Business

Descriptif de service
Cloud Privé

Sommaire

1. AVANT PROPOS 2

2. DEFINITIONS 2

3. OBJET DE CE DOCUMENT 3

4. VUE D'ENSEMBLE DES SERVICES 3

4.1. DESCRIPTION GÉNÉRALE 3
4.2. CLOUD AVENUE [PRIVATE] SOLUTION 4
4.3. COUVERTURE GÉOGRAPHIQUE 4

5. CONTENU DU SERVICE 5

5.1. LES COMPOSANTS 5
5.1.1. Les services inclus 5
5.1.2. Services complémentaires 5
5.2. COMPOSANTS D'INFRASTRUCTURE 6
5.2.1. Capacité de calcul et de stockage 7
5.2.2. Firewall 8
5.2.3. Load balancing 8
5.2.4. Sécurité et identité 9
5.2.5. Backup 9
5.2.6. Haute disponibilité 10
5.2.7. Portail self-service, orchestration, Hybridation 10
5.2.8. Cloud Automation 11
5.2.9. Containers, Kubernetes & PaaS 11
5.3. SERVICES MANAGÉS 12
5.4. CO-LOCATION. 13

6. CONDITIONS D'UTILISATION 13

6.1. PRIX 13
6.2. DURÉE D'ENGAGEMENT MINIMUM 14
6.3. RÉVERSIBILITÉ 14
6.4 LICENCES MICROSOFT 14
6.4.1 Mode locatif 15
6.4.2 Mode mobilité 15

7. SUPPORT ET SERVICE/OPERATION MANAGEMENT 15

7.1. ORGANISATION 15
7.2. SLA / ENGAGEMENTS 16
7.3. OPÉRATION & GOUVERNANCE 18
7.3.1. Gestion des mises à jour 18
7.3.2. Gestion des alarmes 18
7.3.3. Gestion des incidents et problèmes 18
7.3.4. Gestion des demandes de changements 19
7.3.5. Gestion de la capacité et des performances 19
7.3.6. Reporting & Monitoring 20

8. LISTE DES ILLUSTRATIONS 21

1. Avant propos

Certains besoins informatiques des entreprises nécessitent la mise en œuvre de solutions de Cloud privé pour répondre à des contraintes ou exigences qui peuvent être :

- Les applications Legacy qui nécessitent un système d'exploitation et un environnement spécifiques pour fonctionner et être maintenues,
- Confidentialité et isolation des données,
- Sécurité maximale des données et des actifs,
- Traçabilité, proximité, localisation proche et identifiée des données,
- Performance (serveurs dédiés),
- Respect de la réglementation, du droit européen applicable,
- Contrôle par le client du calendrier de maintenance/mise à jour de l'infrastructure,
- Possibilité de mélanger les usages managés et IaaS.
- Besoin d'externaliser une partie de la gestion de l'infrastructure à un partenaire de confiance.

Pour de tels besoins, l'utilisation d'une infrastructure informatique dédiée au client, isolée physiquement et logiquement des autres, est nécessaire.

Pour ces usages, le Prestataire fournit des solutions de Cloud privé sur mesure répondant à une grande pluralité de besoins et offre à ses clients une large gamme de services IT délivrés en mode libre-service et/ou en mode service managés.

2. Définitions

Les termes en majuscules utilisés mais non définis dans ce chapitre auront la signification qui leur est donnée dans les conditions générales ou dans les Conditions Spécifiques Cloud.

"Applications Legacy" désigne des logiciels en place depuis longtemps dans l'entreprise et donc 'hérités' du passé. Bien que potentiellement obsolètes, ils restent essentiels au bon fonctionnement et aux besoins business de l'entreprise.

"Back End" désigne une zone isolée de l'internet et de l'intranet, hébergeant des services ou une application non accessibles via Internet,

"DMZ (Demilitarized Zone)" désigne un sous-réseau isolé par un pare-feu. Ce sous-réseau est composé de machines situées entre un réseau interne (LAN - postes clients), un réseau externe (Internet, le plus souvent) et des réseaux d'échanges d'applications.

"Front End" désigne une zone frontale, hébergeant des services ou des applications accessibles depuis Internet.

"Haute Disponibilté" désigne un système qui est opérationnel en permanence pendant une durée souhaitable. La disponibilité peut être mesurée par rapport à "100% opérationnel" ou "jamais défaillant".

"Machine virtuelle" ou "VM" désigne un environnement logiciel exécutable qui émule un ordinateur hôte. Plusieurs machines virtuelles peuvent être créées dans un seul ordinateur. Chaque utilisateur aura l'illusion de disposer d'un ordinateur complet alors que chaque machine virtuelle est isolée des autres.

"vCPU (Virtual Central Processing Unit)" désigne un composant virtuel dans un ordinateur qui aide à l'exécution de programmes informatiques.

"VLAN (Virtual Local Area Network)" désigne un réseau informatique local logique isolé. Plusieurs VLAN peuvent coexister sur un même commutateur.

"VPN (Virtual Private Network)" désigne une extension des réseaux locaux assurant la sécurité logique fournie par un réseau local. Il s'agit de l'interconnexion de réseaux locaux via une technique de tunneling utilisant des algorithmes cryptographiques.

"Workload domain" désigne une unité logique qui regroupe les nœuds hôtes gérés par un plan de contrôle central avec des caractéristiques spécifiques selon les meilleures pratiques des éditeurs de solutions HCI.

3. Objet de ce document

Le présent Descriptif de Service a pour objet de définir le Service de Cloud privé et d'énoncer les conditions dans lesquelles il est fourni par le Prestataire, en application des Conditions Générales.

Le présent Descriptif de Service est rattachée aux Conditions Spécifiques Cloud.

4. Vue d'ensemble des services

4.1. Description générale

Les solutions de Cloud privé du Prestataire fournissent une infrastructure informatique sur mesure en tant que service ou une plateforme en tant que service servant exclusivement un client dans le centre de données qui répond le mieux à ses besoins, soit le centre de données du client, soit un centre de données hébergé par le Prestataire, de niveau Tier III+/Tier IV.

L'infrastructure du Cloud privé est dédiée au client (contrairement au Cloud public) et est disponible sur l'intranet du client, dans le but de répondre aux exigences fortes de l'organisation en matière de sécurité, de conformité et de localisation. L'infrastructure est conçue pour prendre en charge les charges de travail critiques du client avec le un niveau de performance adapté, la rapidité de déploiement, la garantie de service et l'évolutivité.

