

Descriptif de Service - Qualité de Service Managed Applications

Table des matières

1	OBJET	4
2	PRESENTATION DU SERVICE	4
2.1	APERÇU DU SERVICE	4
2.2	IMPLANTATION GEOGRAPHIQUE	5
3	LES MODELES DE MANAGEMENT	5
3.1	LE MODELE DE DELIVERY DU RUN CO-MANAGE	6
4	MANAGED VCOD	7
4.1	DEFINITION	7
4.2	OBJET	7
4.3	SERVICES INCLUS (MANAGED APPLICATIONS)	7
4.4	PRE-REQUIS.....	8
4.5	CONDITIONS DE PRIX	8
4.6	ACCES AU SERVICE ET SUPPORT	8
5	LE BUILD DES SERVICES ET SERVICE MANAGES.....	8
5.1	LE BUILD ET LE DEPLOIEMENT DES SERVICES DANS LE SoW	8
5.2	GESTION ET COORDINATION DU PROJET PENDANT LA PHASE DE BUILD	10
5.3	METHODOLOGIE DETAILLEE DU BUILD.....	10
5.3.1	<i>Inputs pour le Build</i>	10
5.3.2	<i>Transition du Build au Run</i>	12
6	LE RUN DES SERVICES ET SERVICE MANAGES	12
6.1	ORGANISATION DES SERVICES DE SUPPORT	12
6.2	OBLIGATIONS DU CLIENT	13
6.3	LES OFFRES DE SUPPORT	13
6.3.1	<i>Support Niveau 0 (Service Desk)</i>	14
6.3.2	<i>Support Niveau 1</i>	14
6.3.3	<i>Support Niveau 2</i>	14
6.3.4	<i>Support Niveau 3</i>	15
6.4	GESTION DES INCIDENTS	15
6.5	GESTION DES CHANGEMENTS.....	15
6.6	GESTION DES MISES EN PRODUCTION	16
6.7	GESTION DES CONFIGURATIONS.....	16
6.8	MAINTENANCE PROGRAMMEE	16
6.9	SERVICES D'INFRASTRUCTURE INCLUS.....	16
6.9.1	<i>Service d'antivirus</i>	16
6.9.2	<i>Gestion des correctifs et « services packs »</i>	16
6.9.3	<i>Service de Supervision</i>	17
6.9.4	<i>Services DNS</i>	17
6.9.5	<i>Services NTP</i>	17
6.10	SERVICE DE SAUVEGARDE ET DE RESTAURATION MANAGE	17
6.10.1	<i>Description</i>	17
6.10.2	<i>Caractéristiques</i>	17
6.10.3	<i>Limitations</i>	18
6.11	MANAGED BUSINESS APPLICATION	18
6.11.1	<i>Objectifs</i>	18
6.11.2	<i>Scope of Work</i>	18
6.11.3	<i>Gestion de l'application</i>	19
6.11.4	<i>Synthèse</i>	20
6.11.5	<i>Prérequis</i>	20

6.11.6	Limitations	21
6.11.7	Modèle de facturation	21
6.11.8	Catalogue de changements – en Jetons, par action	21
7	CONTENU DU SERVICE	22
7.1	PRESTATIONS D'ACCOMPAGNEMENT	22
7.1.1	Gestionnaire de Services Managés	22
7.1.2	Gestionnaire de Contrats Managés	22
7.1.3	Technicien référent	22
7.1.4	Conception architecture	22
7.1.5	Expertise DevOps	22
7.1.6	Le Service Reliability Engineer (SRE)	22
7.1.7	Le Data Reliability Engineer (DRE)	24
7.2	OS MANAGE	24
7.3	BASE DE DONNEES MANAGEE	24
7.4	MIDDLEWARE MANAGE	24
7.5	SERVICE MANAGE POUR KUBERNETES®	25
7.6	SERVICES NATIFS HYPERSCALERS	25
7.7	BIG DATA MANAGE	26
7.8	COMPUTER VISION MANAGE	27
7.9	RDS MANAGE	27
7.10	AD MANAGE	28
7.11	SECURITE MANAGEE	28
7.12	CITRIX WORKSPACE MANAGE	29
7.13	FLEXIBLE WORKSPACE USER EXPERIENCE [AVD] – AZURE VIRTUAL DESKTOP	29
7.14	EXCHANGE MANAGE	29
7.15	MANAGEMENT DE SERVEURS HEBERGES EN COLOCATION	30
8	ACCES AU SERVICE	30
8.1	PREREQUIS	30
8.2	PORTAIL – ESPACE CLIENT CLOUD STORE	31
9	ENGAGEMENTS DE QUALITE DE SERVICE	32
9.1	ENGAGEMENTS DE QUALITE DE SERVICE	32
9.2	CREDITS DE SERVICE	32
9.3	PLAGES DE SERVICES	32
9.4	CONDITIONS D'APPLICATION	33
9.5	ENGAGEMENTS ET PENALITES	34
9.5.1	Services de portails	34
9.5.2	Garantie de Taux de Disponibilité (GTD)	34
9.5.3	Garantie de Temps de Rétablissement (GTR)	34
9.5.4	Garantie de Temps de Changement (GTC)	35
10	CONDITIONS D'UTILISATION	35
10.1	DUREE MINIMALE	35
10.2	PRIX	36
10.3	REVISION DES PRIX	36
10.3.1	Révision des prix SYNTEC	36
10.3.2	Révision des prix spécifique	36
10.3.3	Révision des prix des licences et équipements managés	37
10.4	REVENU MINIMUM GARANTI (MRG)	37
10.5	PRIX DES PRESTATIONS DE SUPPORT	37
10.6	PRIX DES TICKETS D'INCIDENTS	37
10.7	PRIX DES UNITES DE SERVICE SUPPLEMENTAIRES	37
10.8	FACTURATION BUILD ET RUN	38
10.8.1	Facturation du Build	38
10.8.2	Facturation du run	38
10.9	REVERSIBILITE SORTANTE	38
10.10	CONDITIONS SPECIFIQUES D'UTILISATION DU SERVICE	38
11	DEFINITIONS	39
12	ANNEXES	43
1.1	OS MANAGE : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-OS-MANAGE/	43

1.2	BASE DE DONNEES MANAGEE : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-BASE-DE-DONNEES-MANAGEE/	43
1.3	MIDDLEWARE MANagé : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-MIDDLEWARE-MANAGE/	43
1.4	SERVICE MANAGE POUR KUBERNETES® : ANNEXE-TECHNIQUE-SERVICE-MANAGE-POUR-KUBERNETES®.PDF	43
1.5	APPLICATION MANAGEE : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-APPLICATION-MANAGEE/	43
1.6	SERVICES NATIFS HYPERSCALERS MANAGES :	43
1.6.1	AZURE : HTTPS://CLOUD.ORANGE-BUSINESS.COM/TECHNICAL-APPENDIX-MANAGED-APPLICATIONS-ON-AZURE/	43
1.6.2	AWS : HTTPS://CLOUD.ORANGE-BUSINESS.COM/TECHNICAL-APPENDIX-MANAGED-APPLICATIONS-ON-AWS/	43
1.6.3	GCP : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-MANAGED-APPLICATIONS-POUR-GCP/	43
1.7	BIG DATA MANagé : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-BIG-DATA-MANAGE/	43
1.8	COMPUTER VISION MANAGE : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-COMPUTER-VISION-MANAGE/	43
1.9	AD MANagé : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-ACTIVE-DIRECTORY-MANAGE/	43
1.10	RDS MANAGE : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-REMOTE-DESKTOP-SERVICE-MANAGE/	43
1.11	SECURITE MANAGEE : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-SECURITE-MANAGEE/	43
1.12	CITRIX WORKSPACE MANAGE : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-CITRIX-WORKSPACE-MANAGE/	43
1.13	FLEXIBLE WORKSPACE USER EXPERIENCE – AZURE VIRTUAL DESKTOP [AVD] : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-FLEXIBLE-WORKSPACE-USER-EXPERIENCE-AVD-AZURE-VIRTUAL-DESKTOP/	44
1.14	EXCHANGE MANAGE : HTTPS://CLOUD.ORANGE-BUSINESS.COM/ANNEXE-TECHNIQUE-EXCHANGE-MANAGE/	44
1.15	MANAGEMENT DE SERVEURS HEBERGES EN COLOCATION :	44

Liste des figures

Figure 1	Catalogue de service Managed Applications	5
Figure 2	Modèle de management Managed Applications	5
Figure 3	Exemple de matrice de responsabilité	7
Figure 4	Principaux modèles de construction du SoW par le Prestataire	9
Figure 5	Modèle de management Managed Applications avec MCR	30
Figure 6	Le portail Cloud Store	31

Liste des tableaux

Table 1	Prestation par niveau de Support	13
Table 2	Description de sauvegarde & restauration	17
Table 3	Politique de rétention standard	17

1 Objet

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

Le présent descriptif est rattaché aux Conditions Spécifiques Intégration Maintenance et Prestations associées.

2 Présentation du Service

2.1 Aperçu du Service

Le Service Managed Applications fournit aux Clients plusieurs **niveaux de management** suivants :

1. **Services de gouvernance et de conseil** : gouvernance pour piloter le projet et services d'orientation et de conseil supplémentaires.
2. **OS managé** : Gestion du système d'exploitation comprenant les tâches nécessaires au bon fonctionnement de l'OS, ainsi que la gestion de protection antivirus et les mises à jour de sécurité.
3. **Base de données managée** : Le service fournit au Client une gestion complète de sa ou ses bases de données, y compris les tâches nécessaires à leur bon fonctionnement, leur optimisation de performance et leurs mises à jour de sécurité.
4. **Middleware managé** incluant tous les logiciels proposés au catalogue par les composants :
 - Serveur Web
 - Serveur Proxy
 - Serveur d'application
 - Serveur de fichiers
 - DDI (DNS DHCP, IPAM)
 - Gestionnaire de code source
5. **Service Managé pour Kubernetes®** : Dans le cadre de ce service, Le Prestataire assure la gestion des clusters Kubernetes® hébergés sur l'infrastructure Cloud Public IaaS Cloud Avenue (Le Prestataire).
6. **Application managée** : gestion des Applications métiers Client (web e-business, ERP, CRM, Finance, RH, etc.) sur procédure Client. Prise en charge du déploiement, la migration et la maintenance de vos environnements SAP.
7. **Services Natifs Hyperscalers managés** : supervision et exploitation des services natifs de cloud et les services PaaS des Hyperscalers (Azure, AWS, GCP, FE).
8. **Big Data managé** : Installation, Suivi et Exploitation des solutions Big Data gérées par le Prestataire dont la solution Log as a Service (LaaS) d'analyse de logs de bout en bout qui aide à la recherche approfondie, à l'analyse et à la visualisation des logs générés par différentes machines.
9. **Computer Vision managé** : solution qui utilise les techniques d'Intelligence Artificielle pour permettre au Client d'extraire les données issues de ses équipements vidéo (caméras) à travers des alertes et de tableau de bord dédié.
10. **RDS managé** : gestion du RDS (Remote Desktop Service) Client, permettant aux utilisateurs d'accéder à distance à des applications Windows, hébergé sur une infrastructure Cloud Public IaaS du Prestataire ou Partenaires (AWS, Azure, GCP).
11. **AD managé** : Le Service AD Managé est un service du Prestataire qui permet de gérer les autorisations et les accès des utilisateurs et des ressources sous forme d'annuaire.
12. **Sécurité managée** : Installation, Suivi et Exploitation des composants de sécurité gérés par le Prestataire.
13. **Citrix Workspace managé** : Le Service Citrix Workspace managé est un service du Prestataire qui permet la gestion du Citrix Workspace du Client sur l'infrastructure du Prestataire.
14. **Service Flexible Workspace User Experience – Azure Virtual Desktop [AVD]** : le Service Azure Virtual Desktop [AVD] est un service du Prestataire qui permet la production et la gestion du Workspace Client sur l'infrastructure Azure.
15. **Exchange managé** : Le Service Exchange managé est un service du Prestataire qui permet de gérer la messagerie Exchange du Tenant du Client.
16. **Management de serveurs hébergés en colocation** : Le Service décrit un service complémentaire de gestion de serveurs physiques, hébergés dans une zone de colocation, fourni par le Prestataire.

Il permet au Client d'exploiter ses serveurs physiques existants, tout en bénéficiant des services managés Managed Applications, dans un modèle hybride.

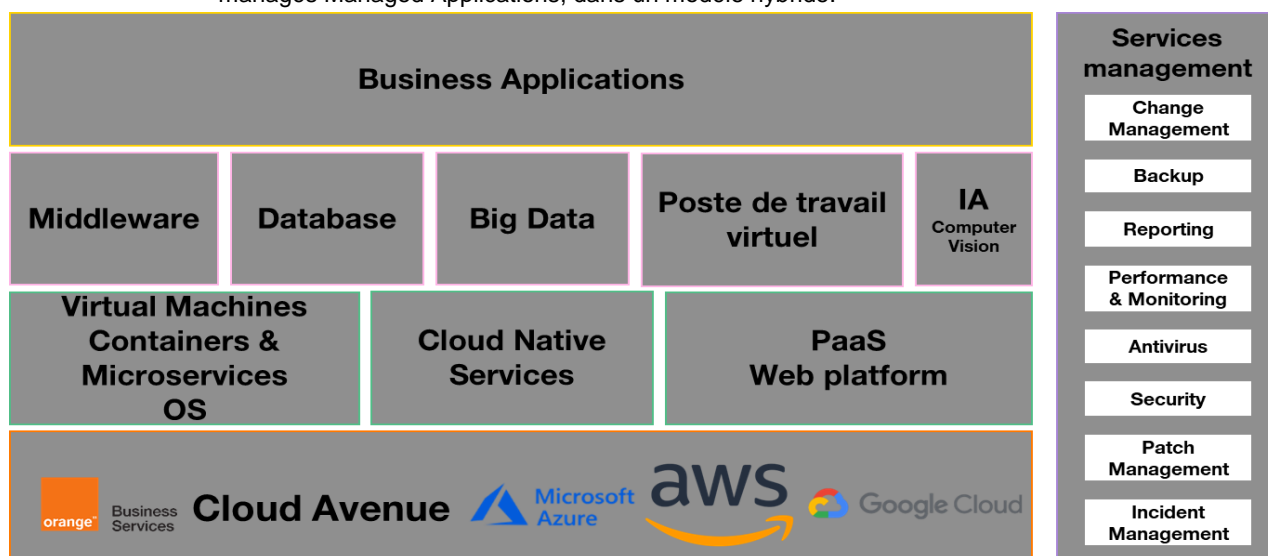


Figure 1 – Catalogue de service Managed Applications

2.2 Implantation géographique

Le Client peut souscrire au Service « Managed Applications » sur chacun des IaaS proposés dans la Commande. Le choix de la Région est fait par le Client au moment de la Commande et consigné dans le dossier d'architecture. Le Service est disponible en France et à l'international.

3 Les modèles de Management

Le Prestataire Services peut soutenir les clients de manière flexible et de différentes manières dans leur utilisation du cloud.

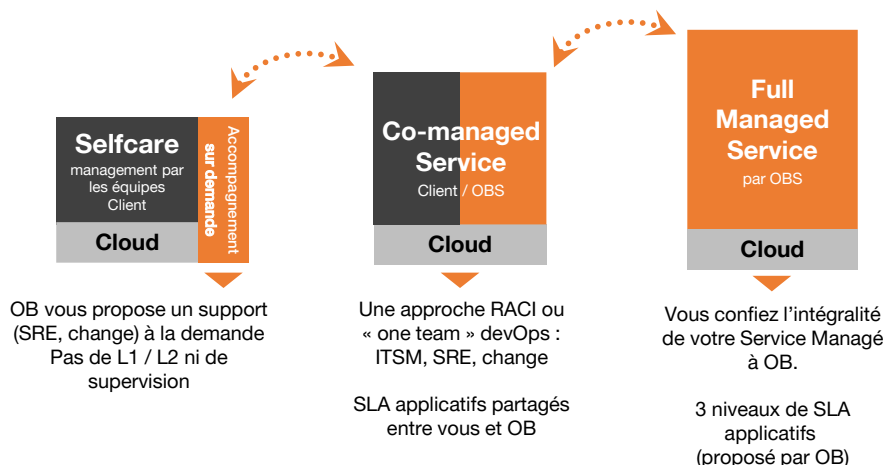


Figure 2 – Modèle de management Managed Applications

L'option "**Fully Managed**" est un modèle dans lequel le Prestataire se charge de tout le déploiement, de la supervision et de l'exploitation des charges de travail du client. Le client a la responsabilité de fournir une charge de travail entièrement testée. Ce modèle est le mieux adapté aux applications et charges de travail stables avec un faible nombre de modifications et de transformations. Il offre une efficacité opérationnelle.

Le modèle de **co-management**, dans lequel le client et le Prestataire partagent les responsabilités du déploiement, de la supervision et de l'exploitation des applications et des charges de travail. Dans ce modèle, le Client prend en charge le développement et les tests de l'application. Le Client peut proposer des modèles de déploiement grâce à un processus de changement. Le Prestataire est responsable de la surveillance et de la maintenance 24 x 7 y compris les heures et les jours non ouvrables et/ou 8 x 5 pour les charges de travail moins critiques. Les deux collaborent à l'aide d'un référentiel Git, d'une chaîne d'intégration et de déploiement continu et d'un outillage partagé pour la surveillance,

la journalisation, les alertes, les tableaux de bord et la communication. Les ingénieurs de fiabilité des services participeront à l'équipe de développement du client pour contribuer à la préparation de l'opérabilité et à son amélioration continue. Ce modèle est un compromis efficace pour obtenir l'agilité de développement, la transformation de l'application et la mise en production fréquente, tout en conservant une assurance de service efficace par la délégation du Prestataire et en préservant les ressources de développement critiques pour les tâches de développement à plus forte valeur ajoutée. Le modèle cogéré peut être complété par un centre d'excellence ou une expertise en matière de cloud.

