temps de rétablissement moyen (MTTR)					
MTTR sur incident P4	N/A	N/A	N/A	N/A	N/A
MTTR sur incident P3	N/A	N/A	N/A	N/A	N/A
MTTR sur incident P2	N/A	N/A	Incident API uniquement 4 heures	Incident API uniquement 4 heures	Incident API uniquement 4 heures
MTTR sur incident P1	N/A	N/A	Incident API uniquement 4 heures	Incident API uniquement 4 heures	Incident API uniquement 4 heures
Assistance sur les bonnes pratiques	Optionnel : Service de Cloud Coach				
Gestion des changements	Optionnel : Offres Managed Application				
Monitoring et supervision OS et applicatifs	Optionnel : Offres Managed Application				
Tarification					
Disponibilité en offre de service de support mono-tenant	N/A	Offre de support Standard mono-tenant	Offre de support Business mono-tenant	Offre de support Premium mono-tenant	Offre de support Business mono-tenant
Nombre de contacts nommés pour un service mono-tenant	N/A	2	5	Illimité	5
Disponibilité en offre de service de supports multi-tenants	N/A	N/A	Offre de support Business multi-tenant	Offre de support Premium multi-tenant	Offre de support Business multi-tenant
Nombre de contacts nommés pour un service multi-	N/A	N/A	Illimité	Illimité	Illimité

Tableau n° 1: *Tableau des Offres de Support*

7.3.2 Self-service pour le Support Flexible Engine

Différents supports et contenus documentaires sont à la disposition du Client sur le Help Center afin de l'accompagner dans l'utilisation des Services.

Documentation API : le Client pourra retrouver les fonctionnalités de la plateforme du Prestataire sur le Help Center et approfondir ses usages.

Ces contenus sont régulièrement mis à jour par le Prestataire.

7.3.3 Le Support Technique

L'équipe Support Technique traite les demandes du Client pour les Services et prend en compte les Incidents déclarés pendant les plages horaires et dans les délais impartis selon l'offre de support souscrite par le Client.

Au titre du Service de Support des offres STANDARD, BUSINESS ET PREMIUM, le Prestataire s'engage à :

- prendre en charge les Demandes et Incidents du Client selon les délais stipulés dans l'offre de support concernée ;
- répondre à toutes demandes d'information concernant le compte du Client, ses Contacts Nommés, ses factures ;
- répondre à toutes demandes d'information sur les fonctionnalités des Services ;
- faire ses meilleurs efforts pour résoudre tout Incident lié au bon fonctionnement des Services ;
- faire ses meilleurs efforts pour résoudre tout Incident sur les APIs des Services Flexible Engine ;
- faire ses meilleurs efforts auprès des Client ayant souscrit une offre de Support BUSINESS ou PREMIUM pour apporter une assistance technique liée à l'utilisation des systèmes d'exploitation fournis par le Prestataire dans le Catalogue. A toutes fins utiles, il est précisé que l'équipe support du Prestataire n'assure pas l'administration directe de systèmes dans le cadre du support de Flexible Engine.

En plus, pour le Service du Support de l'offre BUSINESS EUROPE :

- Les équipes de support N2 et N3 sont basées dans l'Union européenne.

Le Support Technique du Prestataire ne couvre pas :

- les Demandes et Incidents liés à des systèmes d'exploitation / logiciels tiers autres que ceux figurant dans la liste des images disponibles fournies par le Prestataire telle que décrite dans le Catalogue.
- les Demandes et Incidents liés à des systèmes d'exploitation / logiciels non fournis par le Prestataire ;
- les Demandes et Incidents liés à l'architecture ou au logiciel du Client ;
- les Demandes et Incidents liés à des taches d'administration système des machines virtuelles du Client ;
- le développement de code ou scripts.

7.4 Compétences et responsabilités du Client

Le Contact Nommé du Client habilité à contacter le Support Technique est une personne réputée formée et compétente sur l'usage du Cloud et des API des Services.

Le Client s'engage à mettre en place les bonnes pratiques d'usage du cloud et tous les moyens possibles pour traiter les Demandes et résoudre les Incidents déclarés sur son service avant de déclarer un Incident au Support Technique. Il dispose entre autre des API des Services mises à sa disposition pour intervenir par lui-même. Dans le cas où le Client ne serait pas en mesure de traiter la demande ou de résoudre l'Incident détecté sur les Services du fait d'un dysfonctionnement des Services, il pourra alors envoyer la Demande ou l'Incident auprès du Support Technique en suivant la procédure de gestion des Incidents décrite dans les présentes.

7.5 Les interfaces et moyens de contact du Support Client

Le Client devra fournir au Service Client la liste des Contacts Nommés qui sont les seuls habilités à faire une Demande ou déclarer un Incident auprès du Support Technique

Pour ce faire il communiquera au Prestataire une liste désignant nominativement les Contacts Nommés incluant a minima les informations suivantes :

- Nom ;
- Prénom ;
- Fonction ;
- Adresse mail ;
- Téléphone ;
- Plage horaire de disponibilité.

Ces Contacts Nommés seront les seuls points de contacts utilisés pour informer le Client de tout Incident détecté par le Prestataire sur les Services utilisés par le Client. Le nombre de Contacts Nommés habilités à contacter le support est défini dans le **Tableau des Offres de Support** des présentes.

7.6 Description du modèle de support

Le modèle de support définit l'organisation et les échanges entre le support du Client et celui du Prestataire.