Conformément à la configuration définie avec le Client, le Service permet au Client de mettre en place les fonctionnalités suivantes :

- L'hébergement des applications et données : plateformes de développement, test et intégration ; pré-production, production, applications en mode SaaS (Software as a Service).
- Architecture sécurisée avec cloisonnement des services à l'aide de zones de sécurité
- Accès sécurisé aux applications via Internet ou VPN Intranet
- Evolution des infrastructures en fonction des besoins : puissance de calcul, mémoire, stockage, connectivité, architectures sécurisée (front-end, back-end)

Le Prestataire prend en charge la conception, la construction et l'exploitation de la plateforme en assurant sa haute disponibilité 24 heures sur 24 et 7 jours sur 7, la protection des données, la sécurité, la connectivité, l'assurance technique et l'évolution en fonction des besoins du client et selon la gouvernance mise en place avec le client (dans le cadre des accords de niveau de service convenus).

L'offre fournit les services suivants :

- Co-conception et construction de la solution appropriée,
- Livraison de l'infrastructure (HW et SW), dans le monde entier,
- Hébergement de l'infrastructure dans le centre de données d'Orange/Partenaire (lorsqu'il ne se trouve pas dans les locaux du client),
- Mise en œuvre/intégration de la solution dans le système informatique du client,
- Services de sécurité : mises à jour des correctifs de sécurité, antivirus, audits de sécurité,
- Maintien de la solution de Cloud privé en conditions opérationnelles (Service Management),
- Gestion de la solution selon différents modèles :

- Le IaaS (Infrastructure as a Service) est une offre de Cloud computing où le Client bénéficie de ressources informatiques dans un environnement virtualisé via un VPN ou une autre connexion sécurisée. Le Prestataire déploie et gère l'infrastructure (serveurs physiques de calcul/stockage, virtualisation, réseaux et sécurité). Le Client installe et gère le système d'exploitation, le middleware et les applications. IaaS fournit au Client et à ses propres utilisateurs/clients la capacité de provisionner de manière autonome des machines virtuelles (VM) avec le stockage et le réseau associés à la demande dans plusieurs régions.
- Avec PaaS (Platform as a Service), en plus de la fourniture et du maintien en condition opérationnelle de l'infrastructure Cloud, le Prestataire met en œuvre la configuration de l'environnement d'hébergement selon les besoins du client (réseaux virtuels, modèle d'hébergement VM, profil de configuration VM pour les ressources et le stockage), laissant au client le contrôle des applications métier qu'il peut installer, configurer, utiliser et maintenir lui-même.
- Différents niveaux de support sont proposés pour les solutions de Cloud privé, assortis d'engagements de qualité de service par le Prestataire qui varient en fonction du niveau choisi. A des niveaux de support prédéfinis, Standard ou Premium, s'ajoutent des niveaux personnalisables pour répondre aux exigences particulières des clients dans le cadre d'une offre sur mesure.

4.2. Cloud Avenue [Private] solution

Outre une solution 100% sur mesure présentée dans cette description de service, le Prestataire propose à ses clients une solution de Cloud privé standardisée, appelée Cloud Avenue [Private]. Grâce à son architecture rationalisée et standardisée, l'offre Cloud Avenue [Private] convient aux clients qui recherchent les caractéristiques essentielles d'une solution de Cloud privé mais qui souhaitent des coûts plus faibles, une livraison plus rapide et une durée d'engagement réduite. Cette solution est présentée dans une Description de Service spécifique.

4.3. Couverture géographique

Les solutions de Cloud privé peuvent être mises en œuvre dans le monde entier, dans les propres datacenters du client ou hébergées dans les datacenters du Prestataire (plus de 70 datacenters dans le monde).

Figure 1: Couverture géographique

5. Contenu du service

L'offre de Cloud privé du Prestataire est basée sur des blocs de solutions standardisées mêlant infrastructure et services.

5.1. Les composants

5.1.1. Les services inclus

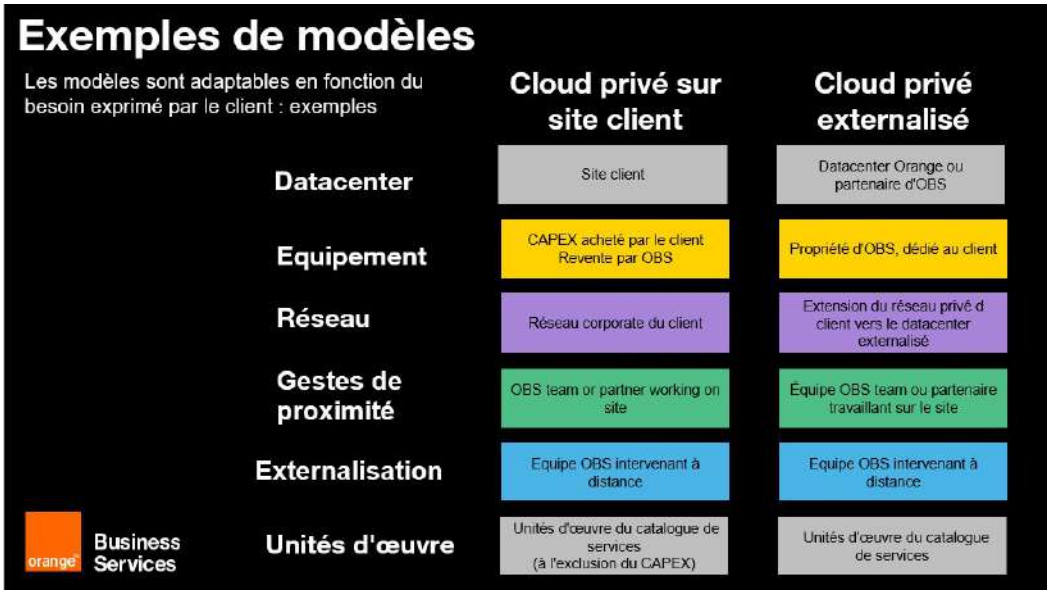
- Fourniture et construction de l'infrastructure du Cloud privé et de toute infrastructure requise pour les services supplémentaires souscrits via le Prestataire.
- Licences matérielles et logicielles pour tous les composants du Cloud privé jusqu'à la couche hyperviseur.
- Configuration et gestion de l'infrastructure de Cloud privé et de toute infrastructure requise pour les services supplémentaires souscrits via le Prestataire.
- Gestion de la solution, y compris la gestion opérationnelle, la surveillance et la maintenance régulière des composants matériels et logiciels du Cloud privé et de tous les services complémentaires souscrits.
- En cas d'hébergement par le Prestataire ou un partenaire, l'espace d'hébergement pour l'infrastructure du Cloud privé (dans deux centres de données distincts avec une connectivité inter-centres de données en cas d'exigences de Haute disponibilité / Disaster Recovery) et toute infrastructure requise pour les services complémentaires souscrits via le Prestataire.
- Fourniture et gestion des images OS requises pour la gestion et la surveillance de la plateforme IaaS du Cloud privé (en option).
- Configuration de la plateforme IaaS avec tous ses composants, comme discuté, convenu et validé avec le client.
- Des revues de service mensuelles régulières menées et organisées par le responsable du service client du Prestataire

5.1.2. Services complémentaires

Les services complémentaires donneront lieu à une proposition commerciale spécifique, à la validation du Client et à une facturation complémentaire.