Le modèle **Selfcare**, dans lequel l'équipe de développement du client est entièrement responsable du développement, du déploiement, de la supervision et de l'exploitation des charges de travail. Dans ce modèle, le Prestataire peut proposer des services professionnels au Client, typiquement sous la forme d'un Centre d'Excellence ou d'Expertise Cloud pour aider le Client à mettre en place les pipelines DevOps, l'outillage, la zone d'atterrissage et l'activité de Build to run. Dans ce modèle, le Prestataire peut également proposer l'ingénierie de la fiabilité des services. Ce modèle est le mieux adapté aux applications et aux charges de travail soumises à un développement et à des modifications intensives avec des déploiements fréquents en production. L'inconvénient est que les développeurs doivent être mobilisés 24 heures sur 24 et 7 jours sur 7 et qu'ils doivent s'occuper de certains aspects opérationnels pendant toute la durée du projet.

Chaque cas de client est spécifique, mais le modèle de co-management prend de l'ampleur, notamment avec l'utilisation de fonctions Cloud Native / PaaS des nuages.

La description du service dans ce document **s'applique à la fois aux services full Managed et aux services co_managed**. Pendant la phase d'Avant-vente ou de conseil, le Client et le Prestataire conviendront du modèle de services managé requis et adapteront le RACI en conséquence. Cela peut varier d'un Client à l'autre, d'un service ou d'une application à l'autre.

3.1 Le modèle de delivery du Run Co-Managé

Le SoW (ou l'étendue des travaux) et le modèle de delivery du RUN sont établis pendant la phase d'avant-vente en fonction des besoins du client. Le présent chapitre établit des lignes directrices qui seront adaptées en fonction du SoW du client.

Le Niveau 3 sont les experts des composants de service. Ils sont les plus compétents pour faire le troubleshooting et résoudre un incident sur un composant de service. Ils mettent en œuvre l'Observabilité, la supervision et les procédures de troubleshooting, la sauvegarde et la procédure de restauration du composant de service. Ils valident les procédures et les transmettent au niveau 2. Ils troubleshootent les incidents et les problèmes en dernier recours lorsque le niveau 2 ne peut pas les résoudre.

Pour les fonctions métier de l'application, le niveau 3 est généralement la responsabilité du client : Les équipes de développement et de test du client - ou des équipes tierces sous-traitées par le client - qui ont codé, déployé et testé l'application métier et la fonction métier. Le client peut sous-traiter le support à l'éditeur du logiciel de l'application métier et de la fonction métier.

Le client peut souscrire aux services SRE et Cloud Expert Services du Prestataire pour renforcer l'équipe.

Si le client demande au Prestataire de prendre en charge le niveau 3 d'une application métier tierce (avec un partenaire potentiel pour la maintenance de l'application tierce), un accord et un cahier des charges spécifiques seront établis.

Pour les IaaS, PaaS, OS, Base de données, il est commun que le client fasse appel au Prestataire pour prendre en charge le Niveau 3. Cependant, d'autres schémas sont possibles et peuvent être discutés et établis lors de la phase d'avant-vente.

Voici un exemple de modèle de responsabilités pour un projet

Component	Level 3	Level 2	Service Desk / Level 1	Comment
Business Application	Customer devops team with contribution of SRE	OBS based on procedures provided by Level 3	OBS	
Business Function	Customer devops team with contribution of SRE	OBS based on procedures provided by Level 3	OBS	
External Interface	Owner of the interface (3rd party ?)	Notifies customer	OBS	Owner of the interface may be a 3rd party
Business Function specifics metrics and alerts on Micro-services, MW, DB, IaaS, PaaS	Customer devops team with contribution of SRE	OBS based on procedures provided by Level 3	OBS	
Middleware	Customer with support of 3rd party editor	OBS based on procedures provided by Level 3	OBS	
Middleware (part of OBS portfolio)	OBS L3	OBS	OBS	Supported middleware and middleware versions
SAP, SAP Hana	OBS L3	OBS	OBS	L3 for SAP business workflows with a partner
Map reduced, ELK (Big data)	OBS L3	OBS	OBS	L3 for Big Data business analysis with a partner or OBS D&D
Database	OBS L3	OBS	OBS	Supported DB versions
Kubernetes cluster	OBS L3	OBS	OBS	
OS	OBS L3	OBS	OBS	Supported OS versions
IaaS & PaaS Cloud Native Services	OBS L3	OBS	OBS	Support from CSP shall be subscribed by customer / or IaaS / PaaS resold by OBS

Figure 3 – Exemple de matrice de responsabilité

Note : pour certaines solutions du portefeuille du Prestataire, typiquement Managed SAP, Managed Computer Vision, Flexible Web Platform, Hub EDI, Corporate e-Invoicing, LogaaS, le Prestataire prend la responsabilité du niveau 3 et a établi un partenariat et un accord de support avec un prestataire de maintenance tierce ou les éditeurs de logiciels impliqués.

4 Managed vCoD

4.1 Définition

Le Service Managed vCoD (Virtual Cloud Director) correspond à l'utilisation du vCoD comme socle d'infrastructure pour les services managés de type Managed OS, Managed Database, Managed Middleware et Managed Applications opérés par le Prestataire.

4.2 Objet

Ce document décrit le rôle du service Managed vCoD dans l'offre Managed Applications et précise la séparation des responsabilités entre :

- la couche infrastructure et virtualisation (CAV), opérée par le Prestataire dans le cadre du service IaaS,
- la couche Managed Applications, opérée par le Prestataire, qui couvre l'administration des OS, bases de données, middlewares et applications déployés sur les VM exposées par vCoD.

4.3 Services inclus (Managed Applications)

- Managed OS : administration et supervision des OS déployés sur vCoD,
- Managed Database : gestion et support des bases de données,
- Managed Middleware : exploitation des middlewares applicatifs,
- Managed Applications : gestion applicative selon le périmètre souscrit.

4.4 Pré-requis

- Souscription préalable au service vCoD (CAV),
- Usage obligatoire du Bastion MASERPAM pour tout accès à privilèges aux VM vCoD,d
- Comptes utilisateurs nominatifs créés via une demande de changement validée.

4.5 Conditions de prix

- Le coût IaaS (couche CAV) est défini séparément dans l'offre Cloud Avenue,
- Les services managés applicatifs sont facturés selon le modèle d'Unités d'Œuvre décrit dans leurs annexes,
- Les coûts liés au Bastion MASERPAM s'appliquent (socle + utilisateurs supplémentaires).

4.6 Accès au service et support

L'accès aux VM et consoles vCoD se fait via le Bastion MASERPAM avec authentification forte. Le support est assuré par le Service Desk du Prestataire conformément aux engagements du Descriptif de Service – Qualité de Service.

5 Le Build des Services et Service managés

5.1 Le Build et le déploiement des services dans le SoW

Le Full Build et le déploiement d'une application métier, des services et des services managés sur une plateforme cloud donnée impliquent :

- **La construction de l'infrastructure cloud comprenant :**
 - o La Landing Zone transverse pour de multiples applications.
 - o L'infrastructure cloud spécifique à chaque application
- **Le déploiement du logiciel de l'application métier sur l'infrastructure.**
- **Le Build de la couche des Opérations, y compris :**
 - o La sélection et la configuration de services utilisés pour les opérations, notamment ceux spécifiques à la plateforme.
 - o La configuration et le déploiement des exporteurs de mesures d'observabilité, de journaux, d'agents, de sauvegarde et d'autres paramètres opérationnels nécessaires aux opérations.
- **L'intégration dans le backend d'administration du Prestataire, y compris :**
 - o La fourniture et la connexion de l'accès administratif à la plateforme cloud.
 - o L'intégration des alertes de surveillance de la plateforme Cloud vers l'outil de supervision du Prestataire Niveau 1 / 2 & 3
 - o L'intégration des procédures de dépannage dans la base de données de connaissances des opérations.
 - o Configuration et fourniture de l'outil ITSM du Prestataire pour le traitement des tickets d'incident et des demandes de changement.
 - o Configuration et mise à disposition du portail du Prestataire pour l'accès aux documents contractuels et à la facturation.

En fonction de l'état d'avancement du projet et de la demande du client, **le SoW restant pour le Build afin de répondre aux critères de RUN peut être le Full Build ou un Build partiel.** Le SoW de Build est discutée lors de la phase d'avant-vente.

Le client **peut conserver ou déléguer une partie des responsabilités de Build du Prestataire :**

- La construction de la couche Infrastructure du Cloud (IaC)
- La construction de la couche des opérations
- L'intégration dans les outils d'administration du Prestataire.

L'estimation de l'effort de Build est personnalisée et dépend du SoW du projet. À la demande du client, le Prestataire peut fournir des ressources d'experts du Cloud et des prestations de SRE pour rejoindre et renforcer l'équipe de développement du client.

Bien que l'effort de Build et son estimation puissent être personnalisés, par souci de simplification et d'anticipation budgétaire de la part du client, **le Prestataire a prédéfini 4 modèles de Build pour une ressource gérée en mode cloud** :

1. **Modèle "No Build"** : Le Prestataire ne fera pas de Build - la ressource n'est pas managée.
 2. **Modèle "Backend Build"** : Le Prestataire effectuera seulement l'intégration de l'environnement du client au backend d'administration. Le client s'occupe de tous les autres aspects de Build.
 3. **Modèle "Operations Build"** : Le Prestataire construira la couche opérationnelle et effectuera l'intégration de l'environnement du client dans son backend d'administration. Le client s'occupe de la construction de l'infrastructure et du déploiement du logiciel.
- **Modèle "Full Build"** : Le Prestataire construira l'infrastructure avec l'IaC, la couche des opérations et l'intégrera dans son backend d'administration. Le client s'occupe du logiciel.

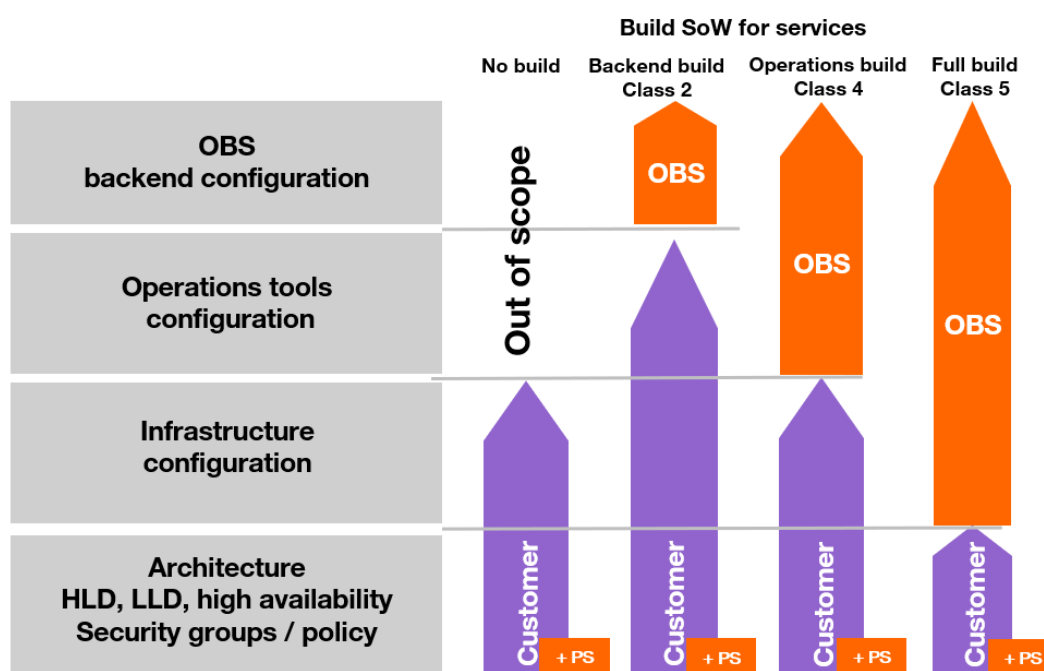


Figure 4 – Principaux modèles de construction du SoW par le Prestataire

En ce qui concerne le SoW, Le Build de la première ressource cloud native d'un type donné implique généralement un effort plus important que le Build d'une ressource ultérieure du même type, car l'IaC peut être réutilisée en grande partie. Cette possibilité dépend de la ressource "cloud native" considérée.

Par conséquent, **chaque modèle de Build distingue** :

- **L'effort et le prix de Build pour la première ressource d'un type donné.**
- **L'effort et le prix de Build pour la ressource suivante du même type.**

Si le SoW diffère des modèles, un SoW sur mesure doit être estimé.

5.2 Gestion et coordination du projet pendant la phase de Build

Pendant la phase de Build, le SoW de la gestion du projet et la coordination de la mise en œuvre des services est défini afin de garantir une exécution efficace du projet entre le client et le Prestataire.

En option, le projet peut nécessiter des **Cloud Experts Services**, des **Service Reliability Engineer** ou **Data Reliability Engineer**.

Ces services sont facturés en fonction du temps et des matériaux.

5.3 Méthodologie détaillée du Build

Ce chapitre décrit la méthodologie de Build suivie par le Prestataire pour le modèle **Full Build**. Il s'agit également de la méthode recommandée au client lors du Build de son infrastructure cloud et de sa couche d'opérations. La qualité du Build déterminera la résilience, la facilité de maintenance, la restauration et l'efficacité des opérationnelle. La méthodologie varie d'un projet à l'autre et, à ce titre, le devis dépend du SoW du projet.

5.3.1 Inputs pour le Build

Pour une estimation précise du Build et le lancement du Build du projet, les prérequis suivants sont nécessaires :

- ✓ Schéma d'architecture de l'application et son plan de déploiement dans la plateforme Cloud.
- ✓ Description des environnements requis (Dev, Préprod, Prod)
- ✓ Politiques de sécurité et contrôle d'accès
- ✓ Topologie des environnements
- ✓ Type et inventaire des applications, middleware, services IaaS/PaaS utilisés
- ✓ SoW et RACI

Si le client fournit ces informations lors de l'avant-vente, le Prestataire établira un devis précis pour le Build.

Dans le cas contraire, si le client ne dispose pas de ces informations lors de la phase d'avant-vente, des hypothèses génériques seront utilisées pour l'estimation du Build. Les spécifications de Build et le devis seront mis à jour pendant la phase initiale du projet après un audit ou après que les informations auront eu été fournies.

Néanmoins, veuillez trouver ci-dessous l'approche de référence par défaut du Prestataire pour le Build de services managés sur une plateforme Cloud donnée. Le SoW variera en fonction des projets des clients.

5.3.1.1 Initialisation du projet : Build de la Landing Zone

Au début du projet, nous construisons une "Landing Zone".

Nous utilisons l'**Infrastructure as Code** (IaC) pour la qualité, la répliquabilité et la reprise après sinistre. Les services de la plateforme Cloud sont déployés à l'aide de ce IaC, par opposition à l'utilisation de l'interface homme-machine :

- Le code de déploiement peut être testé et validé sur un environnement de non-production (par exemple, dev, intégration, staging, préprod) avant d'aller en production.
- Peut être dupliqué et évoluer
- Peut être utilisé pour restaurer le service après un sinistre.
- Peut être versionné
- Peut associer le déploiement des ressources ainsi que la configuration des opérations (surveillance, Logging, sauvegarde...)
- Facultatif : lorsqu'il est disponible dans un outil multicloud, par exemple Terraform, l'IaC peut être exploité pour d'autres cloud avec des changements minimes.

Par défaut, le Prestataire utilise **Terraform et les outils cloud natifs** comme langage pour l'IaC.

- Terraform est plus générique et utilisable sur plusieurs cloud avec des adaptations limitées.

L'IaC est géré avec une chaîne d'outils :

- Par défaut, la préférence serait d'utiliser Terraform.
- En option, des plateformes multicloud peuvent être proposées sur la base **d'OpenSource** agnostiques au cloud comme Concourse, Gitea / Gitlab, Terraform et Rancher, Quay pour les conteneurs. Dans ce cas, un devis spécifique distinct de l'abonnement de la plateforme Cloud sera fait pour l'utilisation de ces outils.
- L'utilisation d'un software Factory spécifique au client nécessite une évaluation de la faisabilité et de la portée car elle a un impact sur les processus de Build et de Run.

3 parties principales du **IaC** sont mises à profit :

1. **Le référentiel basé sur GIT** où la base du code IaC est stockée et versionnée.
2. **Les pipelines** pour le Build
3. **Les pipelines pour les versions/modifications**

En se basant sur les spécifications, le développeur IaC du Prestataire affecté au Build, codera le IaC et préparera les pipelines pour le Build en fonction des plans Terraform.

Par exemple, le code peut être structuré dans plusieurs **pipelines de Build** et plans Terraform pour :

- la souscription,
- management
- Identité
- VM
- Base de données
- etc...

Le développeur IaC testera la qualité du code.

Exemple

- Il fait un pull request sur la branche master
- Il lance automatiquement un Terraform Format, un Terraform validate pour valider la syntaxe.
- Il lance un déploiement sur la plateforme Cloud pour valider le bon déploiement.

Les bibliothèques IaC du Prestataire permettent de gagner du temps dans le développement de l'IaC, néanmoins, les projets ont souvent spécificités et nécessitent des adaptations et des développements sur mesure.

Ensuite, les développeurs du Prestataire créent les "**pipelines de déploiement**".

