Business

Annexe technique au Descriptif de Service Managed Applications

Kubernetes et Conteneur managé avec Caascad

Table des matières

1 Service Caascad

Le service Caascad fournit un outillage pour les opérations orienté DevOps permettant le co-management par le Prestataire et le Client sur des clouds multiples. Le service Caascad est proposé en deux versions :

- Caascad Dédié appelé « Caascad » qui comprend tout l'outillage listé ci-dessous et dont les instances sont dédiées par Client
- Caascad Shared qui est une version limitée (voir section Limitations du service Caascad Shared) et partagée entre plusieurs Clients

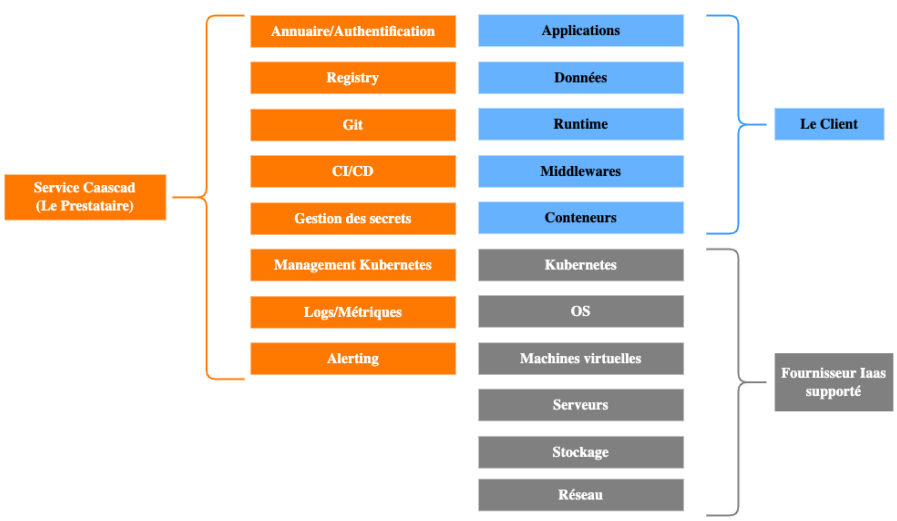
Cet outillage comprend :

- Un service managé d'annuaire et d'authentification centralisée dans lequel le Client peut gérer ses utilisateurs
- Un ensemble d'outils managés as-a-service pour construire, tester et déployer les applications dans le(s) cluster(s) Kubernetes managé(s)
  - La gestion de dépôts d'objets binaires
  - La gestion de versions décentralisée GIT
  - L'automatisation des builds/tests/déploiements
- Un service managé de gestion des secrets
- Des outils managés as-a-service de collecte, stockage, visualisation de logs et de métriques d'infrastructures et applicatives
- Un outil managé as-a-service d'alerting applicatif configurable par le Client
- Un portail résumant l'état du système et facilitant la navigation vers les outils

Cette solution se déploie et utilise les services de l'infrastructure IaaS de service providers compatibles.