- Toute licence de système d'exploitation, de base de données ou d'application pour les machines virtuelles du Client.
- La gestion de tout système d'exploitation, base de données, applications du Client, sauf si souscription de services managés associés.
- La transition, la migration et la transformation des actifs physiques ou des données du client du mode d'exploitation actuel vers le futur mode d'exploitation - sauf si le Prestataire est responsable de la fourniture de ce service.
- Gestion des sauvegardes au niveau des applications.

Figure 2 : Exemple de modèles



5.2. Composants d'infrastructure

Le Prestataire fournit un Virtual Data Center sur du matériel dédié (comprenant : CPU, RAM, capacité de disque, et service de sauvegarde inclus) et des ressources d'architecture sécurisées (pare-feu dédiés, load balancers et appareils de gestion des clés HSM gérés par le Client).

L'offre du Prestataire se concentre sur l'approche Software-Defined Data Center appelée Hyper-Convergence. Une infrastructure hyper-convergée (HCI) consiste à virtualiser le calcul, le stockage et le réseau. Les HCI tirent parti de l'hyperviseur pour fournir une puissance de calcul (Compute), un réseau et un stockage partagé à partir d'une seule plate-forme de serveurs X86 (ce qui signifie que les serveurs utilisés ne sont plus classés par fonction - calcul, routeurs de réseau, pare-feu ou stockage - mais sont des serveurs génériques qui assurent ces services par le biais du logiciel de virtualisation complet du centre de données : Server Virtualization, Software Defined Network et Software Defined Storage).

Le système intégré hyper convergent (HCIS) combine les équipements de calcul, de réseau et de stockage, ce qui dispense de recourir à un réseau de stockage (SAN) classique. Les fonctions de gestion du stockage - ainsi que des capacités optionnelles telles que la sauvegarde, la récupération, la réplication, la déduplication et la compression - sont assurées par la couche de management logicielle, ainsi que le provisionnement de la capacité de calcul.

Le service est configuré pour le client en utilisant des composants standard validés, comme convenu avec le client dans le formulaire de commande.

Pour les besoins du Cloud privé, le Prestataire fournit des solutions sur des technologies de pointe, toutes hyper convergées :

- VMWare : les composants principaux des solutions hyper convergées de VMware sont VMware vSphere et VMware vSAN.
- Nutanix : les composants principaux de Nutanix sont AHV, Volumes et Prism.
- Azure Stack HCI : il fournit une solution hybride Azure sur le site client ou dans le datacenter du Prestataire, prête à être déployée selon les besoins du client et offrant la même expérience utilisateur qu'Azure.

Quelle que soit la technologie et quel que soit le modèle de vente Private Cloud (que les serveurs physiques utilisés par le Prestataire lui appartiennent ou non), toutes les données et applications hébergées fournies par le Client restent la propriété du Client.

Figure 3 : Fonctionnalités des solutions de Cloud privé

Caractéristiques	VMWare	Nutanix (new portfolio 2022)	Azure Stack HCI
Hypervisor	vSphere / ESXi	AHV, vSphere, ESXi, KVM, Xen, Hyper-V	HyperV
Cloud Management Platform	vRO / vRA	Intelligent Operations	Azure Portal / Azure Arc
SDS tool	vSAN	AOS Storage	native
Block Storage	vSAN	Nutanix Kubernetes Engine	native
Object Storage (S3)	Object Storage / Ceph	Objects Storage	native
Files Sharing	vSAN files services	Files Storage	3rd party (Isilon)
SDN (micro segmentation)	NSX-T	Flow Network Security	native
Container orchestration	Tanzu	Nutanix Kubernetes Engine	AKS
Database Management	vFabric	Nutanix Database Service	native
VM Image Management Service	Mirage	Intelligent Operations	native
DR	Veeam / Zerto / vSphere replication /	Nutanix Disaster Recovery	Comvault
Automation Orchestrator	vRO / vRA	Self-Service	native
Life cycle application management	vRealize	Self-Service	native
Resource pool management	Resource pool	Projects	native
Analytics, Optimization	vRops	Cost Governance	native

5.2.1. Capacité de calcul et de stockage

Le Prestataire fournit la capacité de calcul sur la base d'un plan de capacité annuel / mensuel établi avec le Client. La capacité de calcul comprend la puissance du processeur, la mémoire RAM et un ou plusieurs niveaux de capacité de stockage. Ces ressources sont utilisées pour créer les Machines Virtuelles (VMs).

La puissance CPU est exprimée en valeurs vCPU (par cœur de CPU) et la mémoire RAM est exprimée en valeurs GB.

Les types et la capacité de disque fournis sont divisés en valeurs de Go ou To (stockage sur les machines virtuelles). Toute capacité de performance spécifique, si elle est fournie, sera documentée dans les accords de niveau de service régissant les services fournis.

Avec les solutions de Cloud privé, nous définissons des domaines de charge de travail (workloads).

Les classes de services appliquées à la capacité de calcul sont définies par domaine de charge de travail avec les paramètres suivants : ratio vCPU/cœur, ratio vCPU/cœur (récupération), nombre de défaillances de nœuds à tolérer.

Le client peut modifier ses ressources réservées via le processus de contrôle des changements du Prestataire (en supposant qu'une capacité d'infrastructure non réservée suffisante soit disponible).

Les services comprennent :

- L'acquisition de serveurs et de composants,
- L'installation des équipements,
- La fourniture, l'installation, la configuration et la maintenance des outils de gestion,
- La Connectivité physique,
- La configuration initiale du serveur physique (RAM, CPU, stockage),
- La configuration de l'infrastructure IaaS et déploiement de la connexion physique/logique au réseau LAN,
- L'exploitation et support de la plateforme

5.2.2. Firewall

Le Prestataire met en place une Infrastructure sécurisée avec une configuration de pare-feu à haute disponibilité.