- ⇒ Le pipeline de déploiement est la manière dont on déploie l'IaC sur chaque environnement Cloud.
- ⇒ Le pipeline de déploiement automatise le processus de déploiement sur la plateforme de dev, puis d'intégration/staging, puis de préprod, puis de production à titre d'exemple si le Client dispose de tels environnements.
- ⇒ Le release pipeline est une base de code qui évolue selon l'environnement.
- ⇒ Pour chaque environnement, les développeurs IaC du Prestataire définissent des **variables d'environnement** afin d'adapter les consommations des ressources en fonction de la plateforme : par exemple, une petite VM pour le dev, une grande pour la prod.

Un développement sur mesure peut être nécessaire pour répondre au cahier des charges du client et fera l'objet d'un devis spécifique. Par exemple, la mise en œuvre d'un DNS forwarder pour la connectivité de la plate-forme.

Le développeur du Prestataire enrichit les pipelines de Build de l'IaC avec **les outils d'Opération**, à savoir la supervision, le Logging et les sauvegardes. Ensuite, la connexion au système de supervision central du Prestataire Managed Application est configurée pour alerter le niveau 1 en cas d'incident.

Si le client souscrit à des services managés pour la couche applicative, celle-ci sera ajoutée aux pipelines en utilisant Ansible ou Jenkins. Le pipeline peut être découplé ou combiné avec la couche infrastructure.

Les pipelines de **la couche applicative** peuvent déployer les applications sur une variété de services, qu'il s'agisse de IaaS, Kubernetes®, DBaaS ou PaaS, en tirant parti d'un découplage plus ou moins important avec l'infrastructure sous-jacente, d'une agilité plus ou moins grande et d'une séparation des tâches entre la gestion des applications et la gestion de l'infrastructure. Cette architecture est un facteur clé pour apporter de l'agilité aux développeurs d'applications grâce

à l'automatisation PaaS des couches d'infrastructure sous-jacentes. Elle détermine également le RACI entre le Prestataire et les développeurs du client.

Plusieurs RACI peuvent être envisagés entre le Client et le Prestataire en fonction du niveau de délégation souhaité ou en fonction des plateformes d'environnement.

Exemple : il peut y avoir une Software Factory pour le code applicatif sous la responsabilité du Client se déployant sur une infrastructure gérée par le Prestataire grâce à une Software Factory distincte de l'Infrastructure.

Exemple 2 : les développeurs peuvent tester les alarmes par eux-mêmes dans les environnements de développement, d'intégration et de staging et ensuite, grâce aux SoW et aux procédures, ces alarmes peuvent être utilisées par le Prestataire pour le monitoring de l'environnement de production.

5.3.2 Transition du Build au Run

Le Prestataire Managed Applications promeut le principe selon lequel l'équipe en charge du run développe l'IaC. Néanmoins, le développeur de l'IaC doit expliquer l'utilisation de celle-ci à l'ensemble de l'équipe impliquée dans le run, y compris la manière de l'éditer et de la diffuser.

6 Le Run des Services et Service managés

Les éléments ci-dessous décrivent la gestion du Service telle qu'elle est opérée par le Prestataire pour les prestations fournies.

L'organisation des services est la suivante :

- Le Centre de Services, et plus particulièrement le centre de support Client,
- Le soutien de Services avec les processus suivants :
 - La gestion des changements,
 - La gestion des incidents,
 - La gestion des problèmes,
 - La gestion des configurations,
 - La gestion des mises en production.
- La fourniture de Services avec les processus suivants :
 - La gestion des niveaux de services,
 - La gestion de la disponibilité,
 - La gestion de la continuité,
 - La gestion de la capacité,

6.1 Organisation des Services de Support

- Le Centre de services établit 2 points de contact permettant au Prestataire de recueillir les demandes du Client (ex : changement, modifications, dysfonctionnements ...) afin de lui apporter des réponses. Ces deux points de contacts sont les suivants :
-
- Les **Centres Support Client (CSC)** ou **Service Desk** du Prestataire : sont accessibles 24 heures sur 24, 7 jours sur 7 tout au long de l'année. Chaque CSC bénéficie d'une visibilité sur l'ensemble du Service et des applications Client hébergées,
- Le **Gestionnaire de Services Managés** (ou SDM pour Service Delivery Manager)

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

- Prendre en charge les Demandes et les Incidents, ainsi que leur traitement et résolution
- Communiquer les informations appropriées et à jour au Client concernant le traitement des Incidents et des Demandes qui leur ont été dûment déclarés.

6.2 Obligations du Client

Le Client établit et maintient la liste nominative des contacts habilités à transmettre des incidents et à contacter le Service Desk du Prestataire. Le Service Desk ne répond qu'aux personnes dûment désignées munies de leurs identifiants et codes d'accès.

Le contact principal du Client garantit la mise à jour et la validité des informations relatives aux contacts.

6.3 Les offres de Support

Le Prestataire propose les 3 niveaux de support suivants, selon le niveau de criticité des applications auxquelles le Service est destiné : **Initial**, **Standard** et **Premium**.

Ces 3 niveaux de support sont possibles selon 2 chaînes de support **Off-Shore** ou **Full France**, l'un et l'autre déterminé lors de la phase Avant-Vente avec les experts du Prestataire.

Table 1 : Prestation par niveau de Support

Managed Applications		Initial	Standard	Premium
Service Support	Ouverture du service	8x5	24x7	
	Par le portail Cloud Store	✓	✓	
	Par Mail	✓	✓	
	Par Téléphone. Limité à 5 contacts nommés	✓	✓	
OS managé		Initial	Standard	Premium
Supervision	Supervision de l'infrastructure	✓	✓	
	Supervision du système d'exploitation	✓	✓	
Gestion de la capacité	Reporting sur l'utilisation de l'infrastructure (VM)	✓	✓	
	Reporting sur l'utilisation des ressources par VM (ram/cpu/disk)	✓	✓	
Base de données managée		Initial	Standard	Premium
Supervision	Supervision de la base de données	✓	✓	✓
Gestion de la capacité	Reporting sur l'utilisation des ressources par base de données			✓
	Étude de la capacité (en utilisant l'historique et les tendances)			✓
Middleware managé		Initial	Standard	Premium
Supervision	Supervision du middleware	✓	✓	✓
Gestion de la capacité	Reporting sur l'utilisation des ressources par Middleware			✓
	Étude de la capacité (en utilisant l'historique et les tendances)			✓
Application managée		Initial	Standard	Premium
Supervision	Supervision de l'application	✓	✓	✓
Gestion des versions	Nombre de versions max. par mois	1	2	4
	Exécution des scripts livrés par le Client pour le déploiement automatisé	✓	✓	✓
	Maintien des versions précédentes			1 mois
Gestion de la capacité	Reporting sur l'utilisation des ressources par Application (ram/cpu/disk)			✓
	Étude de la capacité (en utilisant l'historique et les tendances)			✓
	Étude de la capacité (en utilisant l'historique et les tendances)			✓

Les services de support sont souscrits pour un minimum de 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 6 mois sur le nouveau niveau souscrit.

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

6.3.1 Support Niveau 0 (Service Desk)

Le Service Desk représente le niveau 0 du Centre de Support Client et assure les services suivants :

- Un point de contact unique pour les interlocuteurs désignés par le Client
- Un numéro de téléphone unique et une adresse de messagerie unique,
- Des échanges en langue française,
- La prise en charge et le traitement des appels téléphoniques client,
- L'identification de l'appelant et de son offre commerciale,
- L'ouverture d'un ticket d'incident ou d'un ticket de change relatif au traitement des appels émanant des Clients,
- L'aiguillage du ticket vers l'équipe de niveau 1 appropriée,
- Le transfert de l'appel Client vers l'équipe de niveau 1.

Le Service Desk assure ses prestations 24 heures sur 24 et 7 jours sur 7.

Les demandes Client sont enregistrées dans des tickets dans le référentiel du Prestataire. Les informations sont renseignées dans le ticket en respectant les procédures décrites dans la documentation produite à l'issue de l'initialisation du service.

6.3.2 Support Niveau 1

Le Support Niveau 1 assure les prestations suivantes :

- Classification des tickets,
- Traitement initial des tickets
- Pilotage de rétablissement des incidents (sollicitation des équipes niveau 2),
- Communication Client,
- Gestion des demandes Clients,
- Alerter pour déclencher la procédure de gestion des incidents majeurs et des crises,
- Clôture des tickets.

La gestion proactive est effectuée par une équipe Monitoring Niveau 1 (processus standard). Cette équipe est responsable des événements sur les éléments d'infrastructures et de services. Pour les événements correspondant à des impacts ou risques d'impacts sur le service, l'équipe ouvre un ticket dans l'application de gestion des incidents Océane et effectue le premier diagnostic (processus standard).

Le Support Niveau 1 assure ses prestations 24 heures sur 24 et 7 jours sur 7.

Les tickets stockés dans le référentiel du Prestataire sont utilisés pour référencer tous les contacts Clients, les actions menées, et permettent d'activer (si nécessaire) les équipes de Niveau 2.

Les tickets restent de la responsabilité du Niveau 1 jusqu'à la clôture du ticket et l'envoi d'un avis de clôture du ticket vers le Client.

6.3.3 Support Niveau 2

Le Support Niveau 2 assure ses prestations 24 heures sur 24 et 7 jours sur 7. Pendant les Heures Non Ouvrables Française, le Support Niveau est réalisé par des acteurs hors site sous Astreinte.

Le Support Niveau 2 (« Technical Management ») assure les prestations suivantes :

- Gestion des changements : sous pilotage et responsabilité du SDM, et après analyse des impacts techniques, des engagements contractuels, de la complétude des procédures et du retour arrière et après évaluation des risques, réalise les actions de « gestion du changement »,
- Gestion des événements : traite les événements de type Warning et déclenche au besoin la gestion des incidents, problèmes ou changements pour ces événements. Le support N2 monitoring configure les outils de surveillance et l'hyperviseur.
- Gestion des Incidents : Support au Service Desk niveau 1 : fournit un soutien dans la résolution des incidents ne relevant pas de la responsabilité du niveau 1 (complexité, nouveau problème, risque de non-respect des SLAs contractuels),
- Gestion des problèmes : sous pilotage et responsabilité du SDM, participe à la gestion des problèmes, analyse, suivi et proposition de correction technique/fonctionnelle palliative et/ou curative,
- Mise en production : sous pilotage et responsabilité du SDM, réalise la mise en œuvre des changements,
- Pilotage des tickets : sous pilotage et responsabilité du SDM, gère les équipes de support et la relation avec les partenaires dans le cadre de la résolution des incidents, de la gestion des problèmes et/ou de la gestion des changements,
- Pilotage des interventions sur site des équipes de proximité,

- Suivi des performances en production : Capacity Planning,
- Support au SDM : pour les comptes rendus d'incident, tableaux de bord, réunions opérationnelles Client,
- Application des procédures d'escalade,
- Maintien opérationnel des composants techniques et des procédures associées : par exemple, la mise à jour des procédures utilisées par le Service Desk et le Support niveau 1.

Ces documents évoluent tout au long de la vie du projet, sous la responsabilité des équipes RUN.

6.3.4 Support Niveau 3

Le Support Niveau 3 assure ses prestations pendant les heures Ouvrables Françaises.

Le Support Niveau 3 (ou Ingénierie) offre un soutien technique au Support Niveau 2 et peut le cas échéant contacter fournisseurs et partenaires du Prestataire.

Le Support Niveau 3 couvre également les activités suivantes :

- Industrialisation et documentation des composants techniques des plateformes (matériel, système d'exploitation, produits applicatives, base de données...),
- Suivi proactif des évolutions techniques (propositions d'upgrade matériel, système d'exploitation...),
- Intégration des releases applicatifs majeurs.
- Gestion des habilitations d'accès au support
- Gestion des accès aux supports éditeurs (Microsoft...)
- Définition des droits métiers et restrictions associées (Accès aux tenants Cloud, AD, CyberArk)

6.4 Gestion des incidents

Le Prestataire intègre un processus de gestion des incidents, incluant le dépôt par le Prestataire des tickets auprès du fournisseur de IaaS du Client. Les objectifs de ce processus consistent à :

- Intervenir aussi vite que possible en cas de pannes réelles ou potentielles des applications du Client hébergé,
- Maintenir la communication entre le Prestataire et le Client concernant la situation liée à l'incident,
- Evaluer un incident pour déterminer s'il risque de se reproduire ou s'il est symptomatique d'un problème chronique.

Le Prestataire traite les incidents :

- En mode proactif, suite à une détection d'un incident par les outils de supervision,
- En mode réactif, suite à une remontée d'incident par le Client via le CSC.

Les différentes étapes de traitement d'un incident (remonté en mode proactif ou réactif) sont :

- Prise en compte de l'incident,
- Classification de l'incident selon sa Priorité,
- Analyse et diagnostic,
- Résolution et reprise de l'activité,
- Clôture du dossier d'incident après accord du Client.

6.5 Gestion des changements

Les points d'entrée pour une demande de changement sont :

- Le Portail Cloud Store,
- Le Centre de Service Client,
- Le Gestionnaires de Services Managés pour les contrats Client qui bénéficient du niveau de support Premium.

Toute demande changement non standard est soumise à validation préalable du Prestataire, qui peut la refuser.

La liste des personnes autorisées à soumettre des demandes de changement est mise à jour par le Client et transmise au Centre de Service Client ou au Gestionnaire de Services Managés pour la prise en compte des modifications.

Si le Prestataire est à l'origine de la demande de changement, il est demandé un accord explicite au Client avant toute mise en œuvre. Exception sera faite à cette procédure en cas de changement nécessité par la résolution d'un Incident de Priorité 1, tel que défini dans le document Qualité de Service. Dans ce cas, le Prestataire notifie le Client dans les meilleurs délais à l'issue de la mise en œuvre du changement.

Les changements demandés pour une exécution pendant les Heures Ouvrées des centres de service Managed Application (CET) sont tarifés selon le nombre de Tokens indiqué dans le Catalogue de Changements. Pour les

changements demandés pour une exécution en dehors des Heures Ouvrées du centre de service Managed Applications les changements sont facturés le double (x2) du nombre de Tokens indiqué dans le Catalogue de Changements pour les Heures Ouvrées. Pour les changements hors catalogue, les équipes le Prestataire fournissent une cotation spécifique.

L'Unité d'œuvre d'un Token est de 30 minutes. Le Prix des Tokens Off-Shore ou Full France est indiqué dans la fiche tarifaire.

Le Client peut acheter des Tokens à la demande ou souscrire un ou plusieurs packs de Tokens mensuels, obligatoirement jusqu'à la fin de la période d'engagement. Les Tokens non consommés d'un pack ne sont pas reportés au mois suivant.

6.6 Gestion des mises en production

Le Prestataire prend en charge les mises à jour proposées par les fournisseurs de matériels et de logiciels. Ceci comprend les mises à jour mineures – correctifs, patches, service packs et les mises à jour majeures.

L'application des mises à jour majeures fera l'objet d'une prestation facturée au Client.

Lorsque le Prestataire décide de la mise en production d'un nouveau composant, la procédure de mise en production est traitée comme une demande de changement, conformément aux règles définies pour la gestion des changements.

Le Prestataire s'assure de la traçabilité de toutes les interventions en production grâce à un outil d'exploitation utilisé par le CSC. Ces données sont conservées par le Prestataire pendant la durée du Contrat et font foi entre le Prestataire et le Client.

6.7 Gestion des configurations

Le Prestataire gère les référentiels qui contiennent la configuration de tous les éléments qui composent le Service.

6.8 Maintenance programmée

Les plages de maintenance récurrentes sont précisées dans le PQSC.

Par ailleurs, certaines tâches d'administration telles que les correctifs ou la maintenance de la sécurité, sont effectuées de manière proactive par le Prestataire.

Les mises à jour récurrentes de sécurité seront déployées en accord avec le client sur un planning prédéfini sur une année.

Exceptionnellement, Le client pourra être averti en cas d'action urgente et/ou importante jugée nécessaire par le Prestataire la protection et au bon fonctionnement de son environnement managé.

6.9 Services d'infrastructure inclus

6.9.1 Service d'antivirus

La solution est composée d'un logiciel antivirus installé sur chaque serveur (Endpoint Protection).

6.9.2 Gestion des correctifs et « services packs »

Le Prestataire met à disposition du Client des correctifs et « services packs » pour 3 niveaux de management :

- OS managé
- Base de données managée
- Middleware managé

Les mises à jour sont testées et validées par le Prestataire avant d'être autorisées sur la plateforme.

Le Client valide l'application ou non des patches.

Pour tout problème lié au déploiement du Service Pack, le Prestataire ne peut être tenu responsable. Le Client peut demander la restauration de la dernière image de la machine virtuelle.

6.9.3 Service de Supervision

Le Prestataire s'engage à contrôler le bon fonctionnement de l'infrastructure et des composants applicatifs de la solution Client 24h sur 24, 7 jours sur 7 et 365 jours par an, pour chaque niveau de management (OS, base de données, middleware et Application) dont il a la responsabilité. Toute alerte correspondant à un dysfonctionnement avéré par les équipes de supervision donne lieu à l'enregistrement d'un incident auprès du Help Desk.

6.9.4 Services DNS

Le Prestataire met à disposition deux services DNS pour répondre aux besoins suivants :

- Résolution des adresses internet
- Gestion des entrées DNS Public du Client

6.9.5 Services NTP

Le Prestataire met à disposition un serveur NTP comme serveur de temps par défaut.

