



Annexe technique au Descriptif de Service Managed Applications Service Managé pour Kubernetes®

Table des matières

1	SERVICE MANAGE POUR KUBERNETES®	2
1.1	<i>Description</i>	2
1.1.1	Prérequis	2
1.1.2	Maintien en conditions opérationnelles	3
1.1.3	Collecte, stockage, visualisation de logs et métriques	4
1.1.4	Managed DevOps Toolkit	4
1.2	<i>Conditions de prix</i>	6
1.3	<i>Catalogue de Change Service Managé pour Kubernetes®</i>	6
1.4	<i>Demandes hors catalogue</i>	7
2	GLOSSAIRE	7

1 Service Managé pour Kubernetes®

1.1 Description

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).

Le service se compose de tout ou partie des éléments suivants :

- Le déploiement de clusters Kubernetes® à la demande à partir de configurations fournies par Le Client.
- La supervision 24 x 7 et le maintien en conditions opérationnelles des clusters Kubernetes® déployés.
- La notification et les interventions sur incidents pour remise en état ou reconstruction à partir du référentiel en cas de dysfonctionnements des clusters Kubernetes®.
- La restauration des clusters Kubernetes® à partir d'un référentiel sauvegardé
- La gestion des changements sur les clusters Kubernetes®.
- Des outils managés de collecte, stockage, visualisation de logs et de métriques d'infrastructure.
- Un outil managé de visualisation qui permet au Client d'observer des métriques et les alertes configurées par Le Prestataire.
- L'accès en option à des outils DevOps (Managed DevOps Toolkit) pour permettre au Client de déployer des applications sur le(s) cluster(s) gérés par Le Prestataire.

Lors du déploiement d'un cluster Kubernetes® par Le Prestataire pour Le Client, l'accès aux ressources et aux fonctionnalités se fait de la manière suivante :

- Le Client reçoit un fichier d'admin kubeconfig contenant le point de terminaison du serveur API du cluster (IP ou nom de domaine) ainsi que les détails d'authentification (nom d'utilisateur, mot de passe ou jeton). Le Client pourra créer d'autres comptes directement au sein du cluster ou obtenir de l'aide Du Prestataire via une demande de Change.
- Utilisation de *kubectl* : En utilisant ce kubeconfig, Le Client peut se connecter directement au serveur API Kubernetes® depuis sa machine locale ou son pipeline CI/CD, sans passer par d'autres outils. Le Client peut exécuter des commandes comme *kubectl get pods* ou *kubectl apply -f myapp.yaml*.
- En parallèle, Le Client peut accéder aux différents services de Managed DevOps Toolkit par des URLs dédiées qui seront fournies suite à la phase d'onboarding. Ces URL et IP sont publiques.

Cette approche garantit une expérience utilisateur fluide et directe pour Le Client dans l'utilisation des services proposés.

1.1.1 Prérequis

Le service Managé pour Kubernetes® nécessite obligatoirement une gouvernance avec Le Prestataire.

L'architecture d'interconnexion réseau et sécurité doit être définie préalablement au déploiement du Service, lors de la phase d'avant-vente ou d'une mission de consulting ; ces services doivent être

opérationnels en prérequis au déploiement du Service Managé pour Kubernetes®. Ils ne font pas partie du Service Managé pour Kubernetes®.

De plus, pour chaque cluster managé par Le Prestataire, un control plane composé de 1 à 3 nœuds master sera déployé. La seule configuration du control plane qui permet de bénéficier de la totalité des SLA du service est celle où les clusters sont orchestrés par 3 nœuds master. La taille de ces nœuds est typiquement de 4 vCPU, 4 Go de RAM et 90 Go de stockage, sauf si, lors de la phase d'avant-vente ou d'une mission de consulting, Le Prestataire constate qu'une configuration différente doit ou peut être envisagée en fonction de la taille du cluster à gérer ou des cas d'usage client à adresser.

Le service Managed DevOps Toolkit est optionnel pour le Service Managé pour Kubernetes®. Pour activer cette option, et avant l'installation et le déploiement, Le Client doit fournir à Le Prestataire la liste des utilisateurs autorisés, incluant leurs identifiants de connexion et adresses email.