La paire de pare-feu est située en amont de la Plateforme d'Hébergement avec des règles restrictives d'analyse et de filtrage du trafic passant par la plateforme et le Centre de Données Virtuel et les VLANs du Client.

Le Client est responsable de la définition de ses propres règles de pare-feu entre les instances virtuelles internes/VLANs et les réseaux externes. Ces règles sont définies pendant la phase de conception/ onboarding puis gérées et mises à jour par le processus de contrôle des changements du Prestataire pendant le Service 'live'.

Selon l'option souscrite par le Client, ce service de pare-feu dédié donne accès à un maximum de 8 zones de sécurité/VLAN liées au trafic du Client (VLAN de trafic), au trafic d'équilibrage de charge (VLAN virtuel) et au trafic d'Orange (VLAN d'administration).

Ces zones de sécurité peuvent être définies comme suit :

- Zones de sécurité Front End (zone internet, zone intranet/VPN avec l'option de connexion VPN) ;
- Zones de sécurité Back End.

Chaque zone de sécurité contient des sous-réseaux d'adresses privées, définis avec le Client, qui peuvent être utilisés pour les machines virtuelles.

Le Client peut demander au Prestataire de configurer ses règles de filtrage via le processus de contrôle des modifications du Prestataire. Le Client doit avoir les connaissances et l'expertise nécessaires pour comprendre les règles de filtrage requises. Tout ajout ou modification demandé par le Client aux règles de filtrage de la Machine Virtuelle est de la seule responsabilité du Client.

5.2.3. Load balancing

L'équilibreur de charge (Load balancer) permet de maximiser la disponibilité des ressources virtualisées en améliorant la répartition de la charge de travail du trafic réseau entrant (HTTP, TCP) entre un ensemble de machines virtuelles, de conteneurs ou de serveurs bare metal. La distribution du trafic se fait selon les algorithmes les plus courants (Round-Robin, Least Connection, IP Source). Avec ce service, le retrait / la réactivation des conteneurs indisponibles / à nouveau disponibles peut être effectué automatiquement. Le service Load Balancer est nécessaire pour déployer et exploiter des architectures de haute disponibilité.

Le Prestataire met en œuvre des dispositifs de load balancing, en mettant en place un matériel redondant pour les machines virtuelles.

La disponibilité des machines virtuelles et le load balancing peuvent être gérés par le load balancer. Le service d'équilibrage de charge est disponible pour toutes les zones sécurisées.

Les fonctionnalités de gestion du trafic comprennent :

- L'équilibrage de charge intelligent (choix entre deux algorithmes : Round Robin et Least Connection),
- La persistance des sources IP.

NB : Pour activer le load balancing, le Prestataire et/ou le Client doivent impérativement autoriser les requêtes ping sur les Machines Virtuelles mutualisées par le load balancer. A défaut, le load balancer ne sera pas actif sur ces Machines Virtuelles qui seront considérées comme éteintes.

Le nombre maximum de règles d'équilibrage de charge est de 10 dans chaque zone de sécurité.

5.2.4. Sécurité et identité

L'offre comprend un service Managed Firewall qui peut être complété par des fonctionnalités optionnelles telles que la détection des intrusions, l'anti-DDOS, le Security Operation Center.

Le Edge Firewall surveille le trafic nord-sud (entre le centre de données et le reste du réseau) pour fournir une fonctionnalité de sécurité périmétrique comprenant un pare-feu, la traduction d'adresses réseau (NAT) ainsi que des fonctionnalités IPSec et SSL VPN site à site.

Le Prestataire sécurise les flux de données dans chaque machine virtuelle et conteneur et offre une micro-segmentation des réseaux virtuels basée sur les principes de virtualisation et de sécurité du réseau NSX proposés par notre VMware.

Des fonctionnalités similaires sont fournies avec la solution Nutanix (Flow) et avec Azure Stack (intégré nativement).

Si nécessaire, le Prestataire peut définir avec le client comment répartir les tâches entre les différents rôles : responsable de la sécurité informatique, utilisateurs, administrateurs et développeurs. Cette segmentation permet d'automatiser les déploiements dans leur périmètre de responsabilité. Les périmètres et les permissions sont contrôlés en option via l'interface vRealize Automation™ (VMware), l'interface Prism Pro (Nutanix), l'interface native (Azure Stack) et intégrés à l'Advanced Directory du client pour gérer les politiques en fonction des groupes auxquels appartiennent les utilisateurs.

Des mises à jour régulières pour corriger les failles de sécurité des infrastructures sous-jacentes sont incluses dans le Service. Le Prestataire étend également ce service à toute externalisation complémentaire qui pourrait être confiée au Prestataire.

5.2.5. Backup

Le Prestataire propose des plans de sauvegarde et de continuité des activités managés pour protéger les entreprises contre les risques de perte de données.

Le Prestataire intègre, exploite, automatise et surveille la solution 24h/24 et 7j/7.

Le service de sauvegarde permet de sauvegarder les données du client sur une base quotidienne ou hebdomadaire et de les restaurer quand nécessaire à une date choisie dans les limites de l'historique de sauvegarde.

La politique de sauvegarde propose 2 modes standards :

- Hebdomadaire-6 (une sauvegarde hebdomadaire avec 6 semaines de sauvegarde), mode par défaut,
- Journalière 15 (une sauvegarde quotidienne avec une sauvegarde de 15 jours).

Des politiques de sauvegarde personnalisées peuvent être étudiées et proposées sur devis au Client.

Un large éventail de solutions techniques est proposé en fonction des besoins du client (données stockées, machines virtuelles, bases de données opérationnelles, etc.), de la quantité, du temps de rétention, de la destination (locale, distante ou Cloud), des objectifs de temps de récupération (RTO)

partiels ou complets, des objectifs de perte de récupération (RLO) tolérables ou intolérables, et de la flexibilité du processus de récupération.

Fondamentalement, le périmètre de gestion du Prestataire couvre les domaines suivants :

- Surveillance des sauvegardes des clients,
- Définition du profil du référentiel de stockage,
- Redémarrage des sauvegardes en cas de défaillance,
- Procédure de restauration à la demande du client,
- Planification de la capacité de la plateforme de sauvegarde.

Le prestataire a sélectionné des solutions pleinement compatibles avec l'environnement VMWare vSphere™ parmi les plus performantes du marché pour fournir une sauvegarde des VMs, une restauration rapide et flexible ainsi que des fonctionnalités avancées pour leur réplication.

Des solutions similaires sont disponibles avec Nutanix (Xi Leap) et Azure Stack (CommVault).