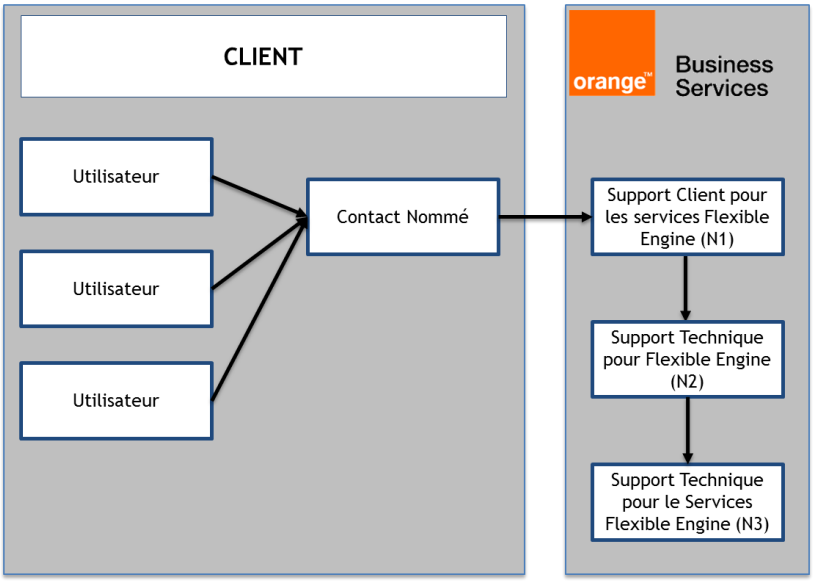


Figure n° 9: *Schéma : Modèle de support pour le Client*

7.6.1 Matrice RACI - support des Services

Dans le cadre des Service de Support, la matrice de responsabilité est la suivante :

Tâche	Client	Le Prestataire
Supervision des infrastructures virtuelles instanciées par le Client, des logiciels et des services du Client	R,A	
Implémentation des bonnes pratiques d'usage du cloud : automatisation des déploiements, procédures de redémarrage / redéploiement, mise en haute disponibilité, règles de sécurité, sauvegardes.	R,A	
Résolution des incidents des services ou des applications du Client en faisant usage éventuellement des API des Services	R,A	
Résolution des incidents liés aux Operating Systems et aux images du Client ou aux Operating Systems modifiés par le Client.	R,A	
Gestion des Demandes et Incidents liés aux Services fournis par le Prestataire	I	R,A
Supervision des infrastructures physiques et des services techniques du Prestataire	I	R,A
Gestion des Demandes de services (cf. Catalogue de Services)	I	R,A

R = Responsible / A = Accountable / C = Consulted / I = Informed

7.6.2 Monitoring des infrastructures virtuelles

Le Prestataire gère la surveillance de sa plateforme et des Services associés. Le périmètre de surveillance du Prestataire couvre l'ensemble des composants physiques (routeurs, firewalls, serveurs …), logiciels (nœuds OpenStack, hyperviseurs …) et services techniques (IAM, LDAP …), à l'exception des infrastructures virtuelles instanciées par le Client (Instances de serveurs cloud, OS, stockage).

7.7 Catalogue des processus

Le modèle de fourniture des Services couvre les principaux processus :

- Gestion des Incidents et des Problèmes ;
- Gestion des Demandes

- Demande standard
- Demande non-standard ;

- Gestion des mises en production ;
- Gestion des changements.

7.7.1 Gestion des Incidents

Cette section, décrit les étapes qui doivent être respectées par le Client pour gérer les Incidents qu'il déclare au Prestataire.

7.7.2 Déclaration d'Incident

7.7.2.1 Incident déclaré par le Client au Support Technique

Le Support Technique met en œuvre le processus de gestion des Incidents uniquement lorsque l'un des cas suivants survient :

- le Client a souscrit à une offre de support
- le Client a créé un Ticket à partir de son Espace Client Cloud, section « Besoin d'Aide »
- le Client envoie un e-mail au Prestataire s'il ne peut accéder à son l'Espace Client Cloud (Offre PREMIUM).
- le Client appelle le Support Technique pour déclarer un Incident critique ou majeur dans le cadre du contrat de support BUSINESS ou PREMIUM uniquement;

Les prérequis à l'ouverture d'un Ticket d'Incident sont les suivants :

- l'Incident concerne exclusivement les Services ; à titre d'exemple, un Incident ne concerne donc pas les architectures, les logiciels, les applications de production, les services conçus et exploités par le Client sur les Services.
- le Client a mis en œuvre les moyens de résolution de l'Incident à sa disposition notamment par l'utilisation des Services (entre autre les API des Services) et n'a pas pu aboutir à la résolution de l'Incident (cf chapitre 5 Compétences et responsabilités du Client)
- seuls les Contacts Nommés désignés par le Client peuvent contacter le support technique du Prestataire ;
- le Client a procédé à la collecte de toute information relative à l'Incident ;
- le Client renseigne les champs obligatoires dans son Ticket dans l'outil de ticketing de l'Espace Client Cloud selon les instructions communiquées par le Prestataire.

7.7.2.2 Processus spécifique en cas d'Incident déclaré par téléphone ou par e-mail

Les informations déclarées par e-mail ou téléphone doivent être complètes et précises.

Afin d'améliorer le processus de déclaration et permettre au Prestataire de traiter l'Incident, le Client s'engage à confirmer l'Incident au Support Technique en utilisant le modèle de déclaration d'Incident dont un modèle figure en annexe des présentes. A défaut, le Prestataire ne pourra traiter la demande du Client.

Afin d'être traités par le Prestataire, les Tickets ou, dans le cas du SUPPORT PREMIUM, les emails envoyés par l'équipe support du Client doivent impérativement contenir les informations suivantes :

- Email de l'administrateur du compte Client
- Objet: « [Numéro de Ticket issu de l'outil de ticketing du Client] Description de l'Incident ».
- Corps: les informations attendues sont décrites ci-dessous dans le « modèle de déclaration de Ticket »

Modèle de déclaration de Ticket		
	Obligatoire	**Description**
> Information Client		
# Information au sujet du déclarant		
Nom de la société du Client	Oui	
Nom du déclarant et fonction	Oui	La personne qui déclare l'incident (ex. un Contact Nommé)
Email du déclarant	Oui	