Les activités suivantes restent de la responsabilité Du Client :

- Fourniture de la spécification des caractéristiques de(s) cluster(s) Kubernetes®.
- La gestion des conteneurs et des applications.

1.1.2 Maintien en conditions opérationnelles

Dans le cadre de l'offre, Le Prestataire prend en charge le maintien en condition opérationnelle des systèmes d'exploitation et de la distribution Kubernetes®.

Les mises à jour du système d'exploitation sont effectuées tous les trois mois, incluant les correctifs de sécurité.

Le Prestataire utilise une distribution Rancher Kubernetes® Engine 2 et suit un système de versionnement avec le format « *M.m.P* » (où *M* représente la version majeure, *m* la version mineure et *P* le patch de sécurité). Voici les détails concernant les mises à jour et le support des versions :

- Mises à Jour Majeures (*M*) : Les mises à jour majeures doivent être coordonnées avec Le Client, car elles affectent des composants essentiels tels que le contrôleur d'ingress, et certains manifests pourraient devenir obsolètes.
- Mises à Jour Mineures (*m*) : Des mises à jour mineures sont généralement publiées tous les trois mois. Les mises à niveau peuvent nécessiter un temps d'arrêt planifié, soit parce que les nœuds master pourraient être temporairement indisponibles, soit pour garantir la compatibilité des opérateurs utilisés par Le Client.
- Correctifs Obligatoires (*P*) : Environ tous les mois, des correctifs obligatoires sont appliqués sans nécessiter la planification d'une fenêtre de maintenance.
- Support des Versions : À tout moment durant le cycle de vie du service, Le Prestataire supporte la version actuelle ainsi que les deux versions mineures précédentes (c'est-à-dire version *M.m.P*, *M.m-1.P*, *M.m-2.P*).

Phase	Activité
Kubernetes® Implémentation	<ul style="list-style-type: none">▪ Création des cluster(s) Kubernetes® avec la distribution Rancher Kubernetes® Engine 2 (RKE2)▪ Installation et configuration du stockage▪ Configuration du réseau, des services d'accès▪ Installation et configuration du service de supervision
Kubernetes® Opérations	<ul style="list-style-type: none">▪ Administration et maintenance des services cœur Kubernetes®▪ Mises à jour mineures et majeures▪ Gestion de la sécurité (mise à jour, contrôle des accès)▪ Supervision du service 24/7▪ Gestion des événements▪ Gestion des logs

1.1.3 Collecte, stockage, visualisation de logs et métriques

Le Service fournit pour chaque cluster Kubernetes® managé, un service de collecte des métriques et des logs. Ces services de collecte sont installés, configurés et managés par Le Prestataire. A l'installation, ces services sont configurés pour collecter les métriques nécessaires Au Prestataire pour rendre le Service Managé pour Kubernetes®.

Sur demande et sur devis, Le Prestataire peut fournir au Client un moyen de définir des endpoints supplémentaires pour la collecte des métriques applicatives. Ces endpoints doivent être déployés dans le cluster Kubernetes® pour être pris en compte.

Le Service fournit un outil managé de visualisation des métriques (Grafana). L'outil de visualisation est configuré par défaut avec un ensemble de tableau de bord. Sur demande et sur devis, Le Prestataire peut fournir au Client, des tableaux de bord Grafana et des alertes Prometheus personnalisés.

Les périodes de rétentions des logs et des métriques sont définies lors de l'On-boarding. Par la suite, Le Client peut demander un changement pour les modifier.

Phase	Activités
Logs/Métriques Implémentation	<ul style="list-style-type: none">▪ Installation et configuration des services de collectes▪ Installation et configuration des services de traitement et stockage long-terme▪ Configuration des rétentions▪ Installation et configuration du service de visualisation▪ Ajout des tableaux de bord par défaut
Logs/Métriques Opération	<ul style="list-style-type: none">▪ Administration des services▪ Mises à jour mineures ou majeures▪ Gestion de la sécurité (mise à jour, contrôle des accès)▪ Supervision du service 24/7▪ Gestion des évènements▪ Gestion des logs

1.1.4 Managed DevOps Toolkit

Le service Managed DevOps Toolkit fournit un outillage pour les opérations orientées DevOps permettant le co-management par Le Prestataire et Le Client sur Cloud Avenue.