6.10 Service de sauvegarde et de restauration managé

Ce Service permet au Client de sauvegarder et de restaurer **au niveau fichier** le contenu des serveurs déployés dans des **environnements physiques** ou dans le **Cloud**

Le Client peut également bénéficier de la sauvegarde managée d'Office 365. Elle permet de sauvegarder les données des applications d'Office 365 : Exchange Online, SharePoint Online, OneDrive for Business et Team. Elle fournit aussi la gestion complète de la restauration granulaire des données Office 365 par application et par politique de sauvegarde.

Ce Service s'appuie sur une solution de sauvegarde type BaaS (intégrée à l'infrastructure du Prestataire). Le coût du Service BaaS est supporté par le Client dans le cadre de l'offre IaaS sous-jacente.

6.10.1 Description

Le Service de sauvegarde et de restauration inclut les Services suivants :

Table 2 : Description de sauvegarde & restauration

Phase	Activités
Sauvegarde & restauration Implémentation	<ul style="list-style-type: none">▪ Installer et configurer l'agent sur les serveurs des Clients▪ Configurer la plateforme centrale de sauvegarde pour effectuer les sauvegardes et les restaurations sur les serveurs des Clients▪ Effectuer un test d'acceptation
Sauvegarde & restauration Opération	<ul style="list-style-type: none">▪ Surveillance des sauvegardes Clients▪ Redémarrage de sauvegarde en cas d'échec▪ Procéder aux restaurations sur demande du Client (via change)▪ Surveiller la plateforme de sauvegarde sur une base 24x7x365▪ Evaluation, planification et exécution des demandes de changement du système▪ Planification de capacité sur la plateforme de sauvegarde

6.10.2 Caractéristiques

Le Service de sauvegarde et de restauration peut être fourni à des Clients qui sont déjà abonnés aux services OS managé, Base de données managée, Middleware managé, Application managée. Ce Service peut être également proposé aux Clients qui ont des besoins de sauvegarde/restoration des données on-premise ou dans le Cloud.

Les politiques suivantes de fréquence et de rétention sont prédéfinies dans le système de sauvegarde du Prestataire.

La première sauvegarde en mode fichier ou pour Office 365 réalisée par le Prestataire est une sauvegarde full, les sauvegardes suivantes sont incrémentales suivant la politique de sauvegarde choisie par le Client.

Table 3 : Politique de rétention standard

Politique de rétention	Détails de la politique	Fichier / Office 365
WEEKLY-1	Une sauvegarde hebdomadaire avec 1 semaine de rétention	✓

Politique de rétention	Détails de la politique	Fichier / Office 365	
WEEKLY-2	Une sauvegarde hebdomadaire avec 2 semaines de rétention	✓	
MONTHLY-1	Une sauvegarde mensuelle avec 1 mois de rétention	✓	
MONTHLY-3	Une sauvegarde mensuelle avec 3 mois de rétention	✓	✓
MONTHLY-6	Une sauvegarde mensuelle avec 6 mois de rétention	✓	✓
MONTHLY-12	Une sauvegarde mensuelle avec 12 mois de rétention	✓	✓
MONTHLY-36	Une sauvegarde mensuelle avec 36 mois de rétention		✓

Les Clients peuvent demander des politiques de rétention spécifiques ainsi que des fréquences de sauvegarde personnalisées. Les demandes spécifiques sont soumises au Prestataire pour validation et feront l'objet d'un devis spécifique pour le Client.

6.10.3 Limitations

Les activités suivantes restent de la responsabilité du Client :

- Tests d'acceptation complets qui seront consignés dans un procès-verbal de recette.
- Décision de restauration d'un fichier ou d'un groupe de fichiers

6.11 Managed Business Application

6.11.1 Objectifs

Le client peut déléguer la supervision continue 24h/24 et 7j/7 des applications métier du Prestataire. Les équipes de développement du client peuvent continuer à faire évoluer le code et l'architecture de l'application métier. Dans le mode de co-management, le SRE du Prestataire participera aux réunions de l'équipe Scrum du client pour contribuer aux enablers nécessaires à la gestion de l'application métier.

Le client et le SRE peuvent se concentrer sur la définition des procédures du Prestataire d'Observabilité et de gestion des fonctions métier et s'appuyer sur des services managés standards pour la gestion des dépendances sous-jacentes.

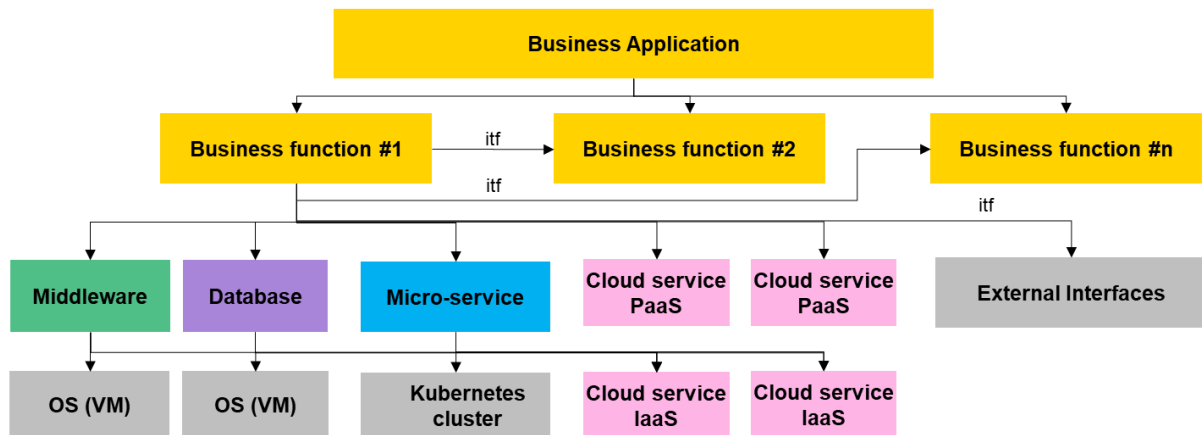
6.11.2 Scope of Work

Le Scope of Work pour le co-management de l'Application métier est défini entre le Client et le Prestataire.

L'architecture de l'Application est expliquée par le client à l'expert du Prestataire pour identifier les composants qui doivent être supervisés et maintenus parmi :

- Les fonctions métier,
- Leurs dépendances aux interfaces avec les autres fonctions métier de l'Application et avec les services externes,
- Leurs dépendances aux systèmes d'exploitation, middleware, bases de données, Microservices, services managés Kubernetes®, Services Cloud, Services Big Data.

Business Application management



L'hypothèse principale pour le co-management de l'application métier est que le logiciel est codé par les développeurs du client ou par un fournisseur tiers de logiciels au client. Le client est responsable - par lui-même ou par l'intermédiaire de son fournisseur - de la maintenance du logiciel et de l'architecture de l'application métier, du fonctionnement de l'application métier et des tests sur l'environnement cloud avant la transition vers le service managé par le Prestataire.

6.11.3 Gestion de l'application

6.11.3.1 Gestion des dépendances

Pour gérer correctement les fonctions métier, il faut gérer les dépendances. Le catalogue de services managés comprend des unités de travail prédéfinies pour les middlewares, bases de données, micro-services, clusters Kubernetes®, OS et services cloud natifs connus. Le client et le Prestataire identifient les dépendances nécessaires à gérer et les ajoutent au SoW conformément à la définition du service dans le catalogue de services (veuillez-vous référer à ce document et à la description d'une application managée).

6.11.3.2 Gestion des interfaces externes

Les dépendances peuvent inclure des interfaces vers des systèmes externes ou des interfaces vers d'autres fonctions métier. Celles-ci doivent également être supervisées afin de détecter et d'identifier rapidement la cause racine d'un incident. La responsabilité de la restauration d'un système externe ne fait pas partie du SoW.

6.11.3.3 Gestion des fonctions métier

Pour les fonctions d'application métier, le SoW sera établie sur la base des données et des livrables fournis par le client :

- Comment la fonction métier est-elle supervisée ? Quel est le RACI entre le client et le Prestataire.
- Quelle est la criticité de la fonction métier pour le service ?
- Quels sont les problèmes connus ? Quelle est la procédure à utiliser pour la restauration ?
- Comment la fonction métier est-elle restaurée en cas de panne ? Est-elle basée sur un redéploiement à partir d'Infra as Code ? Est-elle basée sur la restauration à partir d'une sauvegarde ? Quelle est la procédure ?
- Y a-t-il des routines spécifiques à exécuter ?
- Comment la fonction métier est-elle créée et déployée ? Quelle est la chaîne dev, préprod, prod ? quel est le RACI entre le client et le Prestataire sur les différents environnements ?
- Quelles sont les politiques de sécurité à appliquer et les règles de pare-feu ?
- Un plan catastrophe est-il nécessaire ? Comment est-il réalisé ?
- D'autres services sont-ils requis de la part du Prestataire ? conseil, contrôle de santé, performance, capacité ?
- Quelle est la fréquence des incidents et des changements ?
- Quelle est la fréquence de déploiement des versions ?
- Quelle est la maturité de l'élément ?

Puisque les spécificités des applications métier sont un savoir spécifique du client et de son fournisseur tiers, le client est responsable du support de niveau 3 pour l'application métier (potentiellement par le biais de son fournisseur tiers).

Les tâches de niveau 1 et de niveau 2 du Prestataire consistent à :

- Superviser les fonctions métier convenues dans le SoW
- Appliquer les procédures de remédiation en cas d'incident
- Résoudre un incident sur une dépendance managée
- Notifier et remonter au niveau 3 du client si la résolution n'est pas possible grâce à la procédure.

6.11.4 Synthèse

Le tableau suivant résume le service :

Service	Type	Configuration	Supervision et alertes configurées dans le service de monitoring Cloud natif	Sauvegarde	Procédure de récupération	Gestion des patches	Gestion de l'antivirus	Spécificités
Supervision de la fonction métier	Managé	Le déploiement et le redéploiement de l'application métier sont basés sur le temps et le matériel. Prérequis : Image ou script de déploiement fourni par le client. L'application métier a été testée avec succès sur l'infrastructure avant de passer à l'exécution.	Les exporters de métriques et les alertes vers l'outil de monitoring Cloud natif ou Prometheus fournis par le client comme prérequis.	La sauvegarde et la restauration sont une option. Le client doit identifier les procédures de sauvegarde nécessaires pour protéger les données des applications métier. Et confirmer si la sauvegarde des composants sous-jacents est suffisante ou non.	Procédure de dépannage et de restauration fournie par le client. La procédure doit durer moins de 15 minutes. Sinon, elle sera facturée en fonction du temps. Le client fournit un support de niveau 3.	Le client est responsable du logiciel et des correctifs logiciels.	Le Client est responsable de l'antivirus du logiciel de l'Application métier.	En option : Portée du travail à définir avec le client Prérequis : les dépendances doivent être gérées.
Supervision d'une interface externe	Managé	Le prérequis est que l'interface externe soit exposée et joignable. Hors du champ d'application du service managé.	Une partie du logiciel ou une sonde teste la disponibilité de l'interface externe.	n/a	Le client est informé lorsque l'interface externe est en panne. Le support de l'interface externe est hors du champ d'application du service MA.	n/a	n/a	n/a
Dépendances des services Cloud	Managé	Référez-vous à chaque service cloud managé (selon le catalogue) dont la Business App dépend.						

6.11.5 Prérequis

L'architecture de l'application et son déploiement dans le cloud doivent être définis. L'architecture est hors du champ d'application du service.

L'application doit être déployée et testée par le client avant d'être transférée à l'équipe des opérations.

En général, les tests sont réussis en préproduction, avec un environnement de préproduction iso-production. L'application métier exporte les métriques vers un service de monitoring Cloud natif.

La stratégie de sauvegarde des données et la stratégie de reprise après sinistre sont fournies par le client.
Le troubleshooting et la restauration du service doivent être fournies par le client.
Si une procédure nécessite des logs ou un Dashboard, ceux-ci doivent avoir été développés par le client avant d'être managé par le Prestataire.

Une procédure de remédiation sur incident ne doit pas durer plus de 15 minutes. Au-delà de cette durée, l'effort sera facturé sur la base du temps passé.

Le client doit avoir souscrit au service d'application managée pour les composants sous-jacents dont l'application métier dépend.

6.11.6 Limitations

Les services requis par les Cloud Service Providers pour l'Observabilité, le logging, la supervision et la sauvegarde ne sont pas inclus dans le service et sont donc facturés dans le cadre de l'abonnement au CSP.

Les logiciels d'application métier et la maintenance des applications tierces ne sont pas inclus dans le service. Les clients sont responsables du Patching de l'application, sa vulnérabilité et de l'absence de virus.

Le champ d'application du service Managed Business Application et la responsabilité du Prestataire en matière de sécurité se limitent à la configuration des pare-feux et des groupes de politiques du CSP, conformément aux spécifications du client. Si d'autres services de sécurité sont nécessaires, ils feront partie d'un cahier des charges optionnel convenu d'un commun accord.

Les utilisateurs finaux des applications métier ne sont ni gérés ni supportés.

La gestion des performances des applications fait l'objet d'un cahier des charges et d'un devis sur mesure.

Le Build, le pipeline et le déploiement de l'application sont hors du SoW de l'unité de travail standard. Un cahier des charges spécifique doit être établi.

6.11.7 Modèle de facturation

Service	Unité d'oeuvre
Service Reliability Engineer	Temps et matériel
Fonction métier – supervision – priorité faible	Par source de supervision
Fonction métier – supervision - standard	Par source de supervision
Fonction métier – supervision - critique	Par source de supervision
Interface externe – supervision – priorité faible	Par source de supervision
Interface externe – supervision - standard	Par source de supervision
Interface externe – supervision - critique	Par source de supervision
Sauvegarde de données	SoW
Reprise après sinistre	Scope of Work
Dépendances: OS, middleware, database, Kubernetes®, microservices, big data	Unité d'œuvre du catalogue des services managés
Incident signalé par le client	Par ticket d'incident

6.11.8 Catalogue de changements – en Jetons, par action

Exemples de changement	Effort
Ajout d'une nouvelle alarme	Sur devis ou estimation en jetons en fonction du temps passé. Unité d'œuvre récurrente supplémentaire
Déploiement d'une application métier	Sur devis ou estimation en jetons en fonction du temps passé.
Ajout d'une nouvelle procédure de dépannage à la base de données des connaissances opérationnelles	Sur devis ou estimation en jetons en fonction du temps passé.
Dépannage au-delà de 15 minutes en raison de la longueur d/e la procédure.	Sur devis ou estimation en jetons en fonction du temps passé.

7 Contenu du Service

7.1 Prestations d'accompagnement

7.1.1 Gestionnaire de Services Managés

Le Gestionnaire de Services Managés (ou SDM pour Service Delivery Manager) est l'interlocuteur privilégié du Client pour le bon fonctionnement du Service Managed Applications.

Cette prestation doit obligatoirement être souscrite pour chaque Projet qui inclut au moins un Tenant Managé de niveau de support Premium. Cette prestation n'est pas disponible pour les Projets incluant uniquement des Tenants Managés de niveau de support Standard.

Le Gestionnaire de Service Managé assure les prestations suivantes :

- Participation à la mise en œuvre des évolutions / des améliorations du Service du Client dans la phase de run,
- Suivi du bon fonctionnement du Service du Client dans la phase de run,
- Conseille le Client sur les évolutions possibles des Services souscrits,
- Intervient en escalade – soit à la demande du Client, soit sur sollicitation des équipes du Prestataire, soit de manière proactive,
- Mise en œuvre et pilotage du processus d'assurance qualité,

7.1.2 Gestionnaire de Contrats Managés

Le Gestionnaire de Contrats Managés (ou CBM pour Contract Business Manager) est l'interlocuteur contractuel privilégié de la DSI du Client pour le Service Managed Applications.

Cette prestation doit obligatoirement être souscrite pour chaque Projet qui inclut au moins un Tenant Managé de niveau de support Premium. Cette prestation n'est pas disponible pour les Projets incluant uniquement des Tenants Managés de niveau de support Standard.

Le Gestionnaire de Contrats Managés assure les prestations suivantes :

- Il s'assure du respect des engagements contractuels et commerciaux du Prestataire vis-à-vis du Client
- Il met en œuvre, suit et met à jour l'espace documentaire du Client
- Il anime la gouvernance : Comité de Pilotage et Comité Stratégique
- Il est l'interlocuteur privilégié du Client pour tout ce qui concerne les évolutions contractuelles en vie de solution

7.1.3 Technicien référent

Le Technicien référent est l'interlocuteur technique privilégié du Client dans la phase de run du Service. Cette prestation est préconisée pour les projets complexes.

Le Technicien référent assure les prestations suivantes :

- Organisation des comités techniques visant l'amélioration de la performance de la solution ;
- Investigation sur les dysfonctionnements et proposition de solutions ;
- Etude et réalisation des changes.

7.1.4 Conception architecture

La prestation de conception d'architecture consiste à fournir un dossier d'architecture pour le projet du Client au terme d'une étude basée sur le cahier des charges du Client. Cette prestation est préconisée pour les projets complexes.

7.1.5 Expertise DevOps

La prestation d'expertise DevOps fournit conseil et une assistance technique pour la mise en œuvre par le Client d'une démarche d'intégration / livraison en continu sur son Tenant Managé.

Un rapport contenant les préconisations sera communiqué au Client à la fin de chaque intervention.

7.1.6 Le Service Reliability Engineer (SRE)

Le Service Reliability Engineer (SRE) est un acteur clé des services managés, notamment dans le modèle DevOps et le modèle de Co-management.

Le SRE est un expert nommé, connaissant les opérations et le génie logiciel, participant simultanément à l'exécution du service géré au sein de l'équipe des opérations du Prestataire et travaillant étroitement avec l'équipe de développement du Prestataire.