Téléphone du déclarant	Oui	
# Information au sujet de l'utilisateur		
Nom / prénom de l'utilisateur	Oui	La personne rencontrant l'incident (ex : un Client Final, un utilisateur du Client …)
Email de l'utilisateur	Oui	
Téléphone de l'utilisateur	Non	
> Information sur le Ticket		
# Contexte		
Categorie du Ticket : demande, incident, problème, information	Oui	Permet à l'équipe support de mieux évaluer la nature du ticket
Criticité perçue par le Client : critique, majeur, mineur	Oui	Permet à l'équipe support de mieux évaluer l'urgence de traitement du ticket
ID du tenant	Oui	Clé essentielle permettant à l'équipe Support d'investiguer l'incident.
ID des ressources concernées par l'incident	Oui	Exemple : InstanceID, routerID,…
Service du Prestataire concerné	Oui	Services Compute ou Stockage Objet
Composant impacté	Oui	Services Compute : Authentification, réseau, bloc storage Stockage Objet : authentification, upload/download de fichiers
Login API	Oui	
URL de l'API	Oui	URL utilisée pour accéder à l'API
Adresse IP source accédant à l'API	Oui	L'adresse IP qui accede à l'API
# Description		
Description de l'incident	Oui	Explication du contexte de l'incident
Date et Heure de l'incident	Oui	
Message d'erreur	Si affiché	
Code d'erreur	Si affiché	
Fichier(s) attaché(s)		
Capture d'écran de l'incident	Si pertinent	
Logs relatifs à l'incident	Si pertinent	

Une fois le Ticket créé par le Client, les équipes de support du Prestataire informe le Contact Nommé du Client par édition du Ticket. L'échange entre le Client et le Support Technique se poursuit alors au travers de l'outil de gestion des tickets de l'Espace Client Cloud du Client.

En cas d'échange par email ou par téléphone, un Ticket sera obligatoirement créé et le suivi se fera au travers de ce Ticket.

L'équipe Support Technique définira le niveau de priorité approprié pour l'Incident créé, en se basant sur la criticité de ce dernier. A ce titre, le Support Technique se réserve le droit de modifier la priorité d'un Incident déclaré par le Client.

7.7.3 Traitement des Incidents

Une fois le Ticket créé, le Client est informé par e-mail du statut de traitement de l'Incident.

Le Prestataire s'engage à prendre en compte et faire un premier retour au Client dans des délais qui dépendent de la Criticité de l'Incident (selon la « Matrice de priorité des Incidents » des présentes) et de l'Offre de Support souscrite par le Client. Les engagements de Temps de Réponse Moyen Initial (MTTI) sont décrits dans le **Tableau des Offres de Support** du chapitre 4.1 des présentes.

Il est entendu que tout Ticket ne relevant pas du périmètre de support assuré par le Prestataire sera automatiquement fermé par ce dernier.

En cas de conflit sur le niveau de priorité d'un Incident, le Prestataire appliquera la procédure de re-priorisation telle que décrite au paragraphe « Modification de la sévérité d'un Ticket d'Incident ».

Le Client peut demander au Prestataire de lui fournir un support au travers de la Console Flexible Engine ou des APIs de son tenant. Dans ce cas, il appartient au Client d'inviter la personne du support du Prestataire temporairement dans son tenant.

La personne du support du Prestataire invitée par le Client aura temporairement les mêmes droits que le Client sur la configuration de son tenant.

Lorsque le Prestataire aura terminé son intervention, il appartiendra au Client de supprimer l'invitation de la personne du support du Prestataire.

7.7.3.1 Résolution d'Incident

Une fois que la solution pour résoudre l'Incident a été trouvée (solution de contournement, patch …), l'équipe Support Technique changera le statut du Ticket de « En cours / In progress » à « Résolu / Resolved» et le Client en sera notifié par e-mail.

- si la résolution de l'Incident nécessite une mise en production d'un code applicatif : le Ticket d'Incident sera considéré comme résolu une fois que le code sera disponible dans l'environnement de pré-production, attendant d'être déployé dans l'environnement de production. En cas d'Incident le nécessitant, le processus de mise en production urgente sera appliquée (cf. paragraphe « Changement Urgent »).
- si la résolution ne nécessite pas une mise en production d'un code applicatif, l'Incident sera considéré comme résolu une fois que la solution aura été appliquée dans l'environnement de production.

7.7.3.2 Clôture d'Incident

Lorsque la résolution est confirmée par le Client, le Ticket sera clos par l'équipe Support Technique.

A défaut de confirmation par le Client dans les cinq (5) jours ouvrés à compter de la résolution de l'Incident, le Ticket sera automatiquement clos.

7.7.3.3 Matrice de priorité des Incidents

La Matrice de priorité des Incidents donne la définition de chaque niveau de priorité pour tout Incident sur les Services.

Priorité des Incidents	Définition
P1 – CRITIQUE	Un Incident de priorité 1 signifie ▪ qu'une des API suivante est totalement et durablement indisponible : • API ECS (Elastic Compute Service) • API IMS (Images Service) • API EVS (Elastic Volume Service) • API VPC (Virtual Private Cloud) • API IAM (Identity Authentification Management) • API OBS (Objet Storage Service) • API CCE (Cloud Container Engine) • API MRS (MAP Reduce Service) • API RDS (Relational Database Service) ▪ ou que **l'ensemble des instances et des volumes disques attachés aux** instances du tenant concerné est indisponible, et qu'il est impossible de créer de nouvelles instances et de nouveaux volumes, dans le tenant en utilisant les API des Services. Le Prestataire s'engage sur une Garantie de Temps de Rétablissement (GTR) de 4 heures pour les Clients ayant souscrit une Offre de Support BUSINESS ou PREMIUM, pour les API suivantes : ▪ API ECS (Elastic Compute Service) ▪ API IMS (Images Service) ▪ API EVS (Elastic Volume Service) ▪ API VPC (Virtual Private Cloud) ▪ API IAM (Identity Authentification Management) ▪ API OBS (Objet Storage Service) ▪ API CCE (Cloud Container Engine) ▪ API MRS (MAP Reduce Service) ▪ API RDS (Relational Database Service)

