Business

Service Description
Managed Applications

Table of Contents

List of figures

List of table

1 Definitions

Complementary to the definitions in the General Terms and Conditions the Incorporation, Maintenance and Related Services for Sales of Terminals Specific Terms, the following specific definitions shall apply with respect to this Service Description.

Availability Zone refers to a separate data center sufficiently distant from the others, if any, in the same Region to allow the implementation of a local resilience. Availability Zones in each Region are listed in the Service Description.

Axway Vision Gateway refers to a file transfer gateway that secures the exchange of files between different networks.

CaaSCAD refers to the service name of tooling service for managing Kubernetes clusters, containers, containerized applications. CaasCad also known as Container as a Service Cloud Agnostic Deployment.

CCE Cloud Container Engine refers to a container service of the Provider Flexible Engine cloud.

CFT (Cross File Transfer) refers to the file transfer protocol.

CI/CD (Continuous Integration / Continuous Deployment) refers to the cloud container build and deployment service of the CaaSCAD solution.

Cluster refers to group of nodes delivering a consistent big data processing capability based on a given set of Big Data functions.

CSQP (Customer Service Quality Plan) refers to all measures taken by the Provider to produce services within the Contract scope, in accordance with the Contract's provisions. The CSQP lists the service execution conditions visible to both parties, and not the information over which only the Provider has control and visibility. The CSQP provisions may under no circumstances prevail over Contract stipulations.

Customer Administration Environment means the environment in which the Customer's Service is hosted (build and deployment). The actions of creation, destruction, modification, listing of resources and associated Functionalities are limited to the Provider.

Customer Environment means the environment in which the Customer's containers are deployed. The actions of creation, destruction, modification, listing of resources and associated functionalities are assigned to the Provider and the Customer. The Customer may use this Container to run applications and use IaaS functionalities outside the CaaSCAD solution.

Domain Controller refers to the set of servers running the Active Directory Domain Services role.

Endpoint is a target resource for which the CaasCad tool collects metrics.

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

Full France: the teams that provide the service and/or support are based in France.

General Terms and Conditions refers to the Provider' general terms and conditions for Cloud Services.

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

Kubernetes is an open source software allowing the deployment and management of containers.

Log As A Service refers to the service provide by the components of the ECE (Elastic Cloud Enterprise) suite.

Maintenance Release refers to a Software release that delivers error corrections that are severely affecting a number of customers and cannot wait for the next Major Release or Minor Release. It is identified by the third digit of the release: (x.y.Z)

Managed Base refers to the technical foundation provided by the Provider allowing to implement and operate the subscribed Service Units.

Managed Computer Vision refers to the service employing artificial intelligence for video analysis and allowing customers to gather insights and trigger alerts which are shown through a dedicated customer dashboard.

Managed Tenant refers to the Tenant in which the Customer's Service is hosted. Creation, deletion, modification and listing of these resources and associated Features may be performed by the Provider only.

Middleware refers to the Software component required for an application to run, outside of the operating system (OS) or databases.

Native Hyperscaler Services refers to services provided by the IaaS hyperscalers Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP).

Node refers to a virtual machine included in a Cluster.

Off-Shore: the teams that provide the service and/or support services are partly based outside France.

On-boarding refers to the CaasCad installation, deployment and support service provided by an expert from the Provider.

Platform refers to a subset of the Managed Tenant hosting one or more Big Data Software, which may include several Clusters.

Project refers to a project for which the Customer subscribes to the Service, as referenced in the Purchase Order.

Region refers to a geographical area where the Service is available on one or several Availability Zone(s).

Service refers to the service “Managed Applications” provided for one Managed Tenant. Each Managed Tenant constitutes a separate Service.

Service Pack refers to all updates, corrections and/or improvements to Software delivered as a single installable package.

Service Unit refers to a sub-set of the service provided on a Virtual Machine (VM) or physical server, in the event of managed OS Functionalities, Managed Database or Managed Middleware, and on one or more VM(s) or physical server(s) where the managed Application Functionality is concerned. The Customer subscribes to Service Units using the Order.

Slave Node refers to a dataNode which is responsible for serving read and write requests from the file system’s clients along with performing block creation, deletion and replication upon instruction from the Master Node and tasktracker which is a node in the Cluster

SRE (Site Reliability Engineer) refers to a service of expertise of the Provider for advice and technical assistance on the Customer's environment.

SRF (or **Service Request Form**) refers to the form that must be filled out, describing the technical characteristics of the services to be delivered.**Tenant** refers to a virtual private pool of IaaS resources, only accessible to Users which are authenticated by login and password. Creation, deletion, modification and listing of these resources and associated Features may be performed by those Users only. For VMware-based IaaS, the Tenant is also called an "Organization".