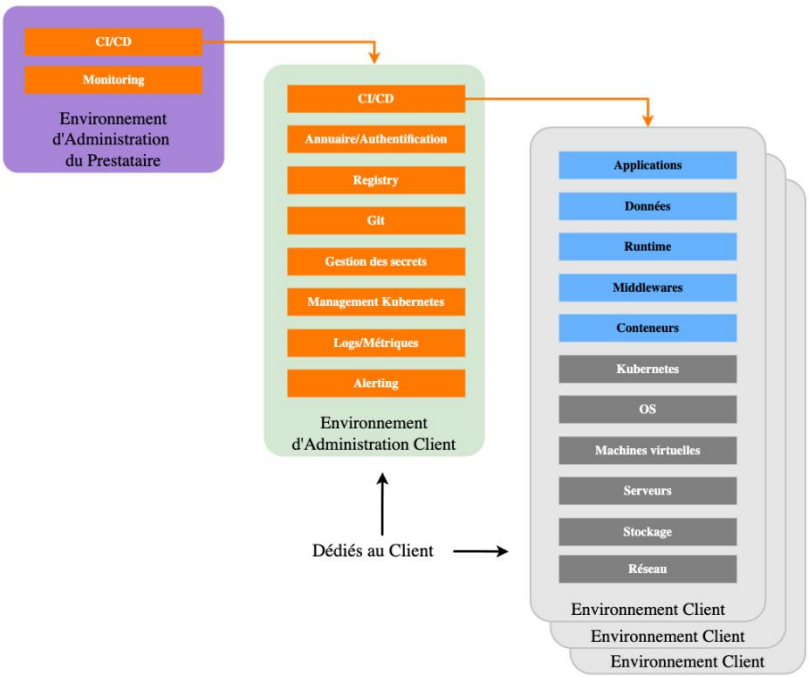
Le schéma suivant représente

- Les applications conteneurisées du Client
- Les services Caascad fourni par le Prestataire
- Les services de Iaas sous-jacent du cloud provider



Partage des responsabilités Client / Prestataire

L'ensemble des outils sont des outils opensource déployés, intégrés et maintenus en conditions opérationnelles de manière industrielle par le Service Caascad. Le schéma suivant décrit le modèle de déploiement du Service :



Les différents environnements

1.1 Accès au Service

1.1.1.1 Prérequis

Les services Caascad, Kubernetes Managé avec Caascad, Conteneur Managé avec Caascad nécessitent obligatoirement une gouvernance avec un Gestionnaire de Services Managés.

Le Service Caascad s'appuie sur un IaaS supporté et ses services, auquel le Client doit souscrire au préalable auprès du cloud provider tiers ou auprès du Prestataire. Les services du cloud provider ne font pas partie du Service. Dans ce cadre, le Client et le Prestataire disposent des niveaux de délégation nécessaires accordés par le client sur son Environnement.

IaaS supportés :

- Flexible Engine du Prestataire, Région Paris
- AWS (Amazon Web Services) de Amazon
- Azure de Microsoft
- La fonctionnalité Cloud Conteneur Engine (CCE), Elastic Kubernetes Services (EKS) ou Azure Kubernetes Services (AKS) est un prérequis au service Caascad
- Les fonctionnalités suivantes du Cloud Provider sont aussi utilisées (non exhaustif) : Virtual Machines, Stockage en volume persistant, réseaux virtuels, NAT Gateway, Gestionnaire de clés d'accès, etc…

Le Service Caascad nécessite en prérequis par cluster Kubernetes dans le tenant Client managé :

- Une machine virtuelle (1 vCPU/ 2GB RAM) avec une adresse IP publique
- Un NAT gateway avec une adresse IP publique

Ces éléments dont le Prestataire pourra déterminer des changements dans le temps pour satisfaire les nouvelles fonctionnalités où l'évolution des exigences de performance ne sont pas inclus dans la tarification de Caascad.

Le Service Caascad déploie des sondes dans les clusters Kubernetes du Client pour les besoins d'administration et de monitoring, ces sondes consomment une fraction de la puissance de calcul des clusters.

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 Caascad. Ils ne font pas partie du service Caascad.

Le service Caascad nécessite entre-autre

- Une connexion Internet pour l'Environnement d'Administration, utilisée pour la mise à jour des logiciels open-source utilisés dans Caascad.

- Une connexion de chaque Environnement Client à l'environnement d'Administration Caascad, utilisée pour l'administration des clusters.
- Un accès des utilisateurs aux URL du service Caascad.

A des fins d'investigation en cas d'incident, le Client autorise le Prestataire à accéder aux logs et métriques stockées dans Caascad.

Au préalable à l'installation et au déploiement, le Client doit fournir au Prestataire :

- La liste des utilisateurs « login » et « email » autorisés à accéder aux Services
- La configuration souhaitée du cluster Kubernetes managé
- Les périodes de rétention de configuration des logs et des métriques.