Le Prestataire propose quatre scénarios avec différents RTO/RPO (Recovery Time Objective/ Recovery Point Objective) :

- Zone de disponibilité (AZ) unique : aucune protection contre la défaillance du site.
- Double AZ, même site : double salle, protection contre la défaillance de la salle.
- Double AZ, sites différents : protection contre les pannes de site.
- Double région : pile de management et pile de production entièrement séparées, place la charge de travail plus près du client.

Les centres de données sont choisis en fonction de la distance et du réseau disponible entre eux.

Hébergement de l'infrastructure dans des centres de données Tier III+/IV proches de l'entreprise et de ses filiales (plus de 70 centres de données Orange dans le monde).

5.2.6. Haute disponibilité

Le Service propose une solution de haute disponibilité basée sur une architecture multi-sites redondante.

La haute disponibilité s'appuie sur une architecture multi-sites redondante. L'ensemble du système est conçu par le Prestataire, selon des architectures de référence validées : datacenters certifiés, réseaux inter-sites redondants et fiables, faible latence entre les sites principaux, équipements certifiés, architecture de virtualisation de datacenter à haute disponibilité pour tout (calcul, stockage, réseau, virtualisation, sécurité ou portail). Les équipes du Prestataire ajustent la conception des Clouds privés pour répondre aux exigences de performance des applications et d'accès aux données.

En cas de défaillance matérielle, le système tolérant aux pannes continue de fonctionner avec le taux de disponibilité conforme aux engagements du Prestataire . Grâce à son support d'externalisation, le Prestataire intervient rapidement pour réparer le matériel défectueux et rétablir le service nominal afin d'éviter une double panne.

5.2.7. Portail self-service, orchestration, Hybridation

Avec l'offre de Cloud privé du Prestataire et selon le mode de management de la solution choisi, le Client peut accéder à une console de self-service, intégrée dans un portail web unifié.

A travers cette console, le Client expose un catalogue de services à ses utilisateurs.

Figure 4 : Portail web client

Les utilisateurs peuvent activer et déployer des services en fonction de leur accréditation d'accès.

En cliquant sur un service, il lance un déploiement validé avec un modèle de référence (pratique informatique, sécurité, support).

Lorsque le Prestataire propose des services managés, le lancement déclenche automatiquement le déploiement d'agents de gestion (monitoring, backup, etc.).

L'éventail des plateformes prises en charge est large (plusieurs Clouds privés, divers équipements informatiques, applications, OSS-ITSM, Clouds publics).

Responsabilités :

- Le Prestataire est responsable de l'infrastructure et de la mise en œuvre des services.
- Le client est responsable de la gestion des utilisateurs.

5.2.8. Cloud Automation

Le Prestataire a défini 3 niveaux dans son offre de Cloud privé, avec un niveau d'automatisation croissant :

- A la demande : Virtualisation des ressources de calcul/stockage allouées par l'administrateur.
- Cloud automatisé : Automatisation des APIs des utilisateurs et orchestration.
- Micro-segmentation : avec la micro-segmentation, il est possible de renforcer et de compléter la sécurité globale d'un système de Cloud en ajoutant un niveau de sécurité latéral Est-Ouest (à l'intérieur du système, entre ses différents composants). La micro-segmentation définit des zones sécurisées au sein du système Cloud permettant d'isoler les charges de travail et de les protéger individuellement en apportant des règles de sécurité plus granulaires qui peuvent s'appliquer directement sur chaque VM ou chaque conteneur.

5.2.9. Containers, Kubernetes & PaaS

Le Client peut utiliser les clusters Kubernetes™, une plateforme standard aux API ouvertes conçue pour le déploiement d'applications de troisième génération (Cloud native) basées sur des conteneurs.

L'orchestrateur Kubernetes™ permet la haute disponibilité des conteneurs, l'équilibrage de charge, l'auto-scaling, des mises à niveau faciles sans perte du service. Il élimine une grande partie des processus manuels liés au déploiement et à la mise à l'échelle des applications conteneurisées. Kubernetes peut s'exécuter sur diverses plateformes de Cloud.

Les conteneurs Docker™ sont portables d'un environnement à l'autre. Les conteneurs embarquent l'OS et les dépendances, ce qui les rend indépendants de l'OS hôte et des autres conteneurs, facilitant ainsi l'intégration.

Le Prestataire propose une solution Kubernetes de niveau production, intégrée et maintenue par son équipe d'exploitation.

le Prestataire met à la disposition de ses clients des solutions d'automatisation des conteneurs avec toutes les technologies de Cloud privé (VMware, Nutanix, Azure Stack HCI) :

- La distribution Kubernetes de Tanzu est supportée par VMware.
- Nutanix propose un moteur Kubernetes (Nutanix Kubernetes Engine).
- Azure Stack HCI donne accès à AKS.

5.3. Services managés

Le Prestataire propose des niveaux progressifs de services managés en option sur l'infrastructure du Cloud privé :

- Managed OS : gestion du système d'exploitation, y compris les tâches liées au serveur et les activités de mise à niveau supplémentaires.
- Managed database : gestion complète de la ou des bases de données du client, y compris les tâches liées au serveur, les activités d'optimisation et de mise à niveau.
- Managed Middleware : gestion complète de tous les logiciels proposés dans le catalogue des composants suivants : Serveur web, serveur d'application, serveur de fichiers, serveur d'annuaire, serveur proxy. La cogestion du Middleware est possible mais doit faire l'objet d'une Offre Personnalisée.
- Managed Application : gestion des applications métier du client (web e-business, ERP, CRM, Finance, HR ...).