P2 – MAJEUR	Un Incident de priorité 2 signifie que le Service de Stockage Objet (OBS) et/ou le Service Compute (ECS) est disponible mais qu'il présente des dysfonctionnements ayant un fort impact sur son utilisation. Ce cas se produit lorsqu'un ou plusieurs éléments constitutifs de la plateforme du Prestataire (critiques ou non critiques) dégradent de manière significative le service concerné. Sont considérés comme des Incidents P2: ▪ une indisponibilité partielle du service concerné. • exemple : échecs d'authentification auprès de l'API IAM qui surviennent de manière intermittente mais récurrente. ▪ une indisponibilité totale d'une ou plusieurs fonctionnalités dégradant significativement le service concerné. • exemple Service Compute (ECS) : impossibilité de démarrer de nouvelles instances, mais les instances existantes fonctionnent. • exemple Service de Stockage Objet (OBS): impossibilité d'uploader un fichier dans le container, mais les fichiers déjà uploadés sont disponibles. • exemple : Perte de connectivité réseaux par intermittence ou forte dégradation démontrée de la qualité des connexions réseaux.
P3 - STANDARD	Un Incident de priorité 3 signifie que le Service de Stockage Objet (OBS) et/ou le Service Compute (ECS) est disponible mais qu'il présente des dysfonctionnements ayant un faible impact sur l'utilisation dudit service. Ce cas se produit lorsqu'un ou plusieurs éléments constitutifs de la plateforme du Prestataire (critiques ou non critiques) dégradent de manière non significative le service concerné, les fonctionnalités essentielles du service concerné restant opérationnelles. Sont considérés comme des Incidents P3 : ▪ un bug applicatif qui modifie l'affichage d'informations relatives à l'utilisation des Services. • exemple : Problème de feuilles de style sur la Console Flexible Engine ▪ une indisponibilité partielle du service concerné causée par un événement ponctuel et temporaire et dont il est possible de restaurer immédiatement la pleine disponibilité du service concerné. • exemple : redémarrage d'un hyperviseur ou d'un firewall. ▪ une indisponibilité partielle d'une ou plusieurs fonctionnalités ayant un impact faible sur l'utilisation du service concerné. • exemple Service Compute (ECS): impossibilité de renommer une machine virtuelle. • exemple Stockage Objet (OBS): impossibilité de lister des fichiers présents dans un container.
Non couvert	Les cas suivants, notamment, ne sont pas couverts : ▪ tout Incident n'ayant pas d'impact sur la plateforme de production ▪ tout Incident lié aux outils de statistiques ▪ tout Incident lié à l'outil de ticketing ▪ tout arrêt de la plateforme causé par une activité planifiée, telle que la maintenance, ou activités ou évènements dont le Prestataire n'a pas la maitrise, tels des dommages dus à un incendie ou bien une coupure du réseau dû au sectionnement d'un câble. En tout état de cause, le Prestataire restera responsable des actions de ses sous-traitants.

7.7.3.4 Modification du niveau de priorité d'un Ticket d'Incident

Le niveau de priorité d'un Ticket d'Incident pourra être modifié comme suit :

Diminution du niveau de priorité des Tickets d'Incidents

Quand un Incident critique P1 ou majeur P2, déclaré par le Client, ne respecte pas les définitions de la matrice de priorité des Incidents, l'équipe Support Technique peut diminuer le niveau de priorité du Ticket.

Le Client peut fournir des informations complémentaires et des détails au sujet de l'Incident, de ses impacts et expliquer le choix de la priorité de l'Incident à l'équipe Support Technique (durant cette période, le statut du Ticket sera modifié de « En cours / In progress » à "En attente / On hold") :

- Si l'Incident correspond bien au niveau de priorité défini par le Client, le niveau défini reste inchangé ;
- A défaut, le niveau de priorité du Ticket est diminué.

En cas de désaccord, le Prestataire définira en dernier ressort le niveau de priorité d'un Incident.

b) Augmentation du niveau de priorité des Tickets d'Incidents

Quand un Incident standard P3, ou un incident majeur P2 déclaré par le Client, ne respecte pas les définitions de la matrice de priorité des Incidents, l'équipe Support Technique peut augmenter le niveau de priorité du Ticket.

Le Client peut fournir des informations complémentaires et des détails au sujet de l'Incident, de ses impacts et expliquer le choix de la priorité de l'Incident à l'équipe Support Technique (durant cette période, le statut du Ticket sera modifié de « En cours / In progress » à "En attente / On hold") :

- Si l'Incident correspond bien au niveau de priorité défini par le Client, le niveau défini reste inchangé ;
- A défaut, le niveau de priorité du Ticket est augmenté.

En cas de désaccord, le Prestataire définira en dernier ressort le niveau de priorité d'un Incident.

7.7.4 Gestion des Problèmes

Le processus de gestion des Problèmes est un processus interne au Prestataire et est assuré par le gestionnaire des Problèmes du Prestataire . A ce titre, le Prestataire n'est tenue à aucun engagement vis-à-vis du Client sur ce périmètre.

Dans le cadre de la mise en place de ce processus de gestion des Problèmes, le Prestataire fait ses meilleurs efforts pour :

- rechercher la (ou les) cause(s) principale(s) qui engendre(nt) les Incidents ;
- identifier la solution qui doit permettre de résoudre définitivement les Incidents ;
- mettre à disposition du Processus Gestion des Incidents des préconisations et bonnes pratiques afin d'assurer la résolution des Incidents dans les meilleures conditions.

Le Prestataire pourra déclencher le processus de gestion des Problèmes en cas d'Incidents critiques P1, d'Incidents récurrents ou d'Incidents dont la root cause n'est pas identifiée.

Si un Problème peut être résolu par une nouvelle version d'un code, d'une application…, il sera traité dans le cadre du processus des changements et/ou des mises en production.

7.7.5 Gestion des mises en production

7.7.5.1 Mise en production de versions majeures

Définition d'une version majeure (code release majeure) : Evolution majeure des Services apportant un ensemble de nouvelles fonctionnalités ayant un impact fort sur les Services ou modifiant de façon structurante l'architecture applicative.

Le planning des mises en production est géré par le Prestataire. Les versions majeures qui sont mises en production correspondent aux versions des Services.