1.1.1.2 Implantation géographique

Caascad est déployé sur l'infrastructure Cloud choisie par le Client :

- Pour Flexible Engine du Prestataire, sur sa Région Paris disposant de trois Zones de Disponibilité situées à St Denis, Pantin et Aubervilliers
- Pour AWS de Amazon, sur les régions disposant du service EKS et autres services managés nécessaires au bon fonctionnement de Caascad
- Pour Azure de Microsoft, sur les régions disposant du service AKS et autres services managés nécessaires au bon fonctionnement de Caascad

1.1.1.3 URLs et Portail Caascad

Les différents Services de Caascad sont accessibles par des URLs dédiées qui seront fournies suite à la phase d'On-boarding.
L'une d'entre elle est l'URL du portail Caascad proposant une page d'accueil et une navigation vers les autres outils en mode centralisé.
Ce Portail est hébergé sur l'Environnement d'Administration Client.
Ces URL et IP sont publiques.

Une documentation de l'ensemble des services Caascad est disponible à l'adresse https://docs.caascad.com

1.2 Prestations d'accompagnement pour le service Caascad

1.2.1.1 On-boarding

Une session d'On-boarding est fournie à l'initialisation du Service : celle-ci comprend la création de l'Environnement d'Administration Client, la création du cluster Kubernetes 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.

La prestation est renouvelée pour le déploiement de chaque Environnement d'Administration Client.

Une prestation complémentaire peut être commandée par le Client.

1.2.1.2 Cloud Expert Services

Les Cloud Expert Services du Prestataire proposent un catalogue de prestations d'expertise DevOps complémentaire au service Caascad.

1.3 Annuaire d'utilisateurs et authentification centralisée

Le Service fournit un Identity Provider (IdP) afin d'autoriser ou de limiter les accès des utilisateurs au Service. L'ensemble des utilisateurs du Client autorisés au Service est défini au sein de l'Identity Provider (IdP). Celui-ci permet la gestion des utilisateurs, groupes et rôles associés.

Les utilisateurs peuvent changer de mot de passe en self-service. L'ensemble des accès aux outils du Service s'authentifie auprès de l'Identity Provider. L'utilisateur dispose d'une connexion en Single Sign-On pour accéder aux outils Caascad.

Les utilisateurs autorisés peuvent créer / supprimer des comptes et leur attribuer / modifier des droits en self-service.

L'annuaire et le service d'authentification sont hébergés sur l'Environnement d'Administration Client.

1.3.1.1 Description

Phase	Activités
Annuaire / SSO **Implémentation**	▪ Keycloak ○ keycloak.ocb-Projet.caascad.com
Annuaire / SSO **Opération**	▪ Mises à jour mineures et majeures ▪ Gestion de la sécurité (mise à jour, contrôle des accès) ▪ Supervision du service 24/7 ▪ Gestion des évènements ▪ Gestion des logs
Annuaire / SSO **Demandes de changement ***	▪ La création de groupe et rôles pour affiner les droits

* selon la politique de **Erreur ! Source du renvoi introuvable.** du chapitre **Erreur ! Source du renvoi introuvable.**

1.3.1.2 Limitations

Les activités suivantes restent de la responsabilité du Client :

- Définition et changement de mot de passe
- Gestion des utilisateurs en self-service

1.4 Service d'inventaire des clusters Kubernetes

Le Service fournit un outil d'inventaire et de visualisation de l'état des clusters Kubernetes afin de permettre au Client de connaitre les détails des déploiements de conteneurs dans les clusters. Ce service s'appuie sur l'utilitaire Rancher disponible en mode lecture seule pour l'utilisateur. Le composant Rancher porte l'autorisation des utilisateurs sur les clusters Kubernetes, l'authentification est gérée par l'IDP.

1.4.1.1 Description

Phase	Activité
Build / Registry **Implémentation**	▪ Authentification au cluster Kubernetes : Rancher ○ rancher.ocb-Projet.caascad.com
Build / Registry **Opération**	▪ 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

1.4.1.2 Limitations

Les activités suivantes restent de la responsabilité du Client :

- Fourniture de la spécification des caractéristiques des clusters Kubernetes managés et de leur localisation par échange de mail ou dossier constitué
- Gestion de son code applicatif
- Pilotage du Déploiement des conteneurs intégrant les mises à jour applicatives

1.5 Dépôt de code, chaîne de Build et de stockage de conteneurs applicatifs

Le Service fournit un dépôt de code (git) 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 et utilise des ressources de l'Environnement d'Administration Client.
L'équipe du Prestataire est administrateur de ce service et l'utilise aussi pour des opérations sur le(s) Environnement(s) Client. Des dépôts dédiés sont mis à disposition pour la génération et la maintenance des tableaux de bord Grafana et d'alertes Prometheus (cf Collecte, stockage, visualisation de logs et de métriques).