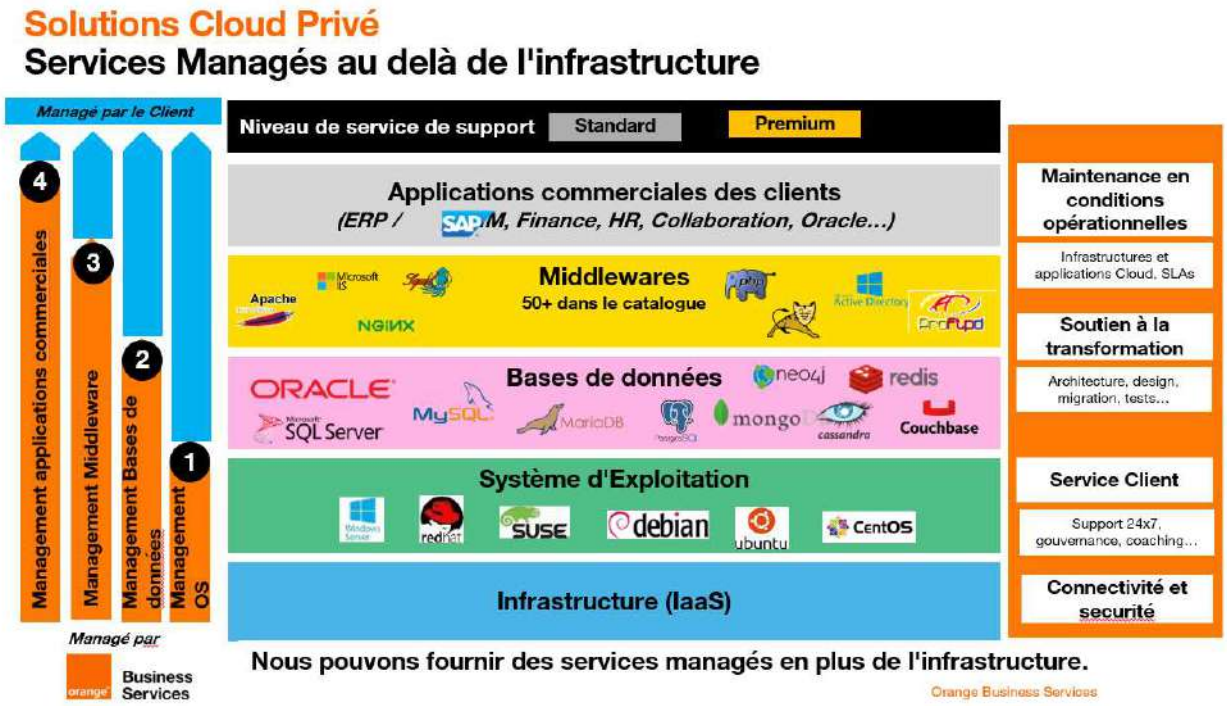
Ces niveaux de services managés étant progressifs, la souscription à un service nécessite la souscription aux niveaux inférieurs (ex : pour les niveaux de gestion Managed Database et Managed Middleware, le Client doit obligatoirement souscrire au niveau de gestion Managed OS).

Le Prestataire exploite l'infrastructure et les applications du client avec un haut niveau d'expertise.

Le Prestataire peut maintenir les applications du client en production, y compris SAP. Le reporting disponible pour le Client remonte les informations suivantes :

- Suivi de la performance des services.
- Carte à 360° des composants du SI : Clouds, charges de travail, systèmes, middleware, applications métier et services.
- Vues des performances des infrastructures et des applications en nuage.
- Rapports sur l'utilisation des services et les événements.
- Surveillance des flux de données entre les applications.

Figure 5 : Services Managés



5.4. Co-location.

Avec les solutions Private Cloud, la colocation est possible pour les besoins non couverts par la virtualisation.

Le Prestataire peut héberger des équipements spécifiques au client dans le même datacenter.

Les équipements hébergés peuvent être gérés par le Prestataire au cas par cas.

6. Conditions d'utilisation

6.1. Prix

Sauf pour Cloud Avenue [Private], l'offre de Cloud privé est entièrement conçue sur mesure. Cela signifie que le devis d'une solution de Cloud privé nécessite une activité de prévente prenant en compte le dimensionnement, le niveau fonctionnel requis et les services managés par le Prestataire.

Avec le modèle Private Cloud as a service, le Prestataire achète l'équipement et tous les éléments nécessaires à la création du service et revend le service sous la forme d'unités de travail d'un catalogue de services couvrant :

- L'équipement matériel, logiciel et les licences (payés soit d'avance à la livraison, soit intégré dans les unités de travail).

- La construction

- L'exploitation

- Le support

- Les engagements

- La gouvernance

Avec le modèle de revente d'équipement + service,

le Prestataire revend l'équipement principal au client.

- L'équipement

Le Prestataire fournit séparément les services d'intégration et les opérations :

- La construction
- L'exploitation
- Le support
- Les engagements
- La gouvernance
- Les services

6.2. Durée d'engagement minimum

La durée habituelle d'un contrat Cloud Privée est de 3 à 5 ans.

6.3. Réversibilité

Conformément aux conditions générales, les conditions de réversibilité sont définies comme suit :

- La durée de la période de réversibilité est limitée à 3 mois.
- Pendant la phase de réversibilité, la " garantie délai de réparation " ne s'applique pas.
- Le Prestataire s'engage notamment à fournir des informations techniques sur l'architecture du service, sous réserve que les informations demandées ne soient pas assimilées à un savoir-faire protégé par le Prestataire.

Dans le cas où il est demandé au Prestataire de fournir une assistance complémentaire à l'assistance définie ci-dessus et de gérer le service, le Client recevra :

- Une proposition d'assistance payante précisant les conditions de son intervention, le personnel dédié aux opérations de réversibilité, les éventuelles installations matérielles et physiques nécessaires.
- Les conditions financières applicables à la mise en œuvre de cette assistance complémentaire.

De son côté, le Client s'engage à fournir toute l'assistance technique, humaine et, le cas échéant, financière nécessaire pour mener à bien la migration du service. Les termes et conditions du Contrat continueront à s'appliquer jusqu'à la fin de la période de réversibilité.

En tout état de cause, le Client sera seul responsable de ses relations avec le repreneur et des agissements de ce dernier.

6.4 Licences 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.

6.4.1 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.

6.4.2 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 d'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.

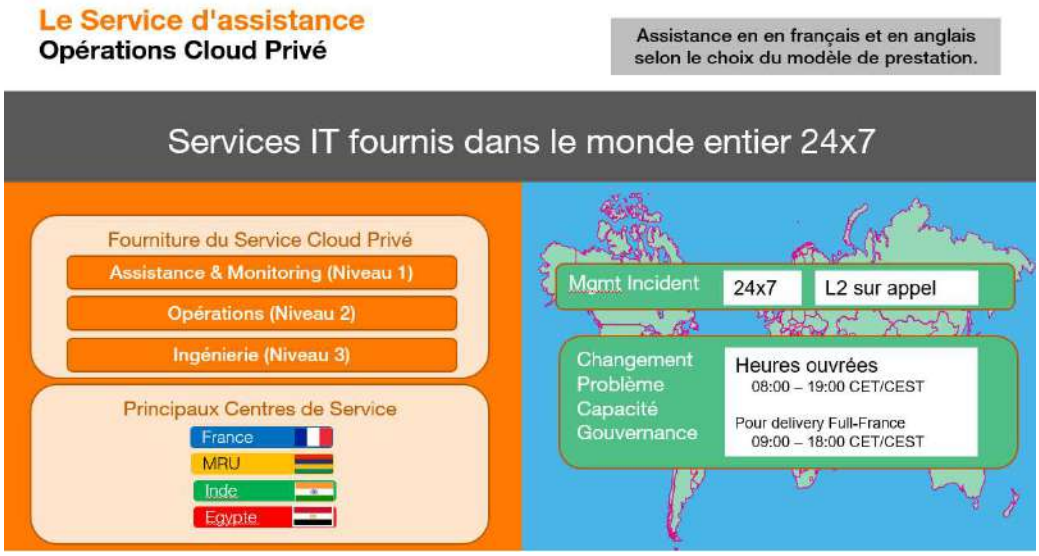
7. Support et service/operation management

7.1. Organisation

le Prestataire met en place une équipe de gouvernance responsable de l'exécution du Contrat et de la relation avec le client tout au long de la durée du Contrat.