Le SRE travaille en étroite collaboration avec l'équipe de développement du Client pour identifier et mettre en œuvre les indicateurs d'Observabilité, l'automatisation des opérations et l'infrastructure en tant que code pour répondre aux besoins de l'entreprise. Il apporte son expertise à l'équipe de développement pour fournir les outils nécessaires à un fonctionnement fiable. A plus long terme, le SRE contribue à l'amélioration continue de la fiabilité de l'application métier et de ses opérations.

Le SRE participe (à distance) à des réunions régulières avec les propriétaires d'applications pour l'alignement des améliorations continues.

7.1.6.1 Livrables

Le SRE contribue, avec l'équipe de développement, aux livrables suivants :

- Lignes directrices pour l'automatisation DevOps (Infra as Code, intégration, etc.) en fonction de la maturité de l'équipe du Client.
- Infra as Code nécessaire pour déployer / redéployer les ressources en cas de perte de service ou de mauvaise configuration.
- Identification et mise en œuvre des mesures d'Observabilité nécessaires pour surveiller l'activité de l'entreprise.
- Définition et gestion des SLO (Service Level Objective), SLI (Service Level Information)
- Mise en place de tableaux de bord automatisés permettant l'analyse des métriques et des tendances. Des conseils pour l'outillage permettant de les mettre en œuvre.
- Identification des alarmes / seuils sur les métriques et mécanisme de collecte des alarmes.
- Identification des procédures de sauvegarde et des mesures de sécurité nécessaires pour l'application et les données afin de répondre aux besoins du Client.
- Rédaction des procédures principales nécessaires au traitement des incidents connus. Procédures qui seront transmises aux équipes opérationnelles de niveau 1 et 2.
 - Les procédures simples sont généralement intégrées dans l'infrastructure en tant que code pour accélérer les actions correctives.
- Révision/ validation des procédures techniques pour les changements proposés par le Service Delivery Manager pour ajout dans le catalogue des changements.
- Identification et mise en œuvre de la collecte des journaux pour détecter les anomalies et faciliter le dépannage de l'application métier. Mise en place de corrélations et d'alertes automatisées à partir de l'analyse des logs.
- Analyse à froid des tableaux de bord, des logs pour la maintenance préventive sur demande.
- Configuration des outils de sécurité et du SIEM (Security Information & Event Management).
- Définition et rédaction de procédures de contrôle récurrentes lorsque cela est nécessaire.
- Critères pour le "go" à la Préproduction. RACI entre le Client et le Prestataire pour le déploiement en préproduction. Automatisation du déploiement si nécessaire.
- Critères de passage en production en tenant compte des contraintes techniques et métier (temps de déploiement, événements particuliers, etc.). RACI entre le Client et le Prestataire pour le déploiement en production. Automatisation du déploiement si nécessaire.

7.1.6.2 Limitations

- L'architecture n'est pas la responsabilité du SRE. Elle relève plutôt de la responsabilité du Client ou d'un architecte, c'est-à-dire du Technical Design Authority (TDA).
- La conception de la reprise après sinistre ne relève pas du mandat du SRE mais d'un TDA.
- Le build et la conception de l'architecture, y compris la reprise après sinistre, le HLD et le LLD, relèvent de la responsabilité du Client ou d'un architecte

7.1.7 Le Data Reliability Engineer (DRE)

Le Service Data Reliability Engineer (DRE) est un acteur clé des services managés dans l'environnement Big Data managé. L'ingénieur en fiabilité des données est chargé d'aider à fournir une disponibilité et une qualité élevées des données tout au long du cycle de vie des données, de l'ingestion à la visualisation.

Les rôles et missions de l'expert DRE sont définis en concertation et peuvent évoluer dans le temps selon vos besoins :

- La définition avec vos équipes métier d'indicateurs et objectifs de niveau de service (SLI/SLO) à atteindre pour garantir la disponibilité et la qualité de la donnée
- La configuration des métriques et du monitoring pour contrôler l'atteinte ou non des objectifs fixés
- La configuration de l'alerting pour détecter et anticiper les problèmes lors du voyage de la donnée : latence, variation anormale de trafic, goulots d'étranglement, erreurs, débit ou saturation sur les pipelines
- L'automatisation et l'optimisation des chaînes de données (pipeline), l'adaptation de scripts d'IaC et du design d'architecture pour atteindre les SLO
- La détection des tâches ayant échoué et l'automatisation de leur relance automatique.
- L'identification avec notre équipe des causes racine suite à incidents complexes et la mise en place de mesures correctives

7.2 OS managé

Le service fournit au Client une gestion complète de son système d'exploitation, y compris les tâches liées aux VM (Machine Virtuelle). Le service est rendu uniquement sur les Tenants Managés du Client.

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – OS managé » accessible ici [Annexe-technique-OS-Manage.pdf](#) applicables au service OS managé, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.3 Base de données managée

Le Prestataire assure l'exploitation technique de la ou des base(s) de données du Client et les activités d'optimisation et de mise à niveau.

Le système d'exploitation, est toujours complètement managé par le Prestataire, le Client doit souscrire obligatoirement à la prestation OS managé.

Pour les DBaaS (DataBase as a Service) managées, les licences des logiciels de base de données sont fournies soit :

- ✓ Dans le cadre du service IaaS souscrit par le Client
- ✓ Par le Prestataire, titulaire des Licences. Dans les autres cas, les licences des Logiciels de base de données sont souscrites,
- ✓ Ou par le Client selon les conditions de l'éditeur des Logiciels.

Pour les DBaaS managées, le coût du service DBaaS est supporté par le Client dans le cadre du service de IaaS qu'il a souscrit.

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – Base de données managée » accessible ici <https://cloud.orange-business.com/annexe-technique-base-de-donnees-managee/> applicables au service Base de données managée, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.4 Middleware managé

Les « middlewares » sont installés et configurés par le Prestataire.

Le système d'exploitation, est toujours complètement managé par le Prestataire, le Client doit souscrire obligatoirement à la prestation OS managé.

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – Middleware managé » accessible ici <https://cloud.orange-business.com/annexe-technique-middleware-manage/> applicables au service Middleware managé, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.5 Service Managé pour Kubernetes®

Le service de gestion des clusters Kubernetes® est proposé par Le Prestataire sur l'infrastructure Cloud Public IaaS Cloud Avenue. Ce service inclut :

- Le déploiement de clusters Kubernetes® selon les configurations fournies par Le Client.
- La supervision 24/7 et le maintien en conditions opérationnelles des clusters.
- La gestion des incidents, incluant la notification et les interventions pour la remise en état des clusters.
- La restauration des clusters à partir d'un référentiel sauvegardé.
- La gestion des changements sur les clusters.
- Des outils managés pour la collecte, le stockage et la visualisation des logs et métriques.
- Un outil de visualisation pour que Le Client puisse observer les métriques et alertes configurées.
- L'accès optionnel à des outils DevOps (Managed DevOps Toolkit) pour le déploiement d'applications sur les clusters.

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – Service Managé pour Kubernetes® » accessible ici [Annexe-technique-Service-Manage-pour-Kubernetes®.pdf](#) applicables au service Service Managé pour Kubernetes®, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire. Application managée

Le niveau de management « Application Managée » permet de fournir au Client les prestations suivantes :

- Installation du serveur d'application,
- Exploitation et administration de l'application,
- Reporting et statistiques de l'application,
- Supervision de l'application
- Sauvegarde de l'application.

Le Prestataire peut prendre en charge la gestion complète des applications du Client sur devis en option.

Managed Applications for SAP® est une application managée métier pris en charge par le Prestataire pour la gestion de vos environnements SAP® :

- Nous vous fournissons des paysages SAP® sur un cloud 100% virtualisé et certifié
- Nous gérons vos environnements afin que vous puissiez vous concentrer sur vos applications et votre activité
- Nous prenons en charge le déploiement, la migration et la maintenance de vos environnements SAP

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – Application managée » accessible ici <https://cloud.orange-business.com/annexe-technique-application-managee/> applicables au service Application managée, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.6 Services Natifs Hyperscalers

Le Prestataire assure l'exploitation technique et la surveillance des Services Natifs AWS, Azure ou GCP du Client, ainsi que les activités d'optimisation et de mise à niveau par la mise en place d'une interconnexion réseau entre la "zone de service" du Prestataire et la plateforme Cloud du fournisseur.

Au début du projet Client :

- ❖ Un audit est nécessaire pour déterminer l'inventaire des ressources à manager, leur Classe de transition, l'étendue du travail restant à accomplir pour être prêt à fonctionner, le RACI et les limitations du service à manager.
- ❖ La construction d'une zone d'atterrissage est nécessaire. Le déploiement de l'infrastructure est modélisé en tant qu'Infrastructure as Code (IaC) pour la qualité, la reproductibilité et la reprise après sinistre. Les Services Natifs, AWS, Azure ou GCP sont déployés à l'aide de ce IaC.

La définition des Classes de transition pour les ressources à transférer puis à manager par le Prestataire sont précisées dans l'annexe technique AWS, Azure ou GCP.

Les tarifs indiqués dans la fiche tarifaire pour les Services Natifs AWS, Azure ou GCP ne concernent que le service délivré par le Prestataire. La tarification des ressources IaaS des Hyperscalers concernés ne sont pas comprises dans la prestation du Prestataire, et apparaissent sur la facture IaaS du Client.

Le prix des services visés dans ce paragraphe et applicable au Client est calculé en tenant compte des éléments suivants :

- ❖ Du nombre d'unités de Services Natifs managées ou pour lesquelles le service managé est souscrit après validation avec le Client à travers un HLD (High Level Design). L'engagement de service et de prix du

Prestataire repose sur les services natifs indiqués dans le HLD ainsi que les micro-services, middleware, application, base de données, sous-jacents.

- ❖ De la Classe de transition appliquée, suite à l'inventaire des ressources à manager, que va réaliser le Prestataire lors de l'audit. Pour certains services, la responsabilité du Prestataire peut se limiter au maintien du laC et la gestion des changes uniquement, ou inclure la supervision.
- ❖ Du SRE (Site Reliability Engineering), qui correspond au maintien de l'infrastructure as code ou à une recommandation pro-active d'amélioration de l'laC par le Prestataire. Une quote-part SRE est incluse en standard dans le Service managé opéré par le Prestataire, une provision est prévue au-delà qui sera facturée en dépense contrôlée par le Client.
- ❖ De la chaîne de support utilisée :
 - ❖ « Standard » via notre chaîne de support localisée au Caire pour le service desk L0/L1
 - ❖ « Full France », dans laquelle le Client peut disposer d'une chaîne Full France ou d'une chaîne Full France avec sécurité renforcée, via notre chaîne de support localisée en France. L'incidentologie (nombre de tickets mensuels L0/L1) sera définie avec le Client et le Prestataire en fonction de son besoin.
- ❖ Du nombre de jours liés à la gouvernance via :
 - ❖ Le gestionnaire de services managés pour le suivi des kpi/reporting mensuels,
 - ❖ Le gestionnaire de contrats managés pour le suivi contractuel et facturation.
- ❖ Du nombre de tenant(s) managé(s) qui héberge(nt) l'environnement du Client, administré et supervisé par les équipes du Prestataire,
- ❖ Du nombre de token(s) à l'unité ou par pack souscrit par le Client pour les « change management » nécessaires au démarrage du projet Client ou en vie de solution.

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans les documents « Annexes techniques au Descriptif de Service Managed Applications – Services Natifs Hyperscalers » accessible ici :

- Azure : <https://cloud.orange-business.com/technical-appendix-managed-applications-on-azure/>,
- AWS : <https://cloud.orange-business.com/technical-appendix-managed-applications-on-aws/>,
- GCP : <https://cloud.orange-business.com/annexe-technique-managed-applications-pour-gcp/>.

applicables aux Services Natifs Hyperscalers, lesquelles pourront faire l'objet de mises à jour régulières par le Prestataire.

7.7 Big Data managé

Big Data managé est un service qui permet aux clients de générer de la valeur à partir de leurs données métiers (telles que la maintenance prédictive, la détection des fraudes ou la connaissance client).

Ce service est composé de différentes solutions qui sont toutes gérées par le Prestataire (Infrastructure et Composants Big Data). Ces solutions fonctionnent avec la même philosophie : Collecter les données en mode batch ou streaming, Stocker les données, traiter les données et visualiser les données.

Le service comprend tout ou partie des éléments suivants :

- Un portail d'administration sécurisé fourni avec la plateforme Big Data,
- Un tenant dédié pour ingérer, stocker, traiter et visualiser les données Client,
- Une solution de surveillance et d'alerte 24h/24 et 7j/7,
- Installation, configuration et maintien en conditions opérationnelles des composants des solutions Big Data par le Prestataire,
- La mise en œuvre par le Prestataire des prestations suivantes sur devis :
 - Audit d'évaluation des données et de l'architecture
 - Migration d'une solution Big Data existante vers l'environnement du Prestataire,
 - Développement des cas d'usage métier avec les partenaires internes du Prestataire,

Les solutions logicielles Big Data suivantes sont proposées et gérées par le Prestataire. Chaque solution peut être sélectionnée en fonction des besoins du client :

- Big Data avec Cloudera CDP / CDF,
- Services natifs Big Data avec Flexible Engine,
- Services natifs Big Data avec Google GCP,
- Services natifs Big Data avec Azure,
- Services natifs Big Data avec AWS,
- Solution Log As A Service.

Pour les Services Big Data proposés en libre-service par le Prestataire de Cloud public (Flexible Engine, GCP, Azure et AWS), le Prestataire gère pour le Client l'infrastructure et les composants Big Data.

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – Big Data managé » accessible ici <https://cloud.orange-business.com/annexe-technique-big-data-manage/> applicables au service Big Data managé, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.8 Computer Vision managé

Le service de Computer Vision managé est un service du Prestataire qui exploite des techniques d'Intelligence Artificielle pour permettre au Client d'extraire les données issues de ses équipements vidéo à travers des alertes et un tableau de bord dédié.

Le Service fourni au Client comprend :

- Une solution logicielle de type Computer Vision
- Une solution d'hébergement de type Cloud exploitée et administrée par le Prestataire.
- Un service global d'exploitation de la solution logicielle et matérielle géré par le Prestataire.
- Des prestations d'accompagnement à la mise en œuvre du service pour les clients
-

Le service se compose des éléments suivants :

- Le développement ou le paramétrage de l'application Computer Vision :
 - Mise en œuvre jeu de données/dataset et outils (entraînement, labellisation, augmentation...),
 - Conception de l'Intelligence Artificielle (framework interne / inférence, apprentissage des moteurs, traitement d'image, vidéo, audio...),
 - Génération et extraction des statistiques, construction de tableaux de bord,
 - Installation de l'application et de sa configuration sur la base de la documentation fournie par le partenaire.
- Exploitation, administration, 24 x 7 de la solution en environnement de production et hors production
- Service de supervision, et maintien du déploiement de la solution
- Tierce Maintenance Applicative avec accompagnement au cycle de vie des données
- La gestion des incidents, des changements, des événements et de la sécurité.

Le Prestataire peut prendre en charge la gestion complète des applications du Client sur devis en option.

Le Prestataire intègre selon les besoins et cas d'usages clients la compétence applicative de son réseau d'ISV (Independent Software Vendor) ou des experts du Prestataire.

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – Computer Vision managé » accessible ici <https://cloud.orange-business.com/annexe-technique-computer-vision-manage/> applicables au service Computer Vision managé, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.9 RDS managé

Le Service RDS (Remote Desktop Service) managé est un Service du Prestataire qui permet la du RDS du Client, hébergé sur une infrastructure Cloud Public IaaS de la liste ci-dessous.

- ✓ Du Prestataire :
 - Cloud Avenue
 - Flexible Engine
- ✓ Des Partenaires :
 - AWS,
 - Microsoft Azure,
 - Google Cloud

Le « RDS managé » s'appuie sur des services complémentaires :

- Un AD managé,
- Des certificats SSL de serveur autosignés ou délivrés par une autorité de certification reconnue

Les prérequis pour cette offre :

- Souscrire à une offre d'infrastructure IaaS pour l'hébergement du service RDS selon les recommandations du Prestataire.
- Souscrire à l'offre OS managé pour les VMs où sont hébergés les composants
- Souscrire à l'offre AD managé pour l'AD nécessaire à la livraison du service RDS

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – RDS managé » accessible ici <https://cloud.orange-business.com/annexe-technique-remote-desktop-service-manage/> applicables au service RDS managé, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.10 AD managé

Dans le cadre de ce Service, nous assurons la gestion de votre AD DS hébergé sur une infrastructure Cloud Public IaaS de la liste ci-dessous.

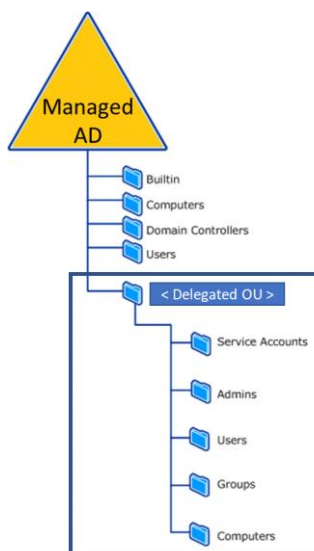
Le Prestataire:

- Cloud Avenue

Flexible Engine Service AS DS managé permet au Client d'administrer les comptes utilisateurs et ordinateurs via une délégation sur une ou plusieurs 'OU'.

