Business

Technical appendix to the Managed Applications Service Description
Managed Service for Kubernetes®

Table of contents

1 Managed Service for Kubernetes®

1.1 Description

As part of this service, the Service Provider manages Kubernetes® clusters hosted on the Public IaaS Cloud Avenue infrastructure (the Service Provider).

The service consists of all or part of the following:

- The deployment of Kubernetes® clusters on demand from configurations provided by the Client.
- The 24 x 7 supervision and operational maintenance of the deployed Kubernetes® clusters.
- Notification and intervention on incidents for restoration or reconstruction from the repository in case of malfunctions of the Kubernetes® clusters.
- Restoring Kubernetes® clusters from a backed up repository
- Change management on Kubernetes® clusters.
- Managed tools for collecting, storing, viewing logs and infrastructure metrics.
- A managed visualization tool that allows the Client to observe metrics and alerts configured by the Service Provider.
- Optional access to DevOps tools (Managed DevOps Toolkit) to allow the Client to deploy applications on the cluster(s) managed by the Service Provider.

When deploying a Kubernetes® cluster by the Service Provider for the Customer, access to resources and functionalities is provided as follows:

- The Client receives a kubeconfig admin file containing the endpoint of the cluster API server (IP or domain name) and authentication details (username, password or token). The Customer may create other accounts directly within the cluster or obtain assistance from the Service Provider via a Change request.
- Using kubectl*: By using this kubeconfig, the Client can connect directly to the Kubernetes®* API server from its local machine or CI/CD pipeline without any other tools. The Client can execute commands like *kubectl get pods* or *kubectl apply -f myapp.yaml*.
- In parallel, the Client can access the different services of the Managed DevOps Toolkit through dedicated URLs that will be provided following the onboarding phase. These URLs and IPs are public.

This approach ensures a smooth and direct user experience for the Customer in the use of the services offered.

1.1.1 Prerequisites

Managed service for Kubernetes® requires governance with the Provider.

The network interconnection and security architecture must be defined prior to the deployment of the Service, during the pre-sales phase or a consulting assignment; these services must be operational as a prerequisite for the deployment of the Managed Service for Kubernetes®. They are not part of the Kubernetes® Managed Service.

In addition, for each cluster managed by the Service Provider, a control plane composed of 1 to 3 master nodes will be deployed. The only configuration of the plane control that allows to benefit from all the SLAs of the service is the one where the clusters are orchestrated by 3 master nodes. The size of these nodes is typically 4 vCPUs, 4 GB of RAM and 90 GB of storage, unless during the pre-sales phase or a consulting mission, The Service Provider notes that a different configuration must or may be considered depending on the size of the cluster to be managed or the customer use cases to be addressed.

Managed DevOps Toolkit service is optional for Kubernetes® Managed Service. To enable this option, and prior to installation and deployment, the Customer must provide the Service Provider with a list of authorized users, including their login credentials and email addresses.

The following activities remain the responsibility of the Client:

- Kubernetes® cluster(s) specification provided.
- Container and application management.

1.1.2 Maintenance in operational condition

As part of the offer, the Service Provider supports the operational maintenance of the Kubernetes® operating systems and distribution.

Operating system updates are performed every three months, including security patches.

The Service Provider uses a Rancher Kubernetes® Engine 2 distribution and follows a versioning system with the format "*M.m.P*" (where *M* represents the major version, *m* the minor version and *P* the security patch). Details on updates and release support are as follows*:*

- Major Updates (*M)*: Major updates should be coordinated with the Client as they affect critical components such as the ingress controller, and some manifests may become obsolete.
- Minor Updates (*m)*: Minor updates are usually released every three months. Upgrades may require scheduled downtime, either because master nodes may be temporarily unavailable or to ensure compatibility of the operators used by Customer.
- Mandatory Patches (*P)*: Approximately every month, mandatory patches are applied without requiring the scheduling of a maintenance window.
- Version Support: At any time during the service life cycle, the Service Provider supports the current version as well as the two previous minor versions (i.e., version *M.m.P, M.m-1.P, M.m-2.P).*

Phase	Activity
Kubernetes® Implementation	▪ Creation of the Kubernetes® cluster(s) with the Kubernetes® Engine 2 (RKE2) Rancher distribution ▪ Storage installation and configuration ▪ Network configuration, access services ▪ Installation and configuration of the supervision service
Kubernetes® Operations	▪ Kubernetes® core services administration and maintenance ▪ Minor and major updates ▪ Security management (update, access control) ▪ Service supervision 24/7 ▪ Event management ▪ Log management

1.1.3 Collection, storage, visualization of logs and metrics

The Service provides for each managed Kubernetes® cluster, a metric and log collection service. These collection services are installed, configured and managed by the Provider. At installation, these services are configured to collect the metrics required by the Provider to render the Managed Service for Kubernetes®.