Le Client est informé par le Prestataire d'une mise en production d'une version majeure avec un délai de prévenance de dix (10) jours ouvrés.

Dans le cas d'une évolution de version d'API des Services qui impliquerait une incompatibilité avec la version antérieure de l'API, le Prestataire s'engage à informer le Client avec un délai de prévenance de soixante (60) jours minimum.

En pareille hypothèse, le Client procédera aux mises à jour nécessaires afin d'assurer la compatibilité de ses services avec les Services. A défaut de mise à jour, le Prestataire ne pourra pas assurer les prestations de support.

7.7.5.2 Mise en production de versions mineures

Définition d'une version mineure (code release mineure) : Toute évolution non qualifiée de majeure. Une version mineure intègre généralement des éléments de correction applicative (bug fix) et/ou des évolutions mineures de composants applicatifs déjà déployés et/ou de nouvelles fonctionnalités ayant un impact faible sur le service concerné.

Le Client est informé par le Prestataire d'une mise en production d'une version mineure avec un délai de prévenance de 24h.

7.7.6 Gestion des demandes

7.7.6.1 Catalogue des demandes de services

Seuls les Contacts Nommés du Client auront la possibilité de formuler des Demandes de service au Prestataire via l'Espace Client Cloud du Client ou par email en spécifiant dans l'objet de la Demande « demande de Support ».

Seules les Demandes suivantes sont possibles pour les Services Flexible Engine :

Nom de la Demande	Type de Demande	Description	Pré-requis	Délai de traitement (à compter de la prise en compte par le Service Client du Ticket)
Demande de création de compte	Standard	Création d'un tenant pour un Client Final sur demande du Client	Ouverture d'un Ticket-demande contenant l'ensemble des informations nécessaires à l'ouverture de compte doit être fournies dans la demande	2 jours ouvrés
Demande de suppression de compte	Standard	Suppression du tenant d'un Client Final sur demande du Client	Ouverture d'un Ticket-demande - le Client aura supprimé toutes les données et stoppé tous les Services à date de la demande	10 jours ouvrés
Demande de modification de quota	Standard	Modification des quotas pour les Services	Autorisation préalable du Prestataire Le Client motivera sa demande en fournissant ses besoins et prévisions d'usage attendus	5 jours ouvrés

7.7.6.2 Demande standard

Une Demande standard ne nécessite pas de développement spécifique. Il s'agit d'une action opérationnelle réalisée par l'équipe support Le Prestataire, à la demande du Client.

Les catégories de Demande standard sont intégrées au catalogue des Demandes de services d'Orange CLOUD FOR BUSINESS tel qu'indiqué à l'article « Catalogue des demandes de Services » des présentes.

Ce type de Demande est pris en charge par l'équipe Support Technique dans le cadre du processus de gestion des Demandes, via des Tickets de type « demande de support ».

7.7.6.3 Demande Non-Standard

Il s'agit d'une Demande qui n'est pas contenue dans le catalogue des Demandes de Services tel qu'indiqué à l'article « Catalogue des Demandes de Services » des présentes. Le Service Client du Prestataire peut être sollicité par le Client, mais Le Prestataire n'est tenu à aucun engagement sur son traitement.

7.7.7 Gestion des changements

7.7.7.1 Demande de Changement (RFC)

Les demandes de changement seront traitées par le processus de Gestion des changements. Ce processus interne au Prestataire permet de garantir une bonne gestion des différents changements opérés sur la plateforme de production du Prestataire. A ce titre, Le Prestataire n'est tenue à aucun engagement vis-à-vis du Client sur ce périmètre.

7.7.7.2 Changement standard

Un changement standard est un changement pré-approuvé qui présente un risque faible, plutôt courant, et qui suit une procédure ou une instruction de travail. Une Demande de Changement (RFC) n'est pas nécessaire pour réaliser un changement standard et son approbation par le comité d'autorisation des changement du Prestataire pour les Services Flexible Engine n'est pas requise.

7.7.7.3 Changement urgent

Pour des raisons critiques de sécurité ou de maintien en condition opérationnelle (pour résoudre un Incident critique ou majeur) sur les Services, Le Prestataire peut réaliser des changements urgents (mise en production d'un code applicatif, opération de maintenance sur les infrastructures …).

Les changements urgents sont réservés à des opérations destinées à corriger des Incidents critiques ou à corriger des dysfonctionnements majeurs ayant un impact immédiat ou imminent sur les services de production.

Ces changements urgents sont soumis à l'approbation du comité d'autorisation des changements urgents du Prestataire (qui se réunit lorsque la situation le nécessite).

7.7.7.4 Changement normal

Tout changement non catégorisé comme standard ou urgent, est considéré comme normal. Les changements normaux sont soumis au comité d'autorisation des changements du Prestataire.

7.7.7.5 Notification de changement

Les trois types de changements, détaillés ci-dessus, peuvent être réalisés par le Prestataire à travers :

- la mise en production de code applicatif ;
- un changement lié à l'infrastructure ;
- un changement lié à une maintenance.

Les informations concernant le délai de prévenance, la durée de l'interruption de service et les notifications sont listées ci-dessous, réparties en fonction du niveau de priorité de ces changements.

TYPE DE CHANGEMENT	NATURE DU CHANGEMENT	DELAI DE PREVENANCE	INTERRUPTION DE SERVICE
URGENT	Code release urgente	Orange Cloud for Business informe le CLIENT dès que possible	Maximum of 3 heures par mois par service concerné
	Maintenance corrective urgente		
NORMAL	Code Release	24 h	
	Code Release Majeure	10 jours ouvrés	
	- Maintenance corrective non-urgente - Maintenance préventive	24 h	
STANDARD	- Demande de service inclus au catalogue de service - Taches techniques sans impact sur la production	N/A	N/A

8 Limitations de Service

8.1 Quota de ressources

Afin de se prémunir contre les usages abusifs ou incontrôlés, le Client est informé que le Prestataire fixe un quota maximal de ressources dans le cadre de l'utilisation des Services. Ce quota peut être ajusté à la demande du Client sous réserve d'acceptation par le Prestataire. Ce quota est disponible en consultation dans la Console Flexible Engine.