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 qu'il souhaite.

La CI est installée dans l'Environnement d'Administration Client. L'agent de la CI est installé dans l'Environnement Client et les travaux gérés par la CI sont effectués dans l'Environnement Client.

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 et utilise des ressources de l'Environnement d'Administration Client.

L'équipe Du Prestataire dispose d'un droit administrateur sur l'ensemble de ces outils. L'accès s'y fait de manière authentifiée et centralisée à travers le service d'Identity Provider (IdP), en SSO.

1.5.1.1 Description

Phase	Activités
Build / Registry Implémentation	▪ Dépôt de code : Gitea ○ git.ocb-Projet.caascad.com ▪ Build : Concourse ○ ci.ocb-Projet.caascad.com ▪ Registry : Quay ○ docker-registry.ocb-Projet.caascad.com
Build / Registry Opération	▪ 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

1.5.1.2 Limitations

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

1.6 Gestionnaire des secrets applicatifs

Le Service fournit un gestionnaire des secrets (Vault by Hashicorp) permettant au Client de gérer lui-même ses secrets applicatifs.

L'intégration de Vault dans service Caascad propose un modèle d'organisation des secrets génériques afin de couvrir un maximum de cas d'usage :

- accès par toutes les applications sur tous les clusters
- accès par les applications d'un namespace particulier sur tous les clusters
- accès par toutes les applications sur un cluster en particulier
- accès par les applications d'un namespace particulier sur un cluster en particulier

Le déploiement du composant Vault Injector est nécessaire pour les applications qui ne s'intègrent pas nativement avec le gestionnaire de secrets Vault. Ce composant est déployé par l'équipe du Prestataire à la demande du Client dans les environnements de son choix.

L'équipe Du Prestataire dispose d'un droit administrateur sur le gestionnaire de secrets. L'accès s'y fait de manière authentifiée et centralisée à travers le service d'Identity Provider (IdP), en SSO.

1.6.1.1 Description

Phase	Activités
Build / Registry Implémentation	▪ Gestionnaire de secrets : Vault ○ Vault.ocb-Projet.caascad.com
Build / Registry Opération	▪ 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

1.6.1.2 Limitations

Les activités suivantes restent de la responsabilité du Client :

- Mise à jour des secrets applicatifs
- L'ajout des annotations dans les manifestes applicatifs pour permettre la récupération des secrets

1.7 Collecte, stockage, visualisation de logs et métriques

Le Service fournit pour chaque cluster Kubernetes managé, un service de collecte des métriques (basé sur Prometheus) et des logs (basé sur Promtail). Ces services de collecte sont installés, configurés et managés par le Prestataire.

A l'installation, ces services sont configurés pour collecter :

- Toutes les métriques fournies par les composants Kubernetes (node-exporter, cAdvisor)
- Les logs de toutes les applications qui s'exécutent dans le cluster Kubernetes et qui loguent à la sortie standard et/ou d'erreur
- Les logs de tous les composants qui s'exécutent sur les nœuds du cluster Kubernetes

Le Prestataire fournit au Client un moyen de définir des Endpoints supplémentaires pour la collecte des métriques applicatives. Ils sont définis dans le Dépôt de Code et doivent être déployés par le Client dans le cluster Kubernetes pour être pris en compte.

Les services de collecte rapatrient, traitent et stockent les métriques et les logs de chaque cluster Kubernetes managé d'une manière centralisée dans l'Environnement d'Administration Client.

Pour le traitement et stockage des logs, le service de collecte utilise l'outil Loki qui consomme le service S3 du IaaS comme back-end de stockage long-terme.

Pour les métriques, le service de collecte utilise l'outil Thanos qui consomme également le service S3 du IaaS comme back-end de stockage long-terme.

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. Cf Gestion des changements

Le Service fournit un outil managé de visualisation des métriques et des logs (Grafana). L'outil de visualisation est configuré par défaut avec un ensemble de tableau de bord et permet au Client de configurer lui-même ses propres tableaux de bord.