Upon request and quotation, the Service Provider may provide the Customer with a means to define additional endpoints for the collection of application metrics. These endpoints must be deployed in the Kubernetes® cluster to be considered.

The Service provides a managed metric visualization tool (Grafana). The visualization tool is configured by default with a dashboard assembly. Upon request and on quotation, the Service Provider may provide the Client with personalised Grafana dashboards and Prometheus alerts.

The retention periods of logs and metrics are defined during the on-boarding. Thereafter, the Customer may request a change to modify them.

Phase	Activities
Implementation **logs/metrics**	▪ Installation and configuration of collection services ▪ Installation and configuration of long-term storage and processing services ▪ Retention Configuration ▪ Installation and configuration of the visualization service ▪ Adding default dashboards
Logs/Metrics **Transaction**	▪ Administration of services ▪ Minor or major updates ▪ Security management (update, access control) ▪ Service supervision 24/7 ▪ Event management ▪ Log management

1.1.4 Managed DevOps Toolkit

The Managed DevOps Toolkit service provides a tool for DevOps-oriented operations allowing co-management by the Provider and the Client on Cloud Avenue.

This toolset includes a set of managed as-a-service tools to build, test and deploy the applications in the Kubernetes® cluster(s) managed by the Provider

- Managing software artifacts repositories
- Decentralized version management GIT
- Automation of builds/tests/deployments
- A managed secret management service

An on-boarding session is provided at the initialization of the Service: this includes the creation of the Managed DevOps Toolkit environment and the provision of the URLs for accessing the Service, the statement of users named in the ticketing system of Support as well as the accompaniment of the Customer by an expert on the configuration and use of it.

The following activities remain the responsibility of the Client:

- Management of its application code.
- Management of the deployment of containers incorporating application updates.

The Service provides a code deposit in order to allow the Client to manage his code by himself. The Client is free to organize his code as he wishes. This service is dedicated to the Client, but the Provider's team is an administrator of this service and also uses it for operations on the Client's Environment(s).

The Service provides a Continuous Integration (CI) tool to allow the Client to create its containerized applications (build, tests and packaging). Jobs are organized in a pipeline to automate tasks. The CI tool allows to perform the usual tasks of Build (compilation, execution of scripts), tests (unit, functional, integration, load) and packaging (Docker). The Client is free to configure the desired pipelines.
The Service provides a Docker Registry to allow the Client to store all its application images. This service is dedicated to the Client.

The Service provides a secret manager based on Hashicorp Vault technology, allowing the Client to manage its application secrets itself. The Service Provider's team has an administrator right on the secrets manager.

The tools made available by the Managed DevOps Toolkit service require the use of a Multi-Factor Authentication (MFA) feature that will be configured by the Provider.

All tools in the Managed DevOps Toolkit are backed up and updated on a regular basis, which could result in temporary and negligible instances access loss.

The following activities remain the responsibility of the Client:

- Application code update and storage in the code repository
- Control of the Build chain
- Deploying applications on Kubernetes® clusters
- Update application secrets
- Adding annotations in the application manifests to allow the recovery of secrets

Managed Application Reporting Service does not apply to Managed DevOps Toolkit
The Managed Application Antivirus Service does not apply to the Managed DevOps Toolkit service that does not manage servers.
The Service Managed DevOps Toolkit does not include IaaS consumption and Client Environment services that Customer must purchase separately from the IaaS provider at its current rates.

1.2 Price conditions

The pricing of the Service is composed of:

- Service Managed for Kubernetes® access fee that includes all the tasks mentioned in the implementation RACI. In order to estimate these costs, a customer needs study is carried out by the Service Provider, following which a quote for access fees is created.
- A recurring monthly "Run" covering Managed Service for Kubernetes® operations maintenance activities indexed on the number of instances managed and configured options.

The monthly recurring prices for "Run" are shown in the table below.

Family	Under Family	Service unit
DevOps Services	Managed Service for Kubernetes®	Per cluster, up to 8 managed worker nodes
DevOps Services	Managed Service for Kubernetes®	By additional managed worker node
DevOps Services	Access to Managed DevOps Toolkit services	Per user with access to at least one Managed DevOps Toolkit service
DevOps Services	Application endpoint monitoring	Per pack of 5 probes

Service rates do not include:

- The price of the infrastructure that the Customer must subscribe from the IaaS provider according to the tariffs in force.
- Requests for change.