8.2 Sauvegardes

Il appartient au Client de réaliser les sauvegardes de ses machines virtuelles et de ses données. Sauf prestation spécifique, les Services Flexible Engine n'incluent pas de sauvegardes systématiques par le Prestataire. Par conséquent, le Prestataire ne peut être tenu responsable de reconstruire les données dans le cadre de l'offre Flexible Engine.

9 ANNEXE 1 : Responsabilités du HDS

L'objectif de cette annexe est de définir les responsabilités du client et du fournisseur pour se conformer aux réglementations HDS. Elle est destinée à être utilisée conjointement avec la description du service Flexible Engine qui définit l'HDS Flexible Engine.

9.1 Matrice des responsabilités du client et du prestataire

	Règle	Détail de la règle	Responsabilité	Responsabilité des clients	Responsabilité du fournisseur
Respect des droits des personnes	Présentation des services aux personnes concernées	Présenter les modalités permettant de garantir l'absence d'opposition pour un motif légitime de l'intéressé à l'hébergement des données le concernant	Client	Le client doit obtenir ou s'assurer de l'absence d'opposition pour un motif légitime de la part des personnes physiques ("patients") dont les données de santé à caractère personnel sont traitées. Ces personnes doivent être clairement informées des éléments suivants - Que l'hébergement de leurs données est sous-traité au prestataire. - Sur les modalités d'accès et de transmission de ces données, étant rappelé que le prestataire n'assurera pas ces obligations.	N/A
	Consentement des personnes à l'accès aux données	Présenter les méthodes utilisées pour garantir que l'accès aux données de santé à caractère personnel et leur transmission éventuelle n'ont lieu qu'avec l'accord des personnes concernées et des personnes désignées par elles.	Client	Le Client est seul responsable de l'accès aux applications professionnelles et aux données personnelles de santé qu'il peut donner à son personnel ou aux professionnels de santé ou directement aux patients.	N/A
	Droits des personnes dans le cadre du GDPR	Mettre à disposition les procédures et moyens pour répondre aux demandes d'exercice des droits des personnes concernées définis par les articles 15 à 22 du RGPD (accès, rectification, effacement, limitation du traitement, portabilité, opposition).	Partagé	Le client est responsable du processus de prise en compte des demandes d'exercice des droits des personnes concernées tels que définis par les articles 15 à 22 du GDPR.	Le Prestataire s'engage à mettre à disposition les procédures et moyens permettant à ses Clients de répondre aux demandes d'exercice des droits des personnes concernées. Les droits visés sont ceux définis par les articles 15 à 22 du RGPD (accès, rectification, effacement, limitation du traitement, portabilité, opposition).

	Règle	Détail de la règle	Responsabilité	Responsabilité des clients	Responsabilité du fournisseur
	Notification en cas de divulgation de données à caractère personnel	Une procédure doit définir les modalités de notification au client d'une transmission à la suite d'une saisie judiciaire, sauf si cette notification est interdite	Partagé	Le client est responsable de la procédure de notification en cas de divulgation de données à caractère personnel.	Le prestataire s'engage à mettre en place une procédure de notification au client en cas de divulgation de données à caractère personnel dans le cadre d'une saisie judiciaire, sauf si cette notification est interdite.
	Objectif	L'hôte ne traite les données à caractère personnel que sur la base d'instructions documentées du client et ne doit pas s'écarter des objectifs spécifiés dans les instructions.	Partagé	Le client s'engage à ne pas traiter les données personnelles fournies par les patients à d'autres fins que celles indiquées dans le consentement.	Le prestataire s'engage à ne pas traiter les données personnelles fournies par ses clients à des fins autres que celles prévues pour l'exécution du contrat du client.
	Gestion des informations personnelles	L'hébergeur doit avoir défini et formalisé une politique de mise à disposition et de restitution des données personnelles à ses clients, ainsi que leur destruction	Le fournisseur	N/A	Le prestataire dispose d'une procédure de réversibilité pour la restitution des données de santé à caractère personnel en cas de résiliation du contrat ou de retrait de la certification.
Contrôle d'accès	Identifiants et autorisations	L'accès aux données personnelles ou aux systèmes utilisés pour leur traitement doit se faire par le biais de comptes nominatifs	Partagé	Le Client est responsable de la mise en œuvre des moyens techniques destinés à assurer l'identification, l'authentification et le contrôle d'accès aux données de santé pour les établissements et les professionnels de santé, pour les personnes concernées par les données hébergées, et pour les autres acteurs (par exemple éditeurs ou intégrateurs) au niveau des applications hébergées du Client.	Dans le cadre d'une offre IaaS, les équipes du Prestataire n'ont pas accès aux données de santé. En ce qui concerne l'administration de l'infrastructure de virtualisation, le prestataire s'engage à tenir à jour un registre des personnes autorisées. Les références utilisées ne doivent pas être réattribuées une fois qu'elles ont été désactivées ou qu'elles ont expiré.
	Accès des parties prenantes aux systèmes	Moyens techniques mis en œuvre pour assurer l'identification et l'authentification et les moyens de contrôle d'accès des participants aux systèmes.	Partagé	Le client est responsable de l'accès de ses parties prenantes aux systèmes d'exploitation, logiciels et applications qu'il gère, ainsi que du contrôle d'accès aux postes de travail de ces parties prenantes.	Le prestataire fournit un dispositif d'authentification aux opérateurs du client qu'il a nominalement autorisés, avec les droits définis dans le cadre du service Flexible Engine.
Télécommunications	Chiffrement des données personnelles transmises sur les réseaux publics	Les données personnelles doivent être cryptées avant d'être transmises sur des réseaux publics.	Client	Le Client s'engage à mettre en œuvre les moyens techniques nécessaires pour assurer un cryptage à l'état de l'art lorsque cela est techniquement possible pour toute transmission de données personnelles de santé sur des réseaux publics.	N/A