1.7.1.1 Description

Phase	Activités
Logs/Métriques **Implémentation**	▪ 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 ○ grafana.ocb-Projet.caascad.com ▪ Ajout des tableaux de bord par défaut
Logs/Métriques **Opération**	▪ 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
Déploiment **Demande de changement ***	▪ Modification de la période de rétention des métriques (globale) ▪ Modification de la période de rétention des logs (globale)

* selon la politique de **Erreur ! Source du renvoi introuvable.** du chapitre **Erreur ! Source du renvoi introuvable.**

1.7.1.2 Limitations

Les activités suivantes restent de la responsabilité du Client :

- Spécification des endpoints de collecte des métriques applicatives
- Configuration des collecteurs de métriques et de logs au travers du dépôt de code

- Configuration des tableaux de bord Grafana spécifiques aux applications Client au travers du dépôt de code

1.8 Collecte, stockage et visualisation des métriques VM

Pour chaque environnement Client, Le Prestataire fournit au Client un moyen de définir des endpoints pour la collecte des métriques applicatives à partir des machines virtuelles. Les informations sur les exporters applicatifs VMs, sont définis par le Client dans le Dépôt de Code et sont déployés par les pipelines CI/CD automatiques du Prestataire.

Les services de collecte de métriques provenant des machines virtuelles, rapatrient, traitent et stockent les métriques d'une manière centralisée dans l'Environnement d'Administration Client.

Les périodes de rétentions des métriques des VMs sont les mêmes que celles des métriques des clusters managés.

1.8.1.1 Description

Phase	Activités
Métriques **Implémentation**	▪ Installation et configuration des services de collecte ▪ Installation et configuration des services de traitement et stockage long-terme ▪ Installation et configuration des pipelines CI/CD
Métriques **Opération**	▪ Administration des services de collecte ▪ Mises à jour des pipelines ▪ Gestion de la sécurité (mise à jour, contrôle des accès) ▪ Supervision du service 24/7 ▪ Gestion des évènements ▪ Gestion des logs

1.8.1.2 Limitations

Les activités suivantes restent de la responsabilité du Client :

- Installation des exporters OS/applicatifs sur les machines virtuelles
- Spécification des endpoints de collecte des métriques OS/applicatifs
- Ouverture des flux réseaux entre les clusters managés et les machines virtuelles monitorées
- Configuration des tableaux de bord des applications installées sur ces VMs

1.9 Alerting

Le Service fournit un service d'Alerting dans chaque Environnement d'Administration Client.

Ce service d'Alerting permet au Client de :

- Gérer son propre ensemble des règles d'alerting se basant sur les métriques applicatives collectées
- Visualiser les alertes mises en place par le Prestataire par défaut
- Visualiser le statut des alertes en temps réel via l'outil managé Karma

1.9.1.1 Description

Phase	Activités
Alerting **Implémentation**	▪ Installation et configuration du service ▪ Configuration des alertes par défaut ▪ Visualisation des alertes ○ karma.ocb-Projet.caascad.com
Alerting **Opération**	▪ 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

1.9.1.2 Limitations

Les activités suivantes restent de la responsabilité du Client :

- Configuration des alertes applicatives et de l'outil Karma au travers du dépôt de code
- Sauvegarde de la configuration des alertes dans le dépôt de code

1.10 Sauvegarde et restauration

Le dépôt de code GIT est sauvegardé quotidiennement. Ces sauvegardes sont conservées 7 jours, puis une sauvegarde hebdomadaire est conservée pour un mois supplémentaire dans l'Environnement d'Administration Client.

Les éléments de configuration de l'ensemble des outils du Service (tableaux de bord, alertes, …) doivent être stockés par le Client dans le dépôt de code afin d'être sauvegardés et préservés lors des mises à jour et des incidents.

Les sauvegardes du dépôt de code sont exclusivement prévues pour le rétablissement du Service par le Prestataire en cas d'Incident. Le mécanisme de restauration du Service consiste à restaurer le dépôt de code GIT à partir de la sauvegarde et à redéployer les outils et leur configuration à partir du dépôt de code restauré.

Les logs et les métriques sont stockés dans l'Object Storage standard de l'Environnement d'Administration Client. Ils ne sont pas répliqués ni sauvegardés de manière supplémentaire.