1.3 Managed Service for Kubernetes® Change catalogue

Family	Under Family	Token Full France	Token Global	Description (complete) Service Request
DevOps Services	Managed Service for Kubernetes®	2	2	Modification of the min max values of nodepool
DevOps Services	Managed Service for Kubernetes®	4	4	Resize nodes and redeploy a cluster for 5 nodes
DevOps Services	Managed Service for Kubernetes®	2	2	Creating a new nodepool
DevOps Services	Managed Service for Kubernetes®	3	3	Add/change external label in Prometheus client
DevOps Services	Managed Service for Kubernetes®	3	3	Added a receiver/route in AlertManager for alerts
DevOps Services	Collection, storage, visualization of logs and metrics	On request	On request	Modification of the retention period for logs or metrics (global)
DevOps Services	Collection, storage, visualization of logs and metrics	On request	On request	Configuration of a new application endpoint monitoring probe
DevOps Services	Collection, storage, visualization of logs and metrics	On request	On request	Configuration of a new custom monitoring dashboard
DevOps Services	Backup and Restore	On request	On request	Restore the code repository from the desired saved version

1.4 Off-catalogue requests

You can make an off-catalogue request and provide the details of your need. We will set up a half an hour phone call with you to ensure the need is well understood. 2 cases arise then:

- If the functional need is immediately qualifiable in simple, medium or complex tasks as defined in the catalogue, the change request is finally reclassified as a catalogue request and can be processed by the operational teams.

- If the functional need is not immediately translatable into simple or complex tasks and this will require a thorough study with a time and lead time, an estimate of the number of Tokens needed for the study will be made. This study is without guarantee of outcome, given the very wide range of functional needs that can be expressed. In case of agreement, the study is carried out and results in a feasibility or not. In case of feasibility, it is accompanied by an assessment of the costs associated with its implementation. These charges will be qualified as simple or complex change requests according to the criteria set out above.

2 Glossary

CI/CD (Continuous Integration/ Continuous Deployment) refers to the service of construction and deployment of containers in the Cloud From the Managed DevOps Toolkit solution provider.

Standard Change means a change initiated by the Customer or the Service Provider, implemented through a procedure validated by the Service Provider and accepted by the Customer. Any change considered as Standard is defined in the list of standard changes of the change catalogue, accessible through the Cloud Store Client Area. The price of standard changes is defined and known to the Customer.
Simple Standard Change refers to a Standard change of a Token at the initiative of the Client or the Service Provider, which requires little effort, or has an impact on a limited number of services, implemented by a procedure validated by the Service Provider and accepted by the Customer. Any change considered as Simple is defined in the standard changes list of the change catalogue accessible through the Cloud Store Client Area.
Complex Standard Change means a Standard change of more than one Token at the initiative of the Client or the Service Provider, which requires a significant effort, or has an impact on several services, implemented by a procedure validated by the Service Provider and accepted by the Customer. Any change considered as a Complex Standard is defined in the list of standard changes in the change catalogue accessible through the Cloud Store Client Area.

Non-Standard Change refers to a change outside the standard catalogue and on a quote at the initiative of the Customer, or the Service Provider, implemented by a procedure validated by the Service Provider and accepted by the Customer.

Accelerated Change refers to a simple or complex standard service change requiring an accelerated production of the Customer's request. The accelerated change price is double the change requested by the Client. The Client has the possibility to request accelerated processing of a simple or complex Standard change in an exceptional manner at a maximum of 6 per year.

Cluster refers to a group of nodes delivering distributed compute/processing capability

Endpoint refers to a specific access point of an application or web service, usually in the form of a URL, that allows interaction with a particular system feature. In the context of application monitoring, an endpoint is a specific target to monitor for assessing the health, performance and availability of a service or part of an application. .

Environment means a virtual private space of resources on the IaaS to which only users authenticated by login and password can have access. The actions of creation, destruction, modification, listing of these resources and associated features are limited to those Users only.

Client Environment refers to the environment in which Client containers are deployed. The actions of creation, destruction, modification, listing of resources and associated functionalities are assigned to the Service Provider and the Customer. The Client may use this tenant to run applications and use IaaS features outside of the Managed DevOps Toolkit solution.

Git is code versioning software.

IaC refers to the infrastructure as code.

IaaS refers to the cloud infrastructure service, including, where applicable, the associated complementary services (such as PaaS, CaaS, DBaaS, etc.), subscribed by the Customer for the purpose of hosting its Managed Tenant.

Kubernetes® refers to open source software for container deployment and management. Kubernetes® is a registered trademark of the Linux Foundation. Please see Kubernetes.io.