	Règle	Détail de la règle	Responsabilité	Responsabilité des clients	Responsabilité du fournisseur
	Traçabilité et intégrité des communications	L'hébergeur doit enregistrer la transmission de données à caractère personnel à des tiers et s'assurer que les données sont reçues par le système cible.	Client	Le client est responsable de l'intégrité des données de santé à caractère personnel lors des transferts effectués sous sa responsabilité	N/A
Traçabilité	Gestion des traces	L'hébergeur doit mettre en œuvre les moyens d'assurer la traçabilité des actions des utilisateurs, des défaillances et des événements liés à la sécurité de l'information.	Partagé	Le client est responsable de la traçabilité de toutes les activités, tant au niveau du système et de l'application qu'au sein de son environnement virtualisé. Le client est responsable de la mise en œuvre du service de traçage du cloud (6.9.2) pour stocker les activités liées à la gestion des services Flexible Engine.	Le prestataire collecte les traces des activités effectuées sur l'interface client du Cloud Store, ainsi que les traces des activités d'administration des équipes de l'infrastructure du prestataire.
	Communication des traces administratives aux clients	Des moyens techniques et organisationnels doivent être mis en œuvre pour communiquer au client les traces des administrateurs.	Fournisseur	N/A	Le fournisseur peut fournir au client des traces de son activité sur l'interface du magasin virtuel, ainsi que des traces des activités d'administration de l'infrastructure si cela est demandé.
	Habilitations requises pour l'accès aux traces d'application	Gestion des autorisations d'accès aux traces de l'application	Client	Le Client est responsable de l'habilitation nominative de chaque opérateur autorisé par lui à accéder à la sauvegarde et à l'archivage des traces sous sa responsabilité.	N/A
	Périmètre lié à la surveillance de l'accès aux données de santé	Périmètre technique en termes d'accès aux données de santé	Client	Le client surveille les logiciels et les applications qu'il gère ainsi que les éléments de sécurité, d'administration et d'exploitation de ces logiciels et applications. La traçabilité des actions sur les logiciels installés par le Client est de la responsabilité du Client.	N/A
Gestion des incidents	Procédures d'alerte et d'escalade	Procédures d'alerte et d'escalade pour répondre aux incidents de sécurité détectés.	Partagé	Le Client définit et met en œuvre des procédures d'alerte et d'escalade relatives aux incidents de sécurité détectés sur les infrastructures virtuelles qu'il gère.	Le prestataire ne traite que les incidents liés à la plateforme et aux services associés, à l'exception des infrastructures virtuelles instanciées par le client (instances de serveurs en nuage, OS, stockage).
	Notification de violation de données	L'hébergeur notifie à son client toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance	Partagé	Le client s'engage à notifier toute violation de données à caractère personnel conformément aux exigences énoncées dans le GDPR.	Le prestataire s'engage à notifier au client toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

	Règle	Détail de la règle	Responsabilité	Responsabilité des clients	Responsabilité du fournisseur
	Classification des incidents	Principes de classification des incidents	Partagé	Le Client définit une classification des incidents détectés sur l'environnement virtualisé dont il a la charge.	Le prestataire définit une matrice de priorité pour les incidents détectés dans son domaine de responsabilité.
Sauvegarde	Sécurité des sauvegardes	La sécurité des sauvegardes de données de santé doit être garantie, quel que soit le support.	Client	Les sauvegardes des données de santé sont contrôlées lors de leur transfert et de leur stockage	N/A
	Sauvegarde des traces	Définition et mise en œuvre d'une politique de sauvegarde des traces	Partagé	Le Client est responsable de la politique de sauvegarde et d'archivage des traces d'accès sur son environnement virtualisé.	Le prestataire est responsable de la politique de sauvegarde et d'archivage des traces d'accès sur le périmètre de l'infrastructure de virtualisation, à l'exception de l'environnement virtualisé instancié par le client.
Continuité du service	Continuité et disponibilité des services	Les exigences en matière de continuité et de disponibilité des services sont identifiées et approuvées conjointement par le client et l'hébergeur. L'hébergeur définit et met en œuvre un plan de continuité des services pour répondre aux exigences définies et approuvées. Le plan de continuité des services est testé régulièrement (au moins une fois par an) et les résultats des tests doivent être enregistrés. La capacité et les performances sont contrôlées régulièrement.	Partagé	Le Client définit et met en œuvre un Plan de Continuité d'Activité sur le périmètre de son environnement virtualisé qu'il instancie (instances de serveurs cloud, OS, stockage).	Le Prestataire définira et mettra en œuvre un Plan de Continuité d'Activité sur le périmètre des plateformes et des Services associés, à l'exception de l'environnement virtualisé instancié par le Client (instances de serveurs cloud, OS, stockage), et réalisera des tests de reprise selon un plan annuel défini. Le prestataire maintient un plan de capacité pour les plateformes afin de répondre aux évolutions attendues.
Gestion de l'évolution	Planification de services nouveaux ou modifiés	Formalise une procédure de planification pour la mise en œuvre ou la modification des services afin de répondre à leurs exigences.	Fournisseur	N/A	Le prestataire a obtenu la certification ISO/IEC 20000-1:2011 pour les éléments suivants Le champ d'application des plateformes couvre toutes les activités liées à l'hébergement de données de santé à caractère personnel.
	Processus de gestion du changement pour les applications	Description du processus de gestion des changements liés aux évolutions du système pour les composants d'application	Client	Le Client installe, met à jour et maintient l'environnement virtualisé dont il a la charge. Le Client définit et met en œuvre les processus de gestion du changement sur ce périmètre.	N/A