1.10.1.1 Description

Phase	Activités
Sauvegarde du Dépôt de Code Git Implémentation	▪ Installation et configuration de la sauvegarde du dépôt de code
Sauvegarde du Dépôt de Code Git Opération	▪ Administration des services de sauvegarde ▪ 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

Phase	Activités
Restauration du Dépôt de Code Git et du service sur incident Implémentation	▪ Restauration du dépôt de code à partir de la version N-1 ▪ Redéploiement des outils du Service à partir du dépôt de code
Restauration du Dépôt de Code Git et du Service sur demande Demande de changement *	▪ Contexte d'une demande de changement de la part du Client ▪ Restauration du dépôt de code à partir de la version sauvegardée souhaitée ▪ Redéploiement des outils du Service à partir du dépôt de code

* selon la politique de **Erreur ! Source du renvoi introuvable.** du chapitre **Erreur ! Source du renvoi introuvable.**

1.10.1.2 Limitations

Les configurations effectuées par le Client sur l'ensemble des outils et collecteurs du Service autrement qu'au travers du dépôt de code ne sont pas sauvegardées. Elles sont donc perdues lors de la remise en service sur incident ou mise à jour du Service.

1.11 Spécificités des mises à jour du service Caascad

Le Prestataire ne fournit pas de service de développement logiciel ni de patch de fonctionnalités sur les logiciels opensource déployés pour le Service. Le Prestataire utilise les évolutions mises à jour par la communauté opensource. Les mises à jour dites "mineures" et les patchs de sécurité seront automatiquement déployés sans notification Client.

Les mises à jour majeures avec interruption de service seront notifiées au Client avec un délai de prévenance de 7 jours avant passage en production. Le Prestataire informera le Client de la fin de support des versions obsolètes.

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

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

1.12 Limitations du service Caascad

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

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

1.13 Limitations du service Caascad Shared

Les fonctionnalités suivantes ne s'appliquent pas à Caascad Shared

- Dépôt de code, chaine de build et stockage des conteneurs
- Collecte, stockage, visualisation des logs et des métriques
- Collecte, stockage, visualisation des métriques VMs
- Alerting
- Sauvegarde et restauration (GIT)
- Gestion des secrets
- Gestion des utilisateurs en self-service dans l'annuaire centralisé

Pour disposer de l'intégralité du service Caascad, le client doit migrer de l'offre "shared" vers l'offre "dédiée". Cette migration est possible à n'importe quel moment à la demande du client.

1.14 Conditions de prix

Les tarifs du service Kubernetes managé avec Caascad n'incluent pas le prix de consommation IaaS, ni des pré-requis IaaS, réseau et sécurité de l'Environnement Client que le Client doit souscrire auprès du fournisseur de l'infrastructure IaaS, réseau et sécurité - dont Le Prestataire - selon ses tarifs en vigueur de la fiche tarifaire.

1.15 Demande de changement

Les demandes de changement sont présentées dans le catalogue de change Managed Applications. Elles sont classées selon 2 niveaux de complexité comme présenté dans le tableau ci-dessous. Pour chaque niveau un nombre de tokens est associé.

Changement Caascad	Critère(s) de qualification	Nombre de Tokens
Simple	▪ Nécessite de 1 tâche pour le traitement	1
Complexe	▪ Nécessite au moins 2 tâches pour le traitement Ou ▪ Nécessite un devis pour le traitement	>= 2

Nous préparons la réalisation d'un changement en concertation avec vous. Une fois la demande est traitée, vous serez prévenu pour valider et clôturer la demande.

1.16 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 Kubernetes managé avec Caascad

Le service Kubernetes managé avec Caascad est un service Du Prestataire qui permet au Client de déléguer la supervision et l'exploitation des clusters Kubernetes utilisés par ses applications et d'utiliser l'outillage as a service Caascad pour l'exploitation des clusters Kubernetes, des conteneurs et des applications conteneurisées en mode DevOps.