Figure 6: Equipe de soutien et d'administration

Figure 7 : Service Desk



- Les demandes en dehors des heures d'ouverture CET/CEST sont traitées au cas par cas pour voir si le service peut être couvert par le service existant 24x7.
- Assistance en français et en anglais selon le choix du modèle de prestation.

7.2. SLA / Engagements

Les engagements de service dépendent de la proposition. Ils comprennent :

Une garantie de disponibilité du service :

- Sur une base mensuelle.
- Engagement selon la classe de service sélectionnée et l'architecture définie.
- Jusqu'à 99,99 % selon l'architecture choisie.

Temps de réparation garanti (GTR) :

- Service 24x7.
- Engagements en fonction de la gravité de l'incident.
- Exemple : GTR inférieur à 2h pour le haut niveau de service standard.

Exécution des changements :

- Exécution des changements en heures ouvrable, possible en option en dehors des heures ouvrables.
- Engagements en fonction de la complexité du changement.

Sauvegarde :

- Engagement uniquement si la sauvegarde est managée par le Prestataire
- Engagement sur 100 % de réussite de réalisation des demandes de restauration, pas d'engagement sur la qualité de la restauration.

Trois niveaux de support sont proposés : Standard, Premium et Personnalisé.

Ils sont sélectionnés en fonction de la criticité des applications du Client auxquelles le service est destiné.

Figure 8 : Incident Management SLA

Engagements SLA Incident

Activité	Service	KPI	Niveau		
			Gravité 1	Gravité 2	Gravité 3
Incident Mgmt	Custom	GTI	Défini selon les exigences du client		
		GTR			
		Rapport			
	Premium	GTI	30min	1h	4h*
		GTR	4h	8h	4 BD
		Rapport	toutes les 1h	toutes les 4h	toutes les 8h*
	Standard	GTI	1h	2h	4h*
		GTR	8h	24h	5 BD
		Rapport	toutes les 4h	toutes les 12h	toutes les 24h*

Les SLA doivent correspondre à la disponibilité offerte par l'architecture de la solution.

*Business Hours
BD=Business Day

Figure 9 : Problem Management SLA

Activité	Service	KPI	Niveaux		
			Critique	Majeur	Mineur
Gestion des problèmes	Custom	Créer	Défini selon les exigences du client		
		Rapport			
	Premium	Créer	2 BD	5 BD	
	Standard	Rapport	hebdomadaire	bi mensuel	mensuel

Figure 10 : Change Management SLA

Activité	Service	KPI	Niveaux		
			Changement Standard		
			Simple	Medium	Complexe
Gestion des Changements	Custom	GTC	Défini selon les exigences du client		
	Premium	GTC	4h	1BD	2BD
	Standard	GTC	8h	2BD	4BD

Quotas de Changements			
	Custom Premium Standard	Par instance managée	1 changement standard par trimestre
		Medium	= x2 simple
		Complexe	= x3 simple
		Heures Ouvrable standard	= x1 simple
		06:00 – 08:00; 19:00 – 22:00	= x2 simple
		22:00 – 06:00; weekend	= x3 simple

7.3. Opération & Gouvernance

7.3.1. Gestion des mises à jour

La gestion des versions de l'infrastructure du client est effectuée par le Prestataire en coordination avec le Client, selon son propre agenda et ses contraintes.

Elle concerne les correctifs de sécurité et de maintenance et les Service packs proposés par les fournisseurs de matériel et de logiciels.

Le Prestataire et le Client conviennent d'une fenêtre de maintenance régulière pour tous les travaux prévus :

- Le Prestataire informe le Client des nouvelles mises à jour/paquets d'applications disponibles.
- Le Prestataire installe les correctifs/mises à jour des packs d'applications après approbation du Client selon le plan de déploiement convenu, par exemple les systèmes de développement en semaine 1 et les systèmes de production en semaine 2 après que le Client a effectué des tests satisfaisants dans l'environnement de développement.
- Les correctifs d'urgence et les mises à jour des progiciels d'application peuvent être installés via le processus standard de gestion des changements.

La maintenance s'applique aussi sur le périmètre des Services Managés optionnels (système d'exploitation, base de données et middleware).

Le Prestataire assure la traçabilité de toutes les mises à jour réalisées sur son périmètre dans un outil d'exploitation dédié. Ces données sont conservées par le Prestataire pendant toute la durée du Contrat.

7.3.2. Gestion des alarmes

Grâce à une gamme d'outils collectant les alarmes sur l'infrastructure, le Prestataire détecte les différents codes d'erreur et les centralise dans le gestionnaire d'événements du Prestataire. Les codes d'erreur sont hiérarchisés selon 2 catégories de gravité : avertissement et erreur. Les alarmes qui en résultent sont transmises au support niveau 2 et traitées selon le processus et la conformité ITIL.

7.3.3. Gestion des incidents et problèmes

Le Prestataire surveille les datacenters, l'ensemble des équipements matériels (compute, storage, network, backup), les composants logiciels (couche de virtualisation) afin de prévenir les incidents au niveau de l'infrastructure et du cluster.

La gestion des incidents concerne les incidents qui peuvent survenir sur tous les éléments de l'infrastructure et des services informatiques du Client sous la responsabilité du Prestataire.

Le Prestataire intègre un processus de gestion des incidents dont les objectifs sont d'intervenir le plus rapidement possible en cas de défaillances réelles ou potentielles, de maintenir la communication entre le Prestataire et le Client sur la situation et d'évaluer la récurrence potentielle d'un incident.

Le suivi et la gestion des incidents sont assurés jusqu'à 24x7x365.

Le Prestataire traite les incidents :

- En mode proactif, suite à la détection par les outils de surveillance, par une administration des correctifs concertée avec le Client et par la gestion du cycle de vie.
- En mode réactif, suite à un incident signalé par le Client. Les incidents sont gérés pour résolution selon les processus standards de gestion des incidents du Prestataire, la classification des incidents et les objectifs de niveaux de service fixés en fonction du niveau de support associé.