Le Prestataire est en charge des activités suivantes :

- Choix des composants nécessaires pour votre Managed AD
- La mise en place du service
- La maintenance
- La configuration et la surveillance des services AD
- La gestion des GPO (hors OU déléguée) et la gestion des services AD
- La sauvegarde standard de l'AD



Les prérequis sont les suivants :

- Souscrire à l'offre OS Managé pour les VMs où est hébergée votre AD,
- Infrastructure composée d'un minimum de 2 VMs selon les recommandations de Microsoft,
- AD mono-forêt, mono-domaine,
- Respecter les bonnes pratiques et les recommandations du Prestataire.

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – AD managé » accessible ici <https://cloud.orange-business.com/annexe-technique-active-directory-manage/> applicables au service AD managé, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.11 Sécurité managée

Le service de Sécurité managée est un service du Prestataire qui permet la gestion des composants de sécurité suivants :

- La gestion de Firewall(s) tiers hébergé(s) sur une infrastructure du Prestataire ou Hyperscalers (Azure, AWS, GCP)
- La gestion de Firewall(s) natif hébergé(s) sur l'infrastructure du Prestataire,
- La gestion de Load Balancer(s) tiers hébergé(s) sur une infrastructure du Prestataire ou Hyperscalers (Azure, AWS, GCP)

La tarification des composants de sécurité du Service de Sécurité managé ainsi que la description technique des composants de sécurité font partie intégrante de la liasse contractuelle de l'offre Managed Applications.

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – Sécurité managée » accessible ici <https://cloud.orange-business.com/annexe-technique-securite-managee/> applicables au service Sécurité managée, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.12 Citrix Workspace managé

Le Service Citrix Workspace managé est un service du Prestataire qui permet la gestion du Citrix Workspace du Client hébergé sur l'infrastructure Cloud Public du Prestataire.

Le Service Citrix Workspace managé inclut :

- La production de l'infrastructure Client.
- Le déploiement des Bureaux Virtuels des Utilisateurs en Option si le Client le souscrit.
- Le maintien en conditions opérationnelles du socle d'infrastructures et des Bureaux Virtuels.
- Le support, qui couvre le traitement des signalisations et des demandes de changement.
- En option, le pilotage de la relation client par un Responsable Service Client (RSC) ou un Service Delivery Manager (SDM).

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – Citrix Workspace managé » accessible ici <https://cloud.orange-business.com/annexe-technique-citrix-workspace-manage/> applicables au service Citrix Workspace managé, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.13 Flexible Workspace User Experience [AVD] – Azure Virtual Desktop

Le Service Flexible Workspace User Experience [AVD] managé est un service du Prestataire qui permet la production et la gestion du Workspace du Client hébergé sur l'infrastructure Cloud Azure.

Le Service Flexible Workspace User Experience [AVD] inclut :

Pour la phase intégration :

- La production standard de l'infrastructure Client et le déploiement des bureaux virtuels.
- Des options de personnalisation de la plateforme AVD payantes.

Pour la vie de solution :

- Un accès au service Azure Virtual Desktop,
- Un abonnement mensuel pour la consommation échue à l'usage des services souscrits sur le cloud Azure,
- L'accès à un service d'assistance technique à la demande et au catalogue de services associés,
- Un abonnement mensuel au service d'assistance technique à la demande.

En option,

La possibilité de souscrire à des services additionnels sur la Marketplace Azure, y compris les licences Microsoft.

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – Service Flexible Workspace User Experience [AVD] managé » accessible ici <https://cloud.orange-business.com/annexe-technique-flexible-workspace-user-experience-avd-azure-virtual-desktop/> applicables au service Flexible Workspace User Experience [AVD] managé, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.14 Exchange managé

Le Service Exchange managé est un Service du Prestataire qui consiste à gérer le service de messagerie Exchange du Tenant du Client. Le Service est souscrit sur l'ensemble des utilisateurs actifs sur le Tenant du client. Le Client peut augmenter sa quantité d'utilisateurs en cours contrat. Les utilisateurs additionnels sont facturés sur la même périodicité que la commande initiale avec régularisation au prorata temporis.

Le Prestataire accompagne le Client durant toute la vie du Contrat : de la mise en place du Service jusqu'au support.

Le Prestataire propose 2 modèles :

- Messagerie Exchange sur Cloud Avenue
- Exchange Online – Office 365

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – Exchange managé » accessible ici <https://cloud.orange-business.com/annexe-technique-exchange-manage/> applicables au service Exchange managé, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

7.15 Management de serveurs hébergés en colocation

Ce Service correspond à un service complémentaire de gestion de serveurs physiques, hébergés dans une zone de colocation, fourni par le Prestataire. Il permet au Client d'exploiter ses serveurs physiques existants, tout en bénéficiant des services managés Managed Applications, dans un modèle hybride.

Ce service exclut explicitement la gestion des baies de colocation, de l'infrastructure réseau ou de la solution de sauvegarde elle-même.

Par l'acceptation du Bon de Commande, le Client accepte expressément les conditions définies dans le document « Annexe technique au Descriptif de Service Managed Applications – Management de serveurs hébergés en colocation » accessible ici [Annexe Management de serveurs hébergé en colocation](#) applicables au service Management de serveurs hébergés en colocation, laquelle pourra faire l'objet de mises à jour régulières par le Prestataire.

8 Accès au Service

8.1 Prérequis

Le Service « Managed Applications » se décline de façon suivante :

- Il peut s'appuyer sur un service de IaaS, auquel le Client doit également souscrire. Dans ce cadre, le Tenant souscrit par le Client est un Tenant Managé, administré par le Prestataire.
- Il peut s'appuyer sur un service de IaaS, auquel le Client doit également souscrire. Dans ce cadre, le Tenant souscrit par le Client est un Tenant Co-Managé, administré par le Prestataire selon un RACI défini entre le Client et le Prestataire.
- Il peut s'appuyer sur l'offre **MultiCloud Ready (MCR)** du Prestataire, une offre qui permet la revente de Services cloud de nos partenaires Hyperscalers AWS, GCP et Azure. **Notre modèle de support sur les services cloud de l'offre Managed Applications sont complémentaires avec notre offre de support sur l'infrastructure.**

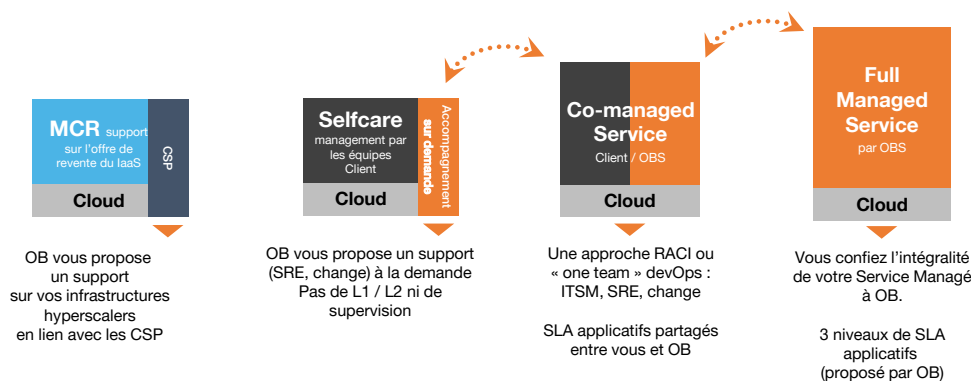


Figure 5 – Modèle de management Managed Applications avec MCR

7.1.1 Tenant Managé

Dans le cas d'un Tenant Managé administré par le Prestataire, le Client devra souscrire le niveau de support IaaS de son choix et sera facturé du support IaaS dans la cadre du contrat correspondant. Pour le IaaS Flexible Engine et Cloud Avenue, le niveau de support à souscrire est « Tenant Managé ».

Le service IaaS correspondant au Tenant Managé sera facturé dès sa mise en service, sans attendre la recette des services managés Managed Applications.

Pour un Tenant Managé, certaines fonctionnalités du IaaS ne seront pas accessibles au Client :

- ⇒ La Gestion des changements, des incidents, des configurations des règles de sécurité réseaux, des évolutions des composants cloud, sont opérés par le Service « Managed Applications »

- ⇒ La console et le reporting IaaS dans le Cloud Store sont accessibles en lecture seule.
- ⇒ Le Client délègue au Prestataire la responsabilité de certaines tâches de gestion de son Tenant Managé, selon les dispositions du présent document.

7.1.2 Les niveaux de management Tenant managé

Le Client a la possibilité de souscrire différents niveaux de management pour un même projet, cependant :

- Pour les niveaux de management Base de Données managée et Middleware managé, le Client doit souscrire obligatoirement au niveau de management OS managé.
- Pour le niveau de management Application Managée, le Client doit obligatoirement souscrire au niveau de management OS managé, et aux niveaux de management Base de Données managée et Middleware managé, Service managés pour Kubernetes®, dès lors que le fonctionnement de son application nécessite la mise en œuvre des composants correspondants.

Chaque serveur virtuel (VM) du Tenant Managé pourra avoir l'un des 4 niveaux de management possibles (OS managé, DB managé, Middleware managé, Application managée). Le niveau de management s'applique à l'ensemble du serveur, il n'est pas possible de faire cohabiter des logiciels à différents niveaux de management sur un même serveur.

Chaque cluster Kubernetes® du Tenant Managé pourra avoir l'un des 2 niveaux de management possibles (Service managé pour Kubernetes®, Application managée). Le niveau de management s'applique à l'ensemble du cluster, il n'est pas possible de faire cohabiter des logiciels à différents niveaux de management sur un même cluster.

Le Client choisit au moment de la commande un niveau de support parmi les trois disponibles (Initial, Standard, Premium) qui s'applique par types d'environnements du Service souscrit par le Client.

Plusieurs types d'environnements sont disponibles :

- Environnement de Production
- Environnement de Pré-Production
- Environnement d'Intégration
- Environnement de Développement

Si le Client souhaite bénéficier de différents niveaux de support, il doit le préciser lors de la souscription par environnement. Le déploiement pourra se faire sur un ou plusieurs Tenants Managés en fonction du SoW partagé entre le Client et le Prestataire.

8.2 Portail – Espace Client Cloud Store



Figure 6 - Le portail Cloud Store

L'Espace Client Cloud Store permet de gérer l'ensemble des contrats souscrits par le Client, notamment grâce aux sections suivantes :

- **Contrat** : cette section permet de visualiser les informations générales des contrats et des commandes réalisées.
- **Tableau de bord** : cette section permet d'accéder à la console IaaS en SSO (Single Sign On), en lecture seule.
- **Services** : permet de commander des services en ligne ou d'accéder aux différents outils de demande de changement.
- **Factures** : permet de consulter l'ensemble des factures en ligne et de visualiser les informations permettant de contacter le service facturation.
- **Documents** : espace de gestion documentaire permettant au Client de consulter les documents organisés en cinq répertoires : Guides utilisateurs, Rapports de performance, Tableaux de bord techniques, Comptes-rendus de réunions, Divers.
- **Support** : permet d'accéder à l'outil de déclaration d'incident et de visualiser les informations permettant de contacter le centre de support Client.
- **Utilisateurs** : permet la gestion des droits utilisateurs sur les différentes offres et sur l'espace Client.

9 Engagements de qualité de service

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

9.1 Engagements de qualité de service

- Le Prestataire s'engage sur la qualité de service dans les conditions définies dans la présente et/ou dans la Proposition Technique et Financière relative au Service concerné.
- Les engagements de qualité de service peuvent donner lieu au paiement d'une pénalité dont le montant est spécifié dans la présente et/ou dans la Proposition Technique et Financière. Cette pénalité constitue une indemnité forfaitaire couvrant le préjudice subi, excluant toute réclamation en dommages-intérêts pour le même motif.

9.2 Crédits de service

- En cas de non-respect relevé par le Client et confirmé par le Prestataire des engagements visés dans la présente et/ou dans la Proposition Technique et Financière, et sur demande expresse du Client, le Prestataire s'engage à émettre, pour le mois concerné, des Crédits de Service conformément aux dispositions dudit document.
- Pour obtenir ces Crédits de Service, le Client devra adresser au Prestataire le formulaire de demande de Crédit de Service dûment rempli au contact mentionné sur la facture, en indiquant en objet « Réclamation SLA » suivi du nom du Service concerné, dans un délai maximum de 30 jours suivant le mois concerné par le non-respect de l'engagement de qualité de service. A défaut, le Client ne pourra prétendre à aucun Crédit de Service.
- Le formulaire de demande est mis à disposition du Client par le Prestataire sur une Interface Utilisateur, ou à défaut est disponible auprès de ses contacts habituels.
- La demande doit détailler la nature du problème, les dates et heures de début et de fin de chaque incident observé, ainsi que les identifiants des ressources impactées. Seuls les incidents ayant fait l'objet d'un ticket pourront être pris en considération. Elle doit également inclure toutes traces système documentant l'incident, pour chaque période concernée. Les traces contenant des données sensibles ou confidentielles doivent avoir été préalablement anonymisées en masquant les informations qui ne peuvent pas être divulguées.
- Dans un délai de 30 jours suivant la demande du Client, le Prestataire confirmera par écrit au Client le montant des Crédits de Service qui lui seront accordés, le cas échéant, au titre de cette demande. En cas de désaccord sur le niveau de service atteint, les enregistrements et informations du Prestataire prévaudront.
- Les Crédits de Service attribués au Client donneront lieu à une remise sur une ou plusieurs de ses factures ultérieure(s) concernant le Service pour lequel les engagements de qualité de service n'ont pas été respectés, à l'exclusion de tout autre mode de remboursement.

9.3 Plages de services

Les « Plages de services » désignent les différentes plages horaires sur lesquelles les services surveillance, exploitation et administration sont rendus :

Plages de services		
Plage de surveillance	24h/24 – 7j/7	La surveillance comprend la mise en place d'outils standards de monitoring technique permettant de détecter tout dysfonctionnement anormal d'un service, de la couche hardware jusqu'au comportement des middlewares. Le monitoring applicatif ne fait pas partie du service standard et sa mise en place doit être traitée en avant-vente.
Plage d'exploitation	Environnement Production : P1 et P2 : 24h/24 – 7j/7 P3 : 09h-18h jours ouvrés Environnement hors production : P1, P2, P3 : 09h-18h jours ouvrés	L'exploitation prend en charge la gestion des incidents techniques remontés par les Clients et le système de monitoring. L'exploitation prend également en charge des changements liés directement à des incidents.

Plage d'administration	09h-18h jours ouvrés	Cette plage correspond à la plage de gestion des demandes de changements : passage des ordres de travaux, des intégrations applicatives (MEP= Mise En Production) non liées à des incidents. Tout changement devant être effectué hors de la plage d'administration fait d'objet d'une proposition commerciale.
------------------------	----------------------	---

Jours ouvrés : Lundi à Vendredi en France métropolitaine, horaires de la France Métropolitaine

9.4 Conditions d'application

8.4.1. Les engagements de qualité de service décrits dans l'article « Engagements et pénalités » des présentes s'appliquent conformément aux Conditions Générales.

8.4.2. Pour la pleine application des engagements de qualité de service du Prestataire et conformément aux conditions générales, le Client s'engage à collaborer avec le Prestataire :

- a) en lui communiquant toute information susceptible de permettre ou de faciliter la délivrance du ou des Services et/ou Produits.
- b) en mettant à sa disposition, dans des délais raisonnables, les moyens nécessaires à ses interventions.
- c) en conformant son environnement aux prérequis nécessaires aux interventions du Prestataire.

8.4.2. Les engagements de qualité de service s'appliquent uniquement aux Unités de Services managés figurant dans le champ d'application des travaux du Prestataire et pour lesquels les prérequis pour les services managés sont fournis et validés par celui-ci. Ils incluent la connectivité, le monitoring, la supervision, le Patching, le backup et les procédures de restauration selon le modèle de responsabilité de Build convenu (cf. Managed Applications - Service Description Technique).

8.4.3. Les engagements de qualité de service s'appliquent aux Unités de Service de production. Ces engagements de qualité de service s'appliquent également aux Unités de Service hors production conformément aux plages d'exploitation et plages d'administration définies ci-dessus. Les pénalités ne s'appliquent pas aux Unités de Service hors production.

8.4.4. Pour les Unités de Services co-managées,

- a) La Garantie de Taux de Disponibilité et la Garantie de Temps de Rétablissement ne s'appliquent pas pendant les périodes où le client est impliqué dans la cause de l'incident.
- b) La Garantie de Temps de Rétablissement ne s'applique pas pour les Unités de Services pour lesquelles le Prestataire n'est pas en charge du support Niveau 3.
- c) Le temps d'investigation et de réparation passé par le Prestataire pour un incident généré par une mauvaise configuration ou action du Client sera facturé au temps passé sous forme de Tokens de Change.
- d) En cas de responsabilité partagée, le Client et le Prestataire doivent collaborer pour atteindre le Temps de Rétablissement Garanti. Ils partageront la charge de temps passé à 50% chacun.

8.4.5 Pour les Unités de Services construites selon le modèle "Backend Build – Class 2" (cf. Managed Applications – Description de Service Technique), le Client étant en charge de la construction de l'infrastructure, de la configuration des outils natifs de l'Hyperscaler et de la fourniture des procédures de rétablissement du service, l'étendue des responsabilités du Prestataire se limite à la détection, à l'investigation et aux possibilités de rétablissement fournis par cette configuration d'outillage et ces procédures.

8.4.6. Les engagements de qualité de service ne s'appliquent pas pendant les périodes où le IaaS du Client n'est pas disponible. Au titre de ces périodes ainsi exclues le Client peut, le cas échéant, faire valoir ses droits à crédits de service auprès de son fournisseur de IaaS, selon ses conditions contractuelles.