Token refers to the work unit used to state the prices applicable to the changes requested by the Customer, as mentioned in the Price List.

Transition class refers to the scope of responsibility of the Customer and the Service Provider for the transition of the Customer environment to the Cloud. An inventory of the resources to be managed is made by the Provider to choose the transition class the most adapted to the Customer context.

Class 2 refers to the scope of the Service Provider's business in which the Service Provider supports the managed service of the resources according to the procedure guide provided by the customer (Change), and in which the Service Provider is responsible for the recovery of data in case of failure. This scope includes the integration of the relevant CSP alarms into the Provider's back-end systems, the input of the customer-provided procedure guides into the Provider's operations knowledge repository, and the preparation of operations.

Class 4 refers to the Provider's scope in which the Provider configures and maintains the CSP's management tools to manage the service as well as the integration into the Provider's backend systems.

Class 5 refers to the scope of the Service Provider in which the Service Provider configures the required Infrastructure as Code (IaC) for the resources and for the relevant CSP management tools as well as integration into the Service Provider's backend system**.**

Workload refers an application environment of the Customer to be executed on a Cloud resource of the Provider

2 Purpose of the document

The purpose of the present Service Description is to define the Managed Applications Service and to set forth the conditions under which it is provided by the Provider, in application of General Terms and Conditions.

3 Overview of the Service

3.1 Overall description

The service Managed Applications provide to Customer the following 11 management levels:

1. **Governance and advisory services**: governance to drive the project and additional guidance and advisory services.
2. **Managed OS:** Operating system management including tasks related to the server and supplementary upgrading activities,
3. **Managed database:** This service provides the Customer with complete database management, including tasks connected with the server and optimisation and upgrading activities.
4. **Managed middleware** including all software offered in the catalogue by the components:
    - Web server
    - Proxy server
    - Application server
    - File server
    - DDI
    - Source Code Manager
5. **Managed Kubernetes with CaasCad**: supervision and operations for Kubernetes clusters with tooling suitable to co-management.
6. **Managed container with CaasCad:** supervision and operations for containers deployed on Kubernetes clusters with tooling suitable to co-management.
7. **CaasCad:** a tool for multi-cloud co-management of the Provider's catalog.
8. **Managed application:** Customer business application management (e-business web, ERP, CRM, Finance, HR, etc.) based on Customer procedures except SAP.
9. **Managed Hyperscaler Native Services**: monitoring and operation of cloud native services and hyperscaler PaaS services (Azure, AWS, GCP).
10. **Log as a Service (LaaS):** The Log As A Service managed with ECE (Elastic Cloud Enterprise) components is a Provider service. It is a complete end-to-end log analysis solution that helps in deep search, analysis and visualization of logs generated by different machines.
11. **Managed Big Data:** Installation, Monitoring and Operation for Big Data solutions managed by the Provider
12. **Managed Security Services:** A service that enables the management of third-party or native security components within the Provider's infrastructures.

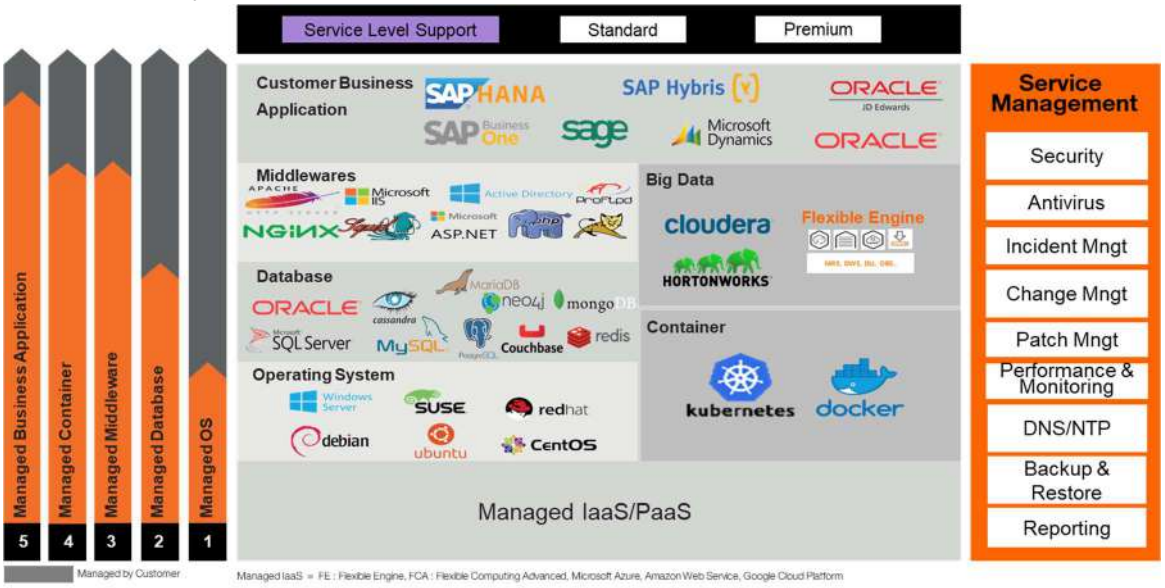


Figure 1 – Managed Applications Service Catalog

The Customer has the possibility of subscribing to different levels of management to for a single Project, however:

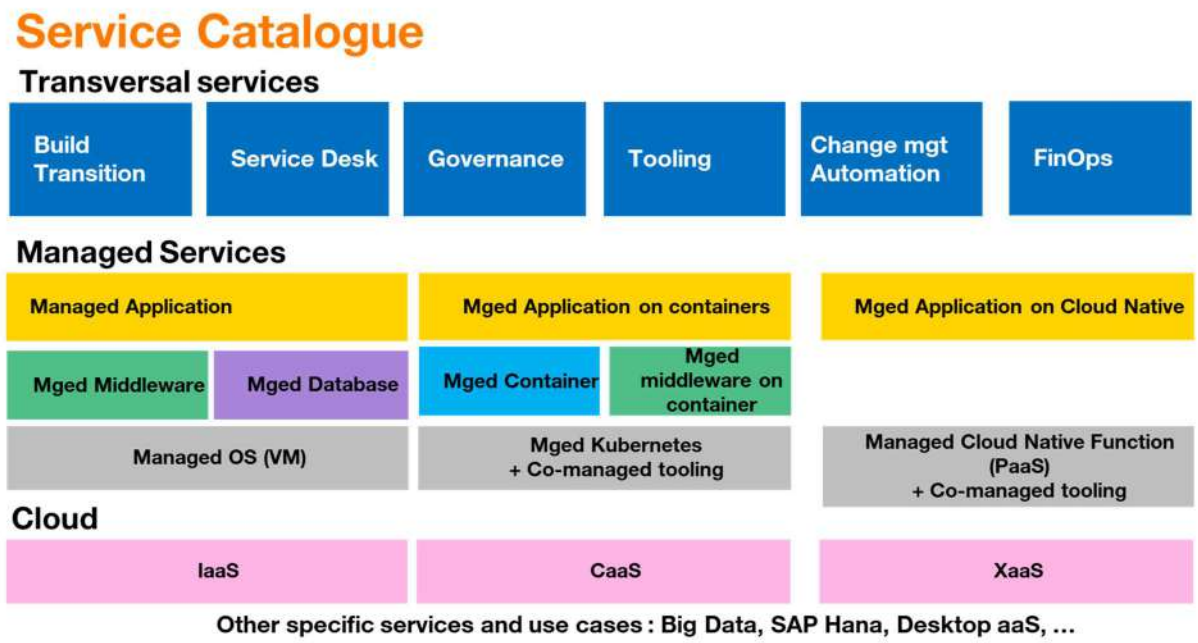
- For the managed database and managed middleware management levels, the Customer is required to subscribe to the managed OS management level as a pre-requisite.
- For the managed container level, the Customer is required to subscribe to the managed Kubernetes level as a pre-requisite.
- At the Managed Application management level, the Customer is required to subscribe to the managed OS management level, the managed database and managed middleware management levels, or to the managed container management level and the managed Kubernetes with CaasCad level, as the application requires that the related components be implemented in order to function.

Each of the Managed Tenant's virtual servers (VM) may have one of the 4 possible management levels. The management level applies to the server in its entirety; different software cannot be hosted at different management levels on a single server.

Each of the Managed Tenant's Kubernetes cluster may have one of the 3 possible management levels (managed Kubernetes, managed container, managed application on containers).

The Customer chooses at the time of ordering a support level among the two available (Standard, Premium) that applies to the entire Service. If the Customer wishes to benefit from different levels of support, he must subscribe to several Services, which will be deployed on separate Managed Tenants.

3.2 The Service Catalogue



3.3 Geographical footprint

The Customer may subscribe to the “Managed Applications” Service on any IaaS proposed in the Order. The Region is selected by the Customer at the time of Order and recorded in the high level design document.

4 Price conditions

4.1 Prices

The pricing of the service is different depending on whether it is:

- Service units ordered at contract signing;

- Additional service units ordered afterwards;

- Backup and restore services;

- On-demand tokens;

- Support services.