Quelle que soit l'origine de l'alerte, le Prestataire nomme un gestionnaire d'incidents, conformément aux recommandations ITIL sur la gestion des incidents :

- Prise en compte de l'incident
- Classification de l'incident en fonction de sa gravité
- Analyse et diagnostic
- Résolution par instruction définie par l'application et reprise de l'exploitation
- Clôture du dossier d'incident après accord du Client

7.3.4. Gestion des demandes de changements

Dans le cadre des services de la solution Private Cloud, le Prestataire gère les demandes de changement de service des clients sur la base des outils et processus d'Orange.

Le Prestataire fournit au Client un accès au portail Managed Services Changes, qui permet au Client d'envoyer des demandes en ligne pour des changements techniques à effectuer par le Prestataire. Le Client peut accéder au portail des changements de service en utilisant un lien sécurisé.

Deux types de demandes de changement :

- Les demandes de changement de service standard dont l'exécution est entièrement documentée dans un catalogue de service de changement et a été testée et approuvée par les opérations du Prestataire. Les demandes de changement de service standard sont soumises et pilotées selon les processus de demande de changement du Prestataire en utilisant les outils de gestion des changements du Prestataire (portail ECE).
- Demandes de changement de service non standard : elle font l'objet d'un devis spécifique et sont soumises à la validation du Prestataire. Le point d'entrée de cette demande est le CBM (Contract Business Manager) ou le Customer Service Center.

7.3.5. Gestion de la capacité et des performances

Le Prestataire fournit un pool de ressources avec une capacité associée qui est limitée par les règles d'ingénierie de résilience (planification cohérente de la capacité).

Le Client bénéficie de l'état de son utilisation de la capacité grâce aux rapports.

Le Prestataire apporte de manière proactive des informations sur la planification de la capacité dans le cadre du processus d'alerte lorsque la capacité utilisée par le Client est sur le point d'atteindre des seuils déterminés contractuellement.

La gestion de la capacité surveille et agit principalement sur :

- Les ressources CPU/RAM,
- Les ressources réseau,
- Les ressources de stockage et de sauvegarde,
- Les licences de logiciels.

Les demandes de ressources supplémentaires font l'objet d'un devis spécifique. Elles sont effectuées par le Prestataire puisque les ressources matérielles physiques sont sous sa responsabilité.

Par défaut, tous les éléments de performance de l'infrastructure du Client sont collectés par le Prestataire.

A partir du niveau de l'OS managé, le Prestataire peut optimiser les performances du cluster.

Périmètre de la gestion de la capacité et de la performance du Prestataire:

- Maintenir les performances optimales des serveurs dans le temps,
- Analyser périodiquement les statistiques de performance des serveurs et hyperviseurs,
- Recommander les changements nécessaires dans les configurations (serveurs et hyperviseurs),
- Analyser et faire des recommandations suite à toute dégradation significative du temps de réponse.

7.3.6. Reporting & Monitoring

Le Prestataire collecte en permanence l'ensemble des métriques techniques de la plateforme, qu'il s'agisse des VMs ou des objets hébergés sur la plateforme (métriques d'infrastructure et d'instance virtuelle).

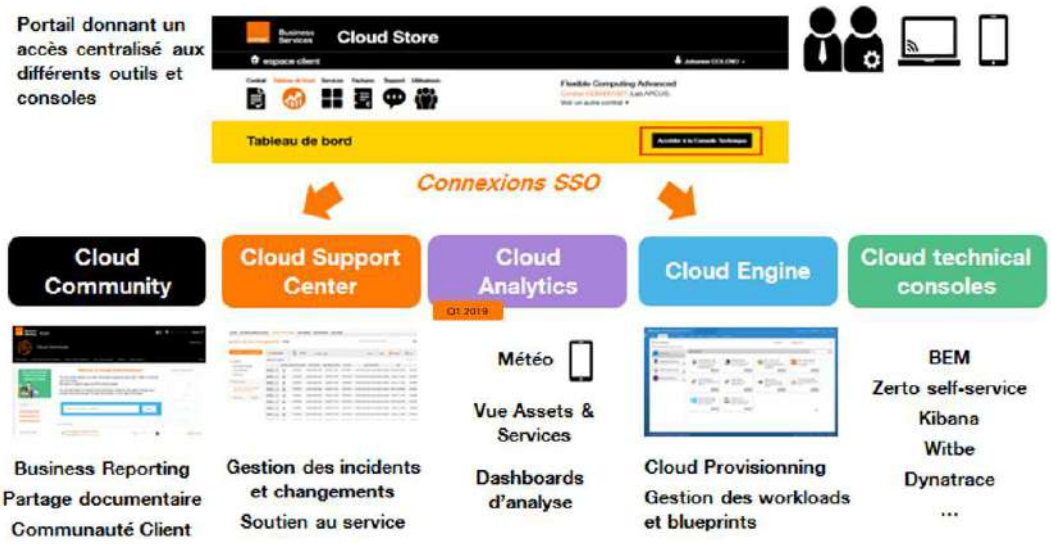
Les métriques d'infrastructure sont ensuite traitées et une panoplie complète d'informations et de statistiques sont mises à la disposition du client sous forme de tableaux de bord ou de rapports :

- Tableaux de bord (ex : via l'accès web de vROPS avec la technologie VMware) avec l'état de santé du cluster en temps réel et les métriques des VMs,
- Rapports opérationnels (alerte, changement, capacité) générés automatiquement et envoyés par email.
- Rapports mensuels (graphiques et tableaux des incidents et changements, tableau récapitulatif des indicateurs de niveau de service par périmètre, nombre d'unités de travail consommées sur la période)
- Rapports d'inventaire : incluant les services et les actifs de la CMDB du Prestataire.

En option, des outils de monitoring spécifiques fournissent des métriques sur les services managés (OS, Middleware, DDB, applications).

Le Client accède aux outils de monitoring/rapports via CloudStore.

Figure 11 : Customer Service Portal



8. Liste des illustrations

Figure 1: Couverture géographique 4
Figure 2 : Exemple de modèles 6
Figure 3 : Fonctionnalités des solutions de Cloud privé 7
Figure 4 : Portail web client 10
Figure 5 : Services Managés 13
Figure 6: Equipe de soutien et d'administration 15
Figure 7 : Service Desk 15
Figure 8 : Incident Management SLA 17
Figure 9 : Problem Management SLA 17
Figure 10 : Change Management SLA 17
Figure 11 : Customer Service Portal 20