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

- Le déploiement de clusters Kubernetes à la demande sur une infrastructure de Conteneur as a Service fournie par le IaaS provider 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 dans Caascad
- L'outillage as a Service Caascad pour l'exploitation des clusters Kubernetes, des conteneurs et des applications conteneurisées.
- La gestion des changements sur les clusters Kubernetes et sur l'outillage Caascad

2.1 Description

Phase	Activité
Kubernetes **Implémentation**	▪ Création des cluster(s) Kubernetes avec la distribution du cloud provider ▪ Installation et configuration du stockage ▪ Configuration du réseau, des services d'accès et des groupes de sécurité associés ▪ Installation et configuration du service de supervision
Kubernetes **Opération**	▪ Administration et maintenance des services Docker et Kubernetes ▪ Mises à jour mineures et majeures ▪ Gestion de la sécurité (mise à jour, contrôle des accès) ▪ Supervision du service 24/7 ▪ Gestion des évènements ▪ Gestion des logs
Kubernetes **Demande de changement ***	▪ Création et destruction d'un cluster Kubernetes managé ▪ Redimensionnement du cluster ou des nœuds sous-jacents

* selon la politique de **Erreur ! Source du renvoi introuvable.** du chapitre **Erreur ! Source du renvoi introuvable.**

2.2 Pre-requis du service

- Le service Caascad pour l'exploitation des clusters Kubernetes, des conteneurs et des applications conteneurisées.

2.3 Limitations

Les activités suivantes restent de la responsabilité du Client :

- Fourniture de la spécification des caractéristiques du cluster Kubernetes managé et de sa localisation
- La gestion des conteneurs et des applications. Pour bénéficier de ce service, le Client doit souscrire une extension au niveau Managed Conteneur et Managed Application.

2.1 Catalogue de Change Kubernetes managé avec Caascad

Managed Kubernetes with CaasCad	Caascad	Caascad	Modification des valeurs min max des nodepool [2tk]
			Redimensionner les nœuds et redéployer un cluster pour 5 noeuds [4tk]
			Création d'une nouvelle nodepool [2tk]
			Restaurer le dépôt de code (Gitea) à partir d'une version sauvegardée [4tk]
			Activation de la fonctionnalité Vault Injector [2tk]
			Réaliser un "hibernate ou wake" du cluster de manière manuelle [1tk]
			Lancer un script de configuration sur un worker spécifique [2tk]
			Changer la période de rétention des logs [3tk]
			Changer la période de rétention globale des métriques [3tk]
			Ajout/modification d'une résolution DNS spécifique dans blackbox-exporter [3tk]
			Ajout/modification external label dans Prometheus client [3tk]
			Mise en place d'un routage des alertes vers un AlertManager externe [3tk]
			Ajout d'un receiver/route dans AlertManager pour les alertes [3tk]

3 Conteneur managé avec Caascad

Le service de Conteneur managé avec Caascad est un service du Prestataire qui permet au Client de déléguer la gestion des conteneurs de ses applications.

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

- Le déploiement de conteneurs à la demande sur des clusters Kubernetes managés à partir d'images, de dockerfiles et de manifestes fournis par le Client.
- La supervision 24 x 7 des conteneurs déployés dans les clusters kubernetes
- La notification et les interventions sur incidents en cas de dysfonctionnements des conteneurs sur la base de procédures agréées avec le Client et formalisées lors de la phase avant-vente.

Sur devis, le Prestataire peut prendre en charge la fourniture d'images conteneurs (OS, et Middleware).

3.1 Description

Les tableaux suivants répertorient les services fournis dans le cadre des services « Conteneur managé avec Caascad »

Table 1: Description des prestations « Conteneur managé avec Caascad»

Phase	Activities
Conteneur **Implémentation**	• Déployer des conteneurs à la demande sur des clusters Kubernetes managés à partir d'images et de manifestes de déploiement fournis par le Client et déposés dans les répertoires et registry Caascad. • Configurer la supervision des conteneurs des clusters Kubernetes managés
Conteneur **Opération**	• Supervision 24 x 7 des conteneurs déployés dans les clusters Kubernetes • Création des tickets d'incidents, investigation et notification du Client sur incident. • Redéploiement de la version N actuelle et N-1 des conteneurs à partir des images et des manifestes déposés dans Caascad* • Redimensionnement des quota alloués aux conteneurs au niveau des POD des clusters Kubernetes* • Déclenchement du support et résolution d'incident du service Managed Kubernetes en cas de problème sur le cluster sous-jacent Kubernetes. • Collecte et stockage des métriques et des logs exportés par les conteneurs dans le service Managed K8S avec Caascad. • Accès aux métriques, logs et alertes des conteneurs dans le service Managed Kubernetes avec Caascad. • Sauvegarde du git contenant les fichiers liés aux conteneurs par le service Managed Kubernetes avec Caascad.