8.4.7. Pour le service Managed Computer Vision, les engagements de qualité de service ne s'appliquent pas au cas où la cause de l'incident est un bug dans le logiciel tiers d'intelligence artificielle utilisé pour entraînement et inférence.

8.4.8. Les restrictions propres à chaque Fonctionnalité sont précisées, le cas échéant, dans l'article « Engagements et pénalités ».

8.4.9. En aucun cas les Crédits de Service accordés au Client ne pourront dépasser 15% du montant mensuel récurrent facturé au Client pour le Service concerné pour le mois concerné.

8.4.10. Un même Incident ne pourra donner lieu à des Crédits de Service à la fois au titre de la GTD et de la GTR. Au cas où les deux seraient applicables, le Crédit de Service le plus élevé des deux sera accordé au Client.

8.4.11 Pour le Service Managé pour Kubernetes®, les engagements de qualité de service s'appliquent uniquement aux clusters comportant au moins trois nœuds de contrôle, avec une version de Kubernetes® validée et supportée par le Prestataire. La mesure de la disponibilité sera effectuée par intervalles de 5 minutes consécutifs. Ce SLA n'inclut pas les temps d'arrêt programmés, la perte de connectivité, ni les défaillances des nœuds Kubernetes® ou des pods s'exécutant sur ces nœuds.

9.5 Engagements et pénalités

9.5.1 Services de portails

Pour les services de portails : Le Prestataire s'engage à assurer un Taux de Disponibilité de chaque portail à hauteur de 99,5%. La liste des portails concernés est la suivante :

- Portail Espace Client Cloud Store (ECCS).

9.5.2 Garantie de Taux de Disponibilité (GTD)

9.5.2.1 Engagement

Le Prestataire s'engage à assurer le Taux de Disponibilité défini dans le tableau ci-dessous pour chaque Fonction Managée, selon le niveau de support souscrit :

Garantie de Temps de Disponibilité			
Plage de service = Plage de surveillance			
Niveau de support	Initial	Standard	Premium
Par Fonction Managée	98,5%	99,5%	
Par Service Managé pour Kubernetes® (disponibilité API Kubernetes®)	98,5%	99,5%	

9.5.2.2 Calcul de l'écart

L'« Ecart de Disponibilité » est calculé comme suit pour le mois concerné pour chaque Fonction Managée impactée par une Interruption :

$$\text{Ecart de Disponibilité} = \text{Garantie de Taux de Disponibilité} - \text{Taux de Disponibilité mesuré}$$

9.5.2.3 Pénalités

Si au cours d'un mois, le Taux de Disponibilité d'une Fonction Managée ou des services portails est strictement inférieur au Taux de Disponibilité Garanti, le Prestataire s'engage à émettre un Crédit de Service égal au pourcentage indiqué dans le tableau ci-dessous du montant mensuel récurrent hors taxe facturé au Client pour la Fonction Managée affectée pour le mois considéré, en fonction de l'Ecart de Disponibilité constaté :

Ecart de Disponibilité	Pourcentage de Crédit de Service
Plus de 0 à 1 point de pourcentage	2%
Plus de 1 à 2 points de pourcentage	5%
Plus de 2 points de pourcentage	10%

9.5.3 Garantie de Temps de Rétablissement (GTR)

9.5.3.1 Engagement

Le Prestataire s'engage à assurer chaque mois 95% des Temps de Rétablissement suivants, selon le niveau de support souscrit, le temps étant comptabilisé uniquement sur les périodes couvertes

Garantie de Temps de Rétablissement				
Plage de service = Plage d'exploitation				
Niveau de support		Initial	Standard	Premium
Priorité de l'incident	Priorité 1	1 jour HO*	8h	4h
	Priorité 2	Pas de SLA	24h	8h
	Priorité 3	Pas de SLA	48h	32h

	Priorité 4	pas d'engagement
--	------------	------------------

* Jours/heures Ouvrés : 9h à 18h CET

9.5.3.2 Calcul de l'écart

L'« Ecart de Rétablissement » est :

- Si le nombre total d'Incidents résolus dans le mois est supérieur ou égal à 5 :

$$\text{Ecart de Rétablissement} = \frac{\text{Nombre d'Incidents résolus hors délais}}{\text{Nombre total d'Incidents résolus dans le mois}}$$

- Si le nombre total d'Incidents résolus dans le mois est inférieur à 5 :

$$\text{Ecart de Rétablissement} = \frac{\text{Nombre d'Incidents résolus hors délais}}{5}$$

9.5.3.3 Pénalités

Si l'Ecart de Rétablissement est supérieur à 5% pour un mois donné, le Prestataire s'engage à un Crédit de Service égal au pourcentage indiqué dans le tableau ci-dessous du montant mensuel récurrent hors taxe facturé au Client pour l'ensemble des Unités de Services de production du Service, pour le mois considéré, en fonction de l'Ecart de Rétablissement constaté :

Ecart de Rétablissement	Pourcentage de Crédit de Service
Plus de 5% à 25%	2%
Plus de 25% à 50%	5%
Plus de 50%	10%

9.5.4 Garantie de Temps de Changement (GTC)

9.5.4.1 Engagement

Le Prestataire s'engage assurer les Temps de Changement suivants pour chaque Unité de Service de production souscrite, selon le niveau de support souscrit, le temps étant comptabilisé uniquement sur les périodes couvertes :

Garantie de Temps de Changement			
Plage de service = Plage d'administration			
Niveau de support	Initial	Standard	Premium
Réalisation d'un changement simple	Pas de SLA	24h	8h
Réalisation d'un changement simple accéléré	Pas de SLA	12h	4h
Réalisation d'un changement complexe	Pas de SLA	72h	48h
Réalisation d'un changement complexe accéléré	Pas de SLA	36h	24h
Réponse à une demande de cotation pour un changement non standard	Pas de SLA	5 JO	3 JO

NB : Les demandes de change pour les Services Natifs > 1 Token sont des demandes de change complexe.

9.5.4.2 Pénalités

Si un changement est réalisé dans un délai plus long que celui indiqué dans le tableau de Garantie de Temps de Changement pour le niveau de support concerné, le Prestataire s'engage à émettre un Crédit de Service égal à 50% du prix du changement correspondant au tarif « paiement à l'usage » du Token.

10 Conditions d'utilisation

10.1 Durée minimale

La durée minimale du Service est d'un an. La durée d'engagement du Client est précisée dans la Commande.

Un Tenant Managé peut accueillir plusieurs Projets du Client, dont les dates de fin d'engagement peuvent être distinctes.

10.2 Prix

La tarification du service est différente selon qu'il s'agit :

- Des unités de service commandées à la signature du contrat ;
- Des unités de service supplémentaires commandées par la suite ;
- Des prestations de sauvegarde et de restauration ;
- Des Tokens à la demande ;
- Des prestations de support.

Le Service est soumis à des frais d'accès au Service et à un minimum de facturation mensuel dont les montants sont indiqués dans la Fiche Tarifaire, auxquels s'ajoute le prix des Unités de Service et prestations souscrites (prestations de restauration, sauvegarde, support et Tokens).

Les prestations de sauvegarde et de restauration, les prestations de support et les Tokens à la demande sont facturés au prix de la fiche tarifaire en vigueur au moment de leur souscription.

Les tarifs sont définis par Région.

Lorsque les tarifs dépendent de la durée d'engagement du Client, la durée d'engagement prise en compte pour la souscription de services complémentaires est égale, sauf disposition contraire, à la durée d'engagement restante arrondie le cas échéant à la durée immédiatement supérieure prévue dans la Fiche Tarifaire.

Les tarifs du Service Managed Applications n'incluent pas le prix du Tenant Managé que le Client doit souscrire par ailleurs auprès du fournisseur de IaaS selon les tarifs en vigueur.

10.3 Révision des prix

10.3.1 Révision des prix SYNTEC

Les prix unités des Services (hors prestations : de sauvegarde et de restauration, prestations de support et tokens à la demande) sont révisibles chaque année à la date anniversaire du Contrat par application de la formule suivante :

$$P1 = P0 \frac{S1}{S0}$$

Où P1 = prix révisé

P0 = prix d'origine

S0 = dernier indice SYNTEC publié à la date de conclusion du Contrat ou à la date de la précédente révision

S1 = dernier indice SYNTEC publié à la date de révision.

Les prix et indices de base sont les prix et indices à la date de la première facturation mensuelle.

Les Prestations facturées en début de période de révision le sont sur la base des derniers indices connus. Une facturation complémentaire sera établie dès que les indices en cause seront publiés et la facturation ultérieure sera ajustée en conséquence.

En cas de disparition de l'indice SYNTEC, le comité ad hoc devra, sous un mois, retenir un nouvel indice et en cas d'impossibilité et pour quelque cause que ce soit, compétence expresse est attribuée à Monsieur le Président du Tribunal de Commerce de Paris, pour définir un indice qui s'intégrera dans la formule de révision. Cet indice devra être choisi de telle sorte qu'il soit le plus proche possible de l'indice disparu.

10.3.2 Révision des prix spécifique

Dans le cas où les équipements utilisés par le Prestataire pour administrer les unités de services du Client requièrent une zone d'hébergement physique, alors les prix de ces unités de service sont révisibles chaque année à la date anniversaire du Contrat – en sus de la révision liée à l'indice SYNTEC – par application de la formule suivante :

$$P = P-1 * [\frac{2}{3} (S/S-1) + \frac{1}{3} (T/T-1)]$$

Dans laquelle :

- P est le montant révisé, P-1 est le montant en vigueur avant la date de révision,

- S est le dernier indice du coût de la construction publié par l'INSEE à la date de la révision (ICC base 100 au 4ème trimestre 1953, trimestriel), et S-1 est l'indice du coût de la construction publié douze mois avant la date de révision,

- T est l'indice mensuel du coût de l'électricité moyenne tension publié par l'INSEE (électricité vendue aux entreprises ayant souscrit un contrat pour capacité > 36 kVA) à la date de révision et T-1, l'indice mensuel du coût de l'électricité moyenne tension publié douze mois avant la date de révision

Dans tous les cas, le Prestataire appliquera à minima les conditions tarifaires liées aux évolutions des coûts de l'énergie publiés par l'INSEE.

En cas de disparition ou de non-publication d'un de ces indices, il sera remplacé par un indice d'effet comparable.

10.3.3 Révision des prix des licences et équipements managés

Le Prestataire se réserve le droit d'augmenter ses prix dans le cas où le fournisseur tiers des licences ou équipements managés nécessaires à la bonne fourniture du Service augmenterait sa liste de prix publique publiée et/ou aurait notifié le Prestataire d'une augmentation de prix pour ces équipements et licences. Cette augmentation sera limitée aux augmentations notifiées par le fournisseur tiers pour les équipements et les licences.

Le Prestataire informera le Client de toute augmentation de prix imposée par le fournisseur tiers et de l'impact sur les prix.

10.4 Revenu Minimum Garanti (MRG)

Le contrat initial stipule le Revenu Global attendu par le Prestataire au titre de la phase de RUN.

En contrepartie des moyens et de l'organisation spécifique mis en place par le Prestataire pour l'exécution du Contrat, le Client s'engage, pendant la phase de RUN, à maintenir un Minimum de Revenu Garanti (MRG global) correspondant à 80% du montant de Revenu Global prévu au Contrat.

A la fin de chaque année de RUN, les Parties s'assureront que le MRG annuel est atteint. Le MRG annuel est calculé en divisant le montant du MRG global par le nombre d'années de RUN prévu au Contrat.

Si le montant effectivement facturé par le Prestataire au titre d'une année de RUN est inférieur au montant du MRG annuel, la différence entre le montant du MRG annuel et le Montant facturé durant l'année (ci-après le « Différentiel ») sera due par le Client au Prestataire et facturée dans les trente (30) jours de la notification écrite par le Prestataire de l'existence de ce Différentiel. En cas de dépassement d'un MRG annuel, ce dépassement viendra participer à l'atteinte du MRG annuel de l'année suivante.

En cas de variation à la hausse du périmètre des prestations (nouvelle(s) prestation(s) et/ou modification des prestations prévues) ayant un impact de prix de plus de 15% par rapport au Revenu Global prévu au Contrat, le MRG Global sera revu à la hausse proportionnellement au pourcentage de variation de prix constaté par les Parties au titre de cette modification de périmètre.

10.5 Prix des prestations de Support

Les prestations de support sont définies au contrat du Client de la manière suivante :

- un niveau de support : Initial, Standard ou Premium
- un type de support : Off-Shore ou full France
- et un nombre de tickets, qui est déterminé spécifiquement pour chaque Client.

Un bilan sera réalisé de manière régulière afin de comptabiliser le nombre de tickets effectivement consommés par le Client sur la période écoulée. Tout dépassement du nombre de tickets défini au contrat sera facturé au prix unitaire du ticket indiqué dans la fiche Tarifaire Managed Applications.

10.6 Prix des Tickets d'incidents

La facturation des tickets d'incidents (Service Desk) est liée à l'environnement du Client. Le Client peut souscrire aux 4 types d'environnements suivants dans le cadre de l'offre Managed Applications en fonction de ses besoins :

- Environnement de Production
- Environnement de Préproduction
- Environnement d'Intégration
- Environnement de Développement

Par ailleurs, il existe quatre niveaux de support auxquels correspondent quatre tarifs de tickets d'incidents :

- Ticket SLA Premium
- Ticket SLA Standard
- Ticket SLA Initial
- Ticket pas de SLA

Dans le cas où un client a souscrit à plusieurs environnements avec des niveaux de support différents selon ses environnements, le tarif des tickets d'incidents sera celui du ticket le plus élevé.

10.7 Prix des unités de service supplémentaires

Le prix des unités de service commandées à la signature du contrat est fixé pendant la période d'engagement du client.

Toute commande d'unités de service différentes des unités de services commandées à la signature du Contrat sera facturée au prix des unités de service de la fiche tarifaire en vigueur au moment de cette commande.

10.8 Facturation Build et Run

10.8.1 Facturation du Build

La facturation du Client par le Prestataire pendant la phase de Build peut se faire de 2 façons suivantes :

1. Pour des petits projets, le Prestataire procède à la facturation de 30% du montant du Build à réception du bon de commande dûment signé par le Client et à la facturation de 70% restant dès la fin de la phase de Build.
2. Pour des projets Client dont le Build s'étalent sur plusieurs mois, le commercial du Client définit des lots / échéances de paiement avec son chef de projet en accord avec le Client. Le Prestataire procède à la facturation du montant du Build par lots en respectant les échéances.

10.8.2 Facturation du run

La facturation du run démarre à la livraison :

- Soit de la totalité du Build,
- Soit d'un lot défini en cas de facturation par lots.

10.9 Réversibilité sortante

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 de Temps de Rétablissement » ne s'applique pas.
- Le Prestataire s'engage notamment à la fourniture des informations techniques sur l'architecture du service (PQSC, SRF), sous réserve que l'information demandée ne soit pas assimilée à un savoir-faire protégé par le Prestataire.
- Le Prestataire se donne le droit de retirer tout produit ou licence contracté par lui-même auprès d'un fournisseur tiers, afin de rester dans les droits légaux d'utilisation de licence de chaque éditeur.
- Dans le cas où une assistance complémentaire à celle définie ci-dessus et un pilotage seraient demandés au Prestataire, le Client recevra :
- Une proposition d'assistance rémunérée précisant les conditions de son assistance, le personnel dédié aux opérations de réversibilité, les éventuelles installations matérielles et physiques nécessaires.
- Les conditions financières applicables à la mise en place de cette assistance complémentaire.

Le Client s'engage de son côté à fournir toute l'assistance technique, humaine et le cas échéant financière requise pour mener à bien la migration du service. Les conditions du Contrat continueront à s'appliquer jusqu'au terme de la Période de Réversibilité.

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

10.10 Conditions spécifiques d'utilisation du Service

Afin de permettre une utilisation des Services conformes au descriptif et au SLA prévus au Contrat, sauf disposition contraire figurant dans le Descriptif de Service, le Client s'engage à maintenir ses équipements interfacés sans passer par un système de routage et filtrage avec les Equipements utilisés par le Prestataire pour fournir les Services ou les Equipements du Client managés par le Prestataire dans le cadre des Services, dans les conditions de mise à jour et de sécurité demandés par les fabricants de ces Equipements ou des éditeurs des logiciels composant ces Equipements.

En conséquence, le Prestataire ne saurait en aucune façon, être responsable en cas de compromission d'un ou plusieurs de ces Equipements visés ci-dessus, rendue possible par l'obsolescence du/de ces Equipement(s) ou l'absence de mise à jour du niveau de sécurité du/des Equipement(s) du fait du Client.

Le Prestataire se réserve le droit de facturer au Client tout ou partie de toute intervention du Prestataire qui s'avèrerait nécessaire pour remettre en état de fonctionnement lesdits Equipements compromis.

Sauf accord contraire entre les Parties, dans le cas où le Client gère ses équipements et/ou disposition contraire contenu dans les Descriptifs de Service, le Client est responsable de la politique de sécurité de ses réseaux, machines virtuelles, Logiciels et Données, et de toute procédure concernant la réaction aux failles de sécurité et aux attaques.

Le Prestataire se réserve le droit d'appliquer toutes les mesures qu'il estimera nécessaires à la sécurité du service : hardening, versions/patching, configuration, scripts et agents, fonctions de sécurité, Anti-virus, montée de version en cas d'obsolescence.

En conséquence, le Prestataire ne saurait en aucune façon être responsable en cas de compromission d'un ou plusieurs Equipements, rendue possible par l'obsolescence du/de ces Equipement(s) ou l'absence de mise à jour du niveau de sécurité du/des Equipement(s) ou par la désactivation du fait du Client.