	Règle	Détail de la règle	Responsabilité	Responsabilité des clients	Responsabilité du fournisseur
Conformité	Certification ISO 27001	Certification ISO/IEC 27001:2013 sur le périmètre des activités d'hébergement de données de santé à caractère personnel.	Fournisseur	N/A	Le Prestataire maintient une certification ISO/IEC 27001:2013 sur le périmètre des plateformes couvrant l'ensemble des activités d'hébergement de données de santé à caractère personnel.
	Champ d'application du SMSI	Le champ d'application du SMSI doit couvrir toutes les activités d'hébergement de données de santé à caractère personnel de l'hébergeur.	Fournisseur	N/A	Le champ d'application du SMSI sélectionné pour la certification ISO 27001 couvre toutes les activités liées à l'hébergement de données de santé à caractère personnel.
	Déclaration d'applicabilité du SMSI	La déclaration d'applicabilité (LoA) du SMSI doit inclure toutes les exigences de la norme de certification HDS.	Fournisseur	N/A	La déclaration d'applicabilité (LoA) du SMSI sélectionnée pour la certification ISO 27001 comprend toutes les exigences du cadre de certification HDS.
	Audit d'application	L'hébergeur doit permettre à ses clients d'effectuer des audits sur les applications mises en production	Fournisseur	N/A	Le prestataire s'engage à mettre en place une procédure pour la réalisation des audits demandés par le client sur les applications mises en production.
	Sous-traitance	L'hébergeur ne doit pas faire appel à un sous-traitant sans en avoir préalablement informé le client.	Fournisseur	N/A	Le prestataire s'engage à informer préalablement le client en cas de recours à un sous-traitant.
	Accords de confidentialité	Les contrats de travail des employés de l'hôte doivent comporter une clause de confidentialité.	Fournisseur	N/A	Le prestataire s'engage à ce que son personnel et ses sous-traitants soient liés par un engagement de confidentialité concernant la diffusion des données à caractère personnel.
	Conformité PGSSI-S	L'hébergeur doit informer ses clients qu'ils sont tenus de se conformer à la PGSSI-S et doit mettre en place un moyen de recueillir l'engagement de cette conformité.	Partagé	Le client s'engage à respecter la PGSSI-S (Politique générale de sécurité des systèmes d'information de santé).	Le fournisseur informe son client qu'il est tenu de se conformer à la PGSSI-S. La signature du présent contrat recueille l'engagement du client.
	Lieux d'hébergement	L'hébergeur doit préciser la liste de tous les pays dans lesquels les données du client sont ou peuvent être hébergées.	Fournisseur	N/A	Le prestataire s'engage à fournir au client une liste de tous les pays dans lesquels les données sont ou peuvent être hébergées, et à permettre au client de choisir le ou les pays dans lesquels ses données de santé seront hébergées.
	Rapport d'audit de certification	L'hébergeur fournira aux clients, sur demande, des rapports d'audit de certification.	Fournisseur	N/A	Le prestataire s'engage à communiquer au client, sur demande, les rapports d'audit de certification.

	Règle	Détail de la règle	Responsabilité	Responsabilité des clients	Responsabilité du fournisseur
Politique de sécurité	Politique de suivi	Définition et mise en œuvre d'une politique de contrôle de l'accès des utilisateurs à l'application	Client	Le Client met en œuvre une politique de surveillance des accès des utilisateurs de l'application (y compris des professionnels et établissements de santé, voire directement des patients). Ce suivi est d'ordre fonctionnel et la définition et la mise en œuvre des mesures de conservation, d'accès et d'utilisation de ces traces n'entrent pas dans le champ de la responsabilité du Prestataire.	N/A
	Politique d'autorisation d'accès aux applications métier	Définition et mise en œuvre d'une politique d'accès aux applications professionnelles	Client	Le Client est seul responsable de la politique d'autorisation d'accès aux applications professionnelles et aux données personnelles de santé qu'il peut donner à son personnel (opérateurs ou autres) ou à des professionnels de la santé, voire directement à des patients.	N/A
Poste de travail	Sécurité du poste de travail	Définition et mise en œuvre d'une politique de sécurité pour les postes de travail	Partagé	Le client est responsable de la politique de sécurité des postes de travail de ses opérateurs (par exemple : gestion des mots de passe, jetons, verrouillage automatique).	Le prestataire est responsable de la politique de sécurité des postes de travail de ses opérateurs

Il incombe au client de veiller à ce que toutes ses responsabilités soient assumées.

Le cas échéant, le prestataire peut demander au client la preuve du strict respect de tout ou partie de ces dispositions si sa responsabilité devait être engagée.

9.2 Respect des normes d'interopérabilité et de sécurité de l'ANS

Le Client garantit avoir mis en œuvre les moyens techniques permettant d'assurer les moyens d'identification, d'authentification et de contrôle d'accès des professionnels et personnes concernés par les données de santé, pour toute opération prévue par le service d'hébergement au titre du présent Contrat.

Le Client s'engage à respecter la PGSSI-S et garantit que, conformément à l'article L1470-5 du code de la santé publique, les systèmes d'information utilisés sont conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24 du code de la santé publique.

9.2.1 Responsabilités du prestataire

Le Prestataire garantit au Client qu'il dispose de la certification requise par les dispositions du Code de la santé publique pour l'hébergement de données de santé à caractère personnel.

Le prestataire ayant reçu des informations, documents ou données quelconques, soit préalablement au bon de commande, soit au cours de son exécution, ne peut, sans autorisation, les communiquer à des personnes autres que celles qui sont habilitées à les connaître.

Le Prestataire est tenu de respecter et de préserver la confidentialité et la sécurité des données à caractère personnel qu'il est amené à traiter. Ainsi, le prestataire s'engage à prendre des mesures de sécurité techniques et organisationnelles, compte tenu de la nature des données et des risques présentés par l'hébergement des données,

afin de préserver la sécurité et l'intégrité des données et, notamment, d'empêcher leur destruction, leur perte, leur altération, leur divulgation ou leur accès non autorisé.

Le prestataire déclare avoir sensibilisé son personnel et ses éventuels sous-traitants à ces stipulations. Conformément à l'article sur la protection des données personnelles des Conditions générales *** REF ? *** , le Prestataire s'engage à ne pas traiter les données de santé à caractère personnel qu'il héberge à d'autres fins que l'exécution du service FE HDS. Le Prestataire s'interdit notamment toute utilisation de ces données à des fins marketing, publicitaires, commerciales ou statistiques.

Section 9.1 présente la matrice des responsabilités entre le Proivider et le Client.