Cet outillage comprend un ensemble d'outils managés as-a-service pour construire, tester et déployer les applications dans le(s) cluster(s) Kubernetes® managé(s) par Le Prestataire

- La gestion de dépôts des software artifacts
- La gestion de versions décentralisée GIT
- L'automatisation des builds/tests/déploiements
- Un service managé de gestion des secrets

Une session d'On-boarding est fournie à l'initialisation du Service : celle-ci comprend la création de l'environnement Managed DevOps Toolkit et la fourniture des URL d'accès au Service, la déclaration des utilisateurs nommés dans le système de ticketing du Support ainsi que l'accompagnement Du Client par un expert sur la configuration et l'utilisation de celui-ci.

Les activités suivantes restent de la responsabilité Du Client :

- Gestion de son code applicatif.
- Pilotage du Déploiement des conteneurs intégrant les mises à jour applicatives.

Le Service fournit un dépôt de code afin de permettre au Client de gérer par lui-même son code. Le Client est libre d'organiser son code comme il le souhaite. Ce service est dédié Au Client, mais l'équipe Du Prestataire est administrateur de ce service et l'utilise aussi pour des opérations sur le(s) Environnement(s) Client.

Le Service fournit un outil de Continuous Integration (CI) afin de permettre au Client de créer ses applications conteneurisées (build, tests et packaging). Les travaux sont organisés sous forme de pipeline pour automatiser les tâches. L'outil de CI permet d'effectuer les tâches habituelles de Build (compilation, exécution de scripts), de tests (unitaires, fonctionnels, d'intégration, de charge) et de packaging (Docker). Le Client est libre de configurer les pipelines souhaités.

Le Service fournit une Docker Registry afin de permettre au Client de stocker l'ensemble de ses images applicatives. Ce service est dédié au Client.

Le Service fournit un gestionnaire de secrets basé sur la technologie Hashicorp Vault, permettant au Client de gérer lui-même ses secrets applicatifs. L'équipe Du Prestataire dispose d'un droit administrateur sur le gestionnaire de secrets.

Les outils mis à disposition par le service Managed DevOps Toolkit nécessitent l'utilisation d'une fonctionnalité de Multi-Factor Authentication (MFA) qui sera configurée par le Prestataire.

L'ensemble des outils de l'option Managed DevOps Toolkit est sauvegardé et mis à jour régulièrement, ce qui pourrait entraîner des pertes d'accès temporaires et négligeables aux instances.

Les activités suivantes restent de la responsabilité Du Client :

- Mise à jour du code applicatif et stockage dans le dépôt de code
- Pilotage de la chaîne de Build
- Déploiement des applications sur les clusters Kubernetes®
- Mise à jour des secrets applicatifs
- L'ajout des annotations dans les manifestes applicatifs pour permettre la récupération des secrets

Le Service de Reporting Managed Application ne s'applique pas à Managed DevOps Toolkit

Le Service d'Antivirus Managed Application ne s'applique pas au service Managed DevOps Toolkit qui ne gère pas de serveurs.

Le Service Managed DevOps Toolkit n'inclut pas la consommation IaaS et services de l'Environnement Client que Le Client doit souscrire séparément auprès du fournisseur de IaaS selon ses tarifs en vigueur.

1.2 Conditions de prix

La tarification du Service est composée :

- Des frais d'accès au Service Managé pour Kubernetes® intégrant toutes les tâches mentionnées dans le RACI d'implémentation. Afin d'estimer ces frais, une étude des besoins client est effectuée par Le Prestataire, suite auquel un devis pour les frais d'accès est créé.
- D'un récurrent mensuel de « Run » couvrant les activités liées au maintien en condition opérationnelle du Service Managé pour Kubernetes® indexé sur le nombre d'instances gérés et les options configurées.

Les prix récurrents mensuels de « Run » se trouvent dans le tableau ci-dessous.