(*) En fonction des procédures agréées par le Client lors de la phase avant-vente.

Les demandes de changement (*) issues du Client incluent :

- Le redéploiement de versions de conteneurs sur les clusters Kubernetes à partir des fichiers stockés dans les outils Caascad
- La création ou modification de routine de chaine de déploiement dans l'outillage Caascad
- La vérification du bon fonctionnement des conteneurs
- La modification des points d'exports des métriques et des logs des conteneurs
- La création et modification des alertes dans les tableaux de bord Caascad.
- L'ajout ou modification d'exporters sur les conteneurs, notamment pour les métriques applicatives.
- La création et modification de tableaux de bord de reporting sur les métriques et les logs dans les outils Caascad
- La structuration des outils git et de la chaine de déploiement (CD) pour intégration avec les process et la chaine d'intégration (CI) déjà employée par le Client.

(*) Pour obtenir la liste exhaustive des changements, se référer au catalogue de changes disponible dans le portail Cloud Store.

3.2 Prérequis du service

- Le service Managed Kubernetes avec Caascad doit être souscrit par le Client auprès du Prestataire
- Les clusters Kubernetes fonctionnels sont créés, et managés par le Prestataire
- La fourniture et dépose par le Client dans le repository et registry Caascad des images Docker, des dockerfiles, des manifestes, et des exporters envoyant les métriques et les logs,
- La validation par le Client des procédures à appliquer sur incident parmi les procédures proposées.

3.3 Limitations

Les activités suivantes restent de la responsabilité du Client :

- Mise à jour des fichiers de déploiement des conteneurs dans le Git Caascad
- Mise à jour des images conteneurs dans le repository Caascad
- La supervision applicative des conteneurs
- Les engagements de bon fonctionnement applicatif
- Les engagements de bon fonctionnement entre les conteneurs et les Machines Virtuelles (VM)
- Les conteneurs stateful

Le Client peut souscrire au service Application Managée pour compléter le service de Conteneur Managé avec la gestion applicative des conteneurs.

3.4 Catalogue de Change Managed Containers avec Caascad

Managed Containers with CaasCad	Container	Container	Déposer, Modifier ou supprimer un manifest dans le dépôt de code Git CaasCad [2tk]
			Déposer, Modifier ou supprimer un Docker file dans le repository CaasCad [2tk]
			Déposer, Modifier ou supprimer une routine dans la chaine déploiement CaasCad [2tk]
			Déployer une image de conteneur sur un cluster depuis le repository & un manifest [2tk]
			Déployer une image de conteneur version N-1 sur un cluster a partir d'un manifest [2tk]
			Déployer une version d'application sur un cluster a partir d'images et de manifests [4tk]
			Vérifier le bon déploiement d'une image de conteneur sur un K8S (hors applicatif) [2tk]
			Vérifier le bon déploiement d'un ensemble de conteneurs sur un K8S (hors applicatif) [4tk]
			Modifier le end point d'un exporter pour orienter les logs et metriques vers CaasCad [2tk]
			Créer/Modifier/Supprimer une alarme dans l'alerter CaasCad [4tk]
			Ajouter / configurer un exporter de métriques applicatives [au temps passé sur devis]
			Ajouter / configurer un dashboard Grafana de métriques / log dans CaasCad [sur devis]
			Structurer le GIT, la CD et outils pour intégration dans les process client [sur devis]

4 Définitions

Caascad désigne le service d'outillage pour l'exploitation des clusters Kubernetes, des conteneurs et des applications conteneurisées. Caascad also known as Conteneur as a Service Cloud Agnostic Deployment

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

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 Caascad.

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 une ressource cible dont l'outil Caascad collecte les métriques.

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

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.

Noeud désigne une machine virtuelle inclue 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

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

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

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.