11 Définitions

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

BaaS (Backup as a Service) désigne le service de sauvegarde en ligne, également appelé sauvegarde dans le Cloud. C'est une méthode de sauvegarde hors site dans laquelle les données d'une entreprise (fichiers, dossiers, applications, ...) sont régulièrement sauvegardées par un fournisseur de services dans un stockage Cloud distant sécurisé via une connexion réseau.

CCE Cloud Conteneur Engine désigne un service de containers du cloud Flexible Engine du Prestataire

CFT (Cross File Transfer) désigne le protocole de transfert de fichiers.

Changement Standard désigne un changement à l'initiative du Client ou du Prestataire, implémenté par une procédure validée par le Prestataire et accepté par le Client. Tout changement considéré comme Standard est défini dans la liste des changements standards du catalogue de changement, accessible à travers l'Espace Client Cloud Store. Le prix des changements standards est défini et connu du Client.

Changement Standard Simple désigne un changement Standard d'un Token à l'initiative du Client ou du Prestataire, qui nécessite peu d'efforts, ou ayant un impact sur un nombre limité de services, implémenté par une procédure validée par le Prestataire et accepté par le Client. Tout changement considéré comme Simple est défini dans la liste des changements standards du catalogue de changement accessible à travers l'Espace Client Cloud Store.

Changement Standard Complexe désigne un changement Standard de plus d'un Token à l'initiative du Client ou du Prestataire, qui nécessite un effort important, ou ayant un impact sur plusieurs services, implémenté par une procédure validée par le Prestataire et accepté par le Client. Tout changement considéré comme Standard Complexe est défini dans la liste des changements standards du catalogue de changement accessible à travers l'Espace Client Cloud Store.

Changement Non Standard désigne un changement hors catalogue standard et sur devis à l'initiative du Client, ou du Prestataire, implémenté par une procédure validée par le Prestataire et accepté par le Client.

Changement Accéléré désigne un changement de service Standard Simple ou Complexe nécessitant une mise en production accélérée de la demande du Client. Le prix du changement accéléré est le double du changement demandé par le Client. Le Client a la possibilité de demander un traitement accéléré d'un changement Standard simple ou Complexe de manière exceptionnelle à raison d'un maximum de 6 par an.

Crédit de Service désigne une compensation financière accordée au Client au titre des pénalités pour non tenue des engagements de qualité de service.

Classe de transition désigne le périmètre de responsabilité Client et du Prestataire pour la transition de l'environnement du Client vers le Cloud. Un inventaire des ressources à manager est effectué par le Prestataire pour choisir la classe de transition la plus adaptée au contexte du Client.

Classe 2 désigne le périmètre du Prestataire dans lequel le Prestataire assure le support du service managé des ressources en fonction du guide de procédure fourni par le client (Change), et dans lequel sa responsable est engagée pour la récupération des données en cas de panne. Ce périmètre comprend l'intégration des alarmes du CSP concernés aux systèmes dorsaux du Prestataire, la saisie des guides de procédures fournis par le client dans le référentiel de connaissances des opérations du Prestataire, et la préparation des opérations.

Classe 4 désigne le périmètre du Prestataire dans lequel le Prestataire configure et maintient les outils de gestion du CSP pour gérer le service ainsi que l'intégration dans les systèmes backend du Prestataire.

Classe 5 désigne le périmètre du Prestataire dans lequel le Prestataire configure l'Infrastructure as Code (IaC) requise pour les ressources et pour les outils du CSP de gestion concerné ainsi que l'intégration dans le système backend du Prestataire.

Cluster désigne un groupe de nœuds délivrant une capacité de calculs/traitement distribués

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

Contrôleur de Domaine désigne l'ensemble des serveurs qui exécutent le rôle Active Directory Domain Services

Computer Vision désigne le service qui exploite des techniques d'Intelligence Artificielle pour permettre au Client d'extraire les données issues de ses équipements vidéo à travers des alertes et un tableau de bord dédié.

Environnement désigne un espace privé virtuel de ressources sur le IaaS 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.

Environnement d'Administration Client désigne l'environnement dans lequel est hébergé le Service du Client (build et déploiement). Les actions de création, destruction, modification, listage des ressources et des Fonctionnalités associées sont limitées au Prestataire.

Environnement Client désigne l'environnement dans lequel sont déployés les conteneurs du Client. Les actions de création, destruction, modification, listage des ressources et des fonctionnalités associées sont attribuées au Prestataire et au Client.

Fonction Managée désigne les Unités de Service ou ensembles d'Unités de Services de production définis ci-dessous:

- L'ensemble des Unités de Service Managé pour Kubernetes® prises collectivement.
- L'ensemble des Unités de Service Flexible Workspace User Expérience AVD Managé prises collectivement.
- L'ensemble des Unités de Service Exchange Managé prises collectivement.
- L'ensemble des Unités de Service Citrix Workspace Managé prises collectivement.
- L'ensemble des Unités de Service RDS Managé prises collectivement.
- L'ensemble des Unités de Service AD Managé prises collectivement.
- L'ensemble des Unités de Service Computer Vision prises collectivement.
- L'ensemble des Unités de Service Big Data Managé prises collectivement.
- Chaque Unité de Service Application Managée prise séparément.
- L'ensemble des Unités de Service Sauvegarde Managée, prises collectivement.
- L'ensemble des Unités de Service Service Natif Hyperscaler, prises collectivement.
- L'ensemble des Unités de Service SAP prises collectivement.
- L'ensemble des Unités de Service Log As A Service prises collectivement. L'ensemble des Unités de Service Middleware Managé, prises collectivement.
- L'ensemble des Unités de Service Base de Données Managée, prises collectivement.
- L'ensemble des Unités de Service OS Managé, prises collectivement

Full France : les équipes qui assurent le service et/ou les prestations de support sont basées en France.

Garantie de Taux de Disponibilité (ou **GTD**) désigne le Taux de Disponibilité sur lequel le Prestataire s'engage, pour une Fonction Managée donnée, en fonction du niveau de support souscrit.

Garantie de Temps de Changement (ou **GTC**) désigne le Temps de Changement sur lequel le Prestataire s'engage en cas de demande de changement, pour les changements décrits au catalogue, en environnement de production et validés par le Prestataire, en fonction du niveau de support souscrit.

Garantie de Temps de Rétablissement (ou **GTR**) désigne le Temps de Rétablissement sur lequel le Prestataire s'engage en cas d'Incident en environnement de production, en fonction du niveau de support souscrit.

Incident désigne un événement non planifié qui provoque une Interruption ou une dégradation du Service ou de la Fonctionnalité concernée. Un Incident est tracé par un ticket de Priorité P1, P2 ou P3.

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. Une Interruption est tracée par un ticket de Priorité P1.

Git désigne un logiciel de gestion de versions de code.

Heures Ouvrées désigne la plage horaire comprise entre 9h et 18h du lundi au vendredi sauf jours fériés français.

IaC désigne l'infrastructure en tant que code.

IaaS désigne le service d'infrastructure cloud, incluant le cas échéant les services complémentaires (tels que PaaS, CaaS, DBaaS, etc.) associés, souscrit par le Client aux fins d'héberger son Tenant Managé.

Jours Ouvrés désigne les jours du lundi au vendredi hors jours fériés français.

Kubernetes® désigne un logiciel open source permettant le déploiement et la gestion de conteneurs. **Kubernetes®** est une marque déposée de la Fondation Linux. Voir kubernetes.io.

Log As A Service désigne le service rendu à partir des composants de la suite ECE (Elastic Cloud Enterprise).

Middleware désigne un composant Logiciel nécessaire au fonctionnement d'une application, en dehors des systèmes d'exploitation (OS) et des bases de données.

MRC (Monthly Recurring Charge) désigne les frais récurrents mensuels.

Nœud désigne une machine virtuelle incluse dans un Cluster.

Nœud esclave désigne un nœud de données qui est chargé de répondre aux demandes de lecture et d'écriture des clients du système de fichiers ainsi que d'effectuer la création, la suppression et la réplication de blocs sur instruction du nœud maître et du suivi des tâches qui est un nœud du cluster

Off-Shore : les équipes qui assurent le service et/ou les prestations de support sont basées pour partie hors de France.

Onboarding désigne la prestation d'installation, de déploiement et la prestation de prise en main fournie par un expert du Prestataire.

Opérations de Maintenance programmées : désigne toutes les opérations de Maintenance ou de Patch Management réalisées à fréquence régulière et anticipées sur les infrastructures matérielles ou logicielles entrant dans le Périmètre.

OTC (One Time Charge) désigne les frais d'initialisation et correspond à une charge unique

Passerelle Axway Vision désigne une passerelle de transfert de fichiers sécurisant l'échange de fichiers entre réseaux différents.

Périmètre : désigne les Éléments de Configuration et les Prestations à effectuer par le Prestataire conformément aux stipulations du Contrat. A la demande du Client, ce Périmètre pourra être modifié soit par avenant soit en phase de RUN.

Plate-forme désigne un sous-ensemble d'un Tenant Managé hébergeant un ou plusieurs Logiciels, qui peuvent inclure plusieurs Clusters.

Priorité désigne les niveaux suivants utilisés pour classer les tickets d'Incident :

- **Priorité 1 (ou P1)** : perte complète des Services pour plusieurs Utilisateurs, ou Incident ayant un impact critique sur les activités du Client.
- **Priorité 2 (ou P2)** : Services dégradés. Les Utilisateurs peuvent accéder aux Services mais connaissent des difficultés ou subissent des délais significatifs.
- **Priorité 3 (ou P3)** : Services fournis avec des délais ou des difficultés mineures. L'activité du Client n'est pas significativement entravée.
- **Priorité 4 (ou P4)** : ces tickets ne correspondent pas à des Incidents et ne donnent lieu à aucun engagement de qualité de service de la part du Prestataire.

Projet désigne le projet pour lequel le Client souscrit au Service et référencé dans la Commande.

PQSC (Plan Qualité Service Client) désigne l'ensemble des dispositions prises par le Prestataire pour produire les prestations sur le périmètre du Contrat, dans le respect des dispositions du Contrat. Le PQSC précise les conditions d'exécution des prestations visibles par les deux Parties et non des informations dont la maîtrise et la visibilité n'appartiennent qu'au Prestataire. Aucune disposition du PQSC ne saurait remettre en cause les dispositions du Contrat.

RACI désigne la définition des responsabilités entre le Client et le Prestataire. R = Responsable, A = Autorité redevable, C= Consulté, I = Informé.

Région désigne une zone géographique dans laquelle le Service est disponible sur une ou plusieurs Zone(s) de Disponibilité.

SRE (Site Reliability Engineer) désigne une prestation d'expertise du Prestataire pour des conseils et assistance technique en continu sur l'environnement du Client.

DRE (Data Reliability Engineer) désigne une prestation d'expertise du Prestataire dans l'environnement Big Data managé.

Service désigne le service « Managed Applications » fourni pour un Tenant Managé. Chaque Tenant Managé Client constitue un Service distinct.

Services Natifs Hyperscalers désigne les services fournis par les IaaS hyperscalers que sont Amazon Web Services (AWS), Microsoft Azure (Azure), et Google Cloud Platform (GCP).

Service Pack désigne un ensemble de mises à jour, corrections et/ou améliorations de Logiciels livré sous forme d'un package unique qui peut être installé en une seule opération.

SIEM (Security Information and Event Management) désigne la gestion des informations et des événements liés à la sécurité.

Socle Managé désigne le socle technique fourni par le Prestataire permettant d'installer et d'opérer les Unités de Service souscrites.

SoW : Scope of Work en anglais, désigne l'étendue des travaux ou le périmètre des travaux pendant la phase d'avant-vente en fonction des besoins du client

SRF (Service Request Form) désigne le formulaire à remplir pour décrire les caractéristiques techniques des services à délivrer.

SSO (Single Sign-On) désigne une méthode permettant à un Utilisateur d'accéder à plusieurs fonctionnalités en ne procédant qu'à une seule authentification.

Taux de Disponibilité désigne, sauf disposition contraire pour une Fonctionnalité spécifique, le taux défini par la formule suivante :

$$\text{Taux de Disponibilité} = \frac{(t_{\text{mois}} - t_{\text{interruption}} + t_{\text{exclusion}})}{t_{\text{mois}}}$$

où :

- t_{mois} est le temps pendant lequel la Fonctionnalité concernée est souscrite pour le mois considéré
- $t_{\text{interruption}}$ est le temps d'Interruption de la Fonctionnalité concernée pendant le mois considéré
- $t_{\text{exclusion}}$ est le temps d'Interruption de la Fonctionnalité concernée pendant le mois considéré qui est exclu des engagements de qualité de service du Prestataire au titre des dispositions contractuelles, telles que les interventions programmées.

Les Taux de Disponibilité sont calculés sur la base du mois calendaire. Le Taux de Disponibilité d'une Fonction Managée est la moyenne des Taux de Disponibilité des Unités de Services qui la constituent.

Taux de Disponibilité désigne, sauf disposition contraire pour une Fonctionnalité spécifique, le taux défini par la formule suivante :

$$\text{Taux de Disponibilité} = \frac{(t_{\text{mois}} - t_{\text{interruption}} + t_{\text{exclusion}})}{t_{\text{mois}}}$$

où :

- t_{mois} est le temps pendant lequel la Fonctionnalité concernée est souscrite pour le mois considéré
- $t_{\text{interruption}}$ est le temps d'Interruption de la Fonctionnalité concernée pendant le mois considéré
- $t_{\text{exclusion}}$ est le temps d'Interruption de la Fonctionnalité concernée pendant le mois considéré qui est exclu des engagements de qualité de service du Prestataire au titre des dispositions contractuelles, telles que les interventions programmées.

Les Taux de Disponibilité sont calculés sur la base du mois calendaire. Le Taux de Disponibilité d'une Fonction Managée est la moyenne des Taux de Disponibilité des Unités de Services qui la constituent.

Temps de Changement désigne le temps qui s'écoule entre la demande de changement et sa fin de mise en œuvre notifiée par le Prestataire, dont on retire les périodes pendant lesquelles les engagements du Prestataire ne s'appliquent pas.

Temps de Rétablissement désigne le temps qui s'écoule entre l'ouverture d'un ticket d'Incident et sa résolution, dont on retire les périodes pendant lesquelles les engagements du Prestataire ne s'appliquent pas.

Tenant désigne un espace privé virtuel de ressources sur le IaaS 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 associées sont limitées à ces seuls Utilisateurs. Pour les IaaS en technologie VMware, le Tenant est également appelé « Organisation ».

Tenant Managé désigne le Tenant dans lequel est hébergé le Service du Client. Les actions de création, destruction, modification, listage des ressources et des Fonctionnalités associées sont limitées au Prestataire.

Token désigne l'unité d'œuvre utilisée pour exprimer les prix applicables aux changements demandés par le Client, tels qu'indiqués dans la Fiche Tarifaire.

URL (Uniform Resource Locator) désigne un point d'accès sous forme d'adresse web.

Unité de Service désigne un sous-ensemble du service fourni sur une Machine Virtuelle (VM) ou sur un serveur physique dans le cas des Fonctionnalités d'OS managé, de Database managée ou de Middleware managé, et sur un(e) ou plusieurs VM ou serveur(s) physique(s) dans le cas de la Fonctionnalité d'Application managée. Le Client souscrit aux Unités de Service au moyen du Bon de Commande.

Workload désigne un environnement applicatif du Client qui doit être exécuté sur une ressource Cloud du Prestataire

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 Disponibilités de chaque Région sont listées dans le Descriptif de Service.

12 Annexes

- 1.1 **OS managé** : [Annexe-technique-OS-Manage.pdf](#)
- 1.2 **Base de données managée** : <https://cloud.orange-business.com/annexe-technique-base-de-donnees-managee/>
- 1.3 **Middleware managé** : <https://cloud.orange-business.com/annexe-technique-middleware-manage/>
- 1.4 **Service Managé pour Kubernetes®** : [Annexe-technique-Service-Manage-pour-Kubernetes®.pdf](#)
- 1.5 **Application managée** : <https://cloud.orange-business.com/annexe-technique-application-managee/>
- 1.6 **Services Natifs Hyperscalers managés** :
 - 1.6.1 **Azure** : <https://cloud.orange-business.com/technical-appendix-managed-applications-on-azure/>
 - 1.6.2 **AWS** : <https://cloud.orange-business.com/technical-appendix-managed-applications-on-aws/>
 - 1.6.3 **GCP** : <https://cloud.orange-business.com/annexe-technique-managed-applications-pour-gcp/>
- 1.7 **Big Data managé** : <https://cloud.orange-business.com/annexe-technique-big-data-manage/>
- 1.8 **Computer Vision managé** : <https://cloud.orange-business.com/annexe-technique-computer-vision-manage/>
- 1.9 **AD managé** : <https://cloud.orange-business.com/annexe-technique-active-directory-manage/>
- 1.10 **RDS managé** : <https://cloud.orange-business.com/annexe-technique-remote-desktop-service-manage/>
- 1.11 **Sécurité managée** : <https://cloud.orange-business.com/annexe-technique-securite-managee/>
- 1.12 **Citrix Workspace managé** : <https://cloud.orange-business.com/annexe-technique-citrix-workspace-manage/>

- 1.13 Flexible Workspace User Experience – Azure Virtual Desktop [AVD] :** <https://cloud.orange-business.com/annexe-technique-flexible-workspace-user-experience-avd-azure-virtual-desktop/>
- 1.14 Exchange managé :** <https://cloud.orange-business.com/annexe-technique-exchange-manage/>
- 1.15 Management de serveurs hébergés en colocation :** [Management de serveurs hébergés en colocation](#)