Famille	Sous Famille	Unité de service
DevOps Services	Service Managé pour Kubernetes®	Par cluster, jusqu'à 8 nœuds worker managés
DevOps Services	Service Managé pour Kubernetes®	Par nœud worker managé additionnel
DevOps Services	Accès aux services Managed DevOps Toolkit	Par utilisateur ayant accès à au moins un service Managed DevOps Toolkit
DevOps Services	Monitoring endpoint applicatif	Par pack de 5 sondes

Les tarifs du Service n'incluent pas :

- Le prix de l'infrastructure que Le Client doit souscrire par ailleurs auprès du fournisseur de IaaS selon les tarifs en vigueur.
- Les demandes de changement.

1.3 Catalogue de Change Service Managé pour Kubernetes®

Famille	Sous Famille	Token Full France	Token Global	Libellé (complet) Demande de Service
DevOps Services	Service Managé pour Kubernetes®	2	2	Modification des valeurs min max des nodepool
DevOps Services	Service Managé pour Kubernetes®	4	4	Redimensionner les nœuds et redéployer un cluster pour 5 noeuds
DevOps Services	Service Managé pour Kubernetes®	2	2	Création d'une nouvelle nodepool
DevOps Services	Service Managé pour Kubernetes®	3	3	Ajout/modification external label dans Prometheus client
DevOps Services	Service Managé pour Kubernetes®	3	3	Ajout d'un receiver/route dans AlertManager pour les alertes
DevOps Services	Collecte, stockage, visualisation de logs et métriques	Sur devis	Sur devis	Modification de la période de rétention des logs ou des métriques (globale)
DevOps Services	Collecte, stockage, visualisation de logs et métriques	Sur devis	Sur devis	Configuration d'une nouvelle sonde de monitoring d'endpoint applicatif
DevOps Services	Collecte, stockage, visualisation de logs et métriques	Sur devis	Sur devis	Configuration d'un nouveau tableau de bord de monitoring personnalisé
DevOps Services	Sauvegarde et restauration	Sur devis	Sur devis	Restauration du dépôt de code à partir de la version sauvegardée souhaitée

1.4 Demandes hors catalogue

Vous pouvez faire une demande hors catalogue et fournir les détails de votre besoin. Nous organiserons un point téléphonique d'une ½ h avec vous pour s'assurer de la bonne compréhension du besoin. 2 cas se présentent alors :

- Si le besoin fonctionnel est immédiatement qualifiable en tâches simples, moyennes ou complexes tel que défini au catalogue, la demande de Changement est finalement reclassée en demande au catalogue et peut être traitée par les équipes opérationnelles.
- Si le besoin fonctionnel n'est pas immédiatement traduisible en tâches simples ou complexes et que cela nécessitera une étude approfondie avec une durée et un délai de réalisation, une estimation du nombre de Tokens nécessaire pour l'étude sera faite. Cette étude est sans garantie de résultat compte-tenu de la très grande diversité de besoins fonctionnels qui peuvent être exprimés. En cas d'accord, l'étude est réalisée et aboutit à une faisabilité ou pas. En cas de faisabilité, celle-ci s'accompagne d'une évaluation des charges afférentes à sa réalisation. Ces charges seront qualifiées en demandes de changement simple ou complexe selon les critères énoncés plus haut.

2 Glossaire

CI/CD (Continuous Integration / Continuous Deployment) fait référence au service de construction et de déploiement de conteneurs dans le Cloud Du Prestataire de la solution Managed DevOps Toolkit.

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.

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

Endpoint désigne un point d'accès spécifique d'une application ou d'un service web, généralement sous forme d'URL, qui permet d'interagir avec une fonctionnalité particulière du système. Dans le contexte du monitoring d'applications, un endpoint représente une cible précise à surveiller pour évaluer la santé, les performances et la disponibilité d'un service ou d'une partie d'une application. .

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 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. Le Client peut utiliser ce tenant pour exécuter des applications et utiliser des fonctionnalités IaaS hors de la solution Managed DevOps Toolkit.

Git désigne un logiciel de gestion de versions de code.

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.

Kubernetes[®] désigne un logiciel open source permettant le déploiement et la gestion de conteneurs. Kubernetes[®] est une marque déposée de Linux Foundation. Veuillez consulter [Kubernetes.io](https://kubernetes.io).