The Service is subject to a Service access fee and a monthly minimum charge, the amounts of which are indicated in the Price List, plus the price of the Service Units and services subscribed to (restoration, backup, support and Tokens).

Backup and restore services, support services and on-demand tokens are charged at the price of the Price List in effect at the time of their subscription.

The prices are defined per Region.

When the prices depend on the duration of the commitment, the commitment period taken into account for the subscription of additional services is equal to the remaining commitment duration rounded up when applicable to the duration immediately superior existing in the Price List.

The rates of the Managed Applications Service do not include the price of the Managed Tenant, to which the Customer must subscribe otherwise from the IaaS supplier according to the current rates.

4.2 Price revision

The prices of the Services (excluding backup and restoration services, support services and tokens on demand) may be revised each year on the anniversary date of the Contract by applying the following formula: P1 = P0 x S1 / S0
Where P1 = revised price
P0 = initial price
S0 = last SYNTEC index published on the date the Contract was entered into or on the date of the previous revision
S1 = last SYNTEC index published on the revision date.
If the SYNTEC index disappears, a new index shall be chosen so that it is as close as possible to the removed index.

4.2.1 Specific price revision

If the equipment used by the Service Provider to administer the Customer's service units requires a physical hosting area, then the prices of these service units may be revised each year on the anniversary date of the Contract - in addition to the revision linked to the SYNTEC index - by applying the following formula:

P = P-1 * [⅔ (S/S-1) + ⅓ (T/T-1)]

Where:
- P is the revised amount, P-1 is the amount in effect prior to the revision date,

- S is the latest construction cost index published by INSEE at the revision date (ICC base 100 at 4th quarter 1953, quarterly), and S-1 is the construction cost index published twelve months prior to the revision date,

- T is the monthly index of the cost of medium-voltage electricity published by INSEE (electricity sold to companies with a contract for capacity > 36 kVA) at the revision date, and T-1 is the monthly index of the cost of medium-voltage electricity published twelve months prior to the revision date.

In all cases, the Service Provider will apply at least the tariff conditions linked to changes in energy costs published by INSEE.

In the event of the disappearance or non-publication of one of these indices, it will be replaced by an index of comparable effect.

4.2.2 Revision of prices for licenses and managed equipment

The Service Provider reserves the right to increase its prices if the third-party supplier of the licenses or managed equipment necessary for the proper delivery of the Service increases its published public price list and/or notifies the Service Provider of a price increase for such equipment and licenses. This increase will be limited to the increases notified by the third-party supplier for equipment and licenses.

The Service Provider will inform the Customer of any price increase imposed by the third-party supplier and the impact on prices.

4.3 Guaranteed Minimum Revenue (GMR)

The initial contract stipulates the Global Revenue expected by the Service Provider during the RUN phase.

In return for the resources and specific organization put in place by the Service Provider for the execution of the Contract, the Client undertakes, during the RUN phase, to maintain a Guaranteed Minimum Revenue (GMR) corresponding to 80% of the amount of Global Revenue provided for in the Contract.

At the end of each RUN year, the Parties shall ensure that the annual GWA is achieved. The Annual GWA is calculated by dividing the Aggregate GWA amount by the number of RUN years provided for in the Contract.

If the amount actually billed by the Provider for a RUN year is less than the Annual GWA amount, the difference between the Annual GWA amount and the Amount billed during the year (hereinafter the "Differential") shall be owed by the Client to the Provider and billed within thirty (30) days of the Provider's written notification of the existence of such

Differential. In the event that an annual MRG is exceeded, the excess will contribute to the annual MRG for the following year.

In the event of an increase in the scope of services (new service(s) and/or modification of planned services) having a price impact of more than 15% compared to the Global Revenue provided for in the Contract, the Global MRG shall be revised upwards in proportion to the percentage of price variation noted by the Parties for this change in scope.

4.4 Price of the Support

Support services are defined in the Customer contract as follows:
- a support level: Initial, Standard or Premium
- a type of support: Off-Shore or Full France
- and a number of tickets, which is determined specifically for each Customer.

An assessment will be made on a regular basis to count the number of tickets actually used by the Customer over the past period. Any excess of the number of tickets defined in the contract will be invoiced at the unit price of the ticket indicated in the Managed Applications Price list.

4.5 Incident ticket prices

Service Desk billing is linked to the Customer's environment. The Customer can subscribe to the following 4 types of environment as part of the Managed Applications offer, according to his needs:
- Production environment
- Pre-production environment
- Integration environment
- Development environment

In addition, there are four levels of support to which correspond four rates for trouble tickets:
-Ticket SLA Premium
-Ticket SLA Standard
-Ticket SLA Initial
-Ticket no SLA

If the Customer has subscribed to several environments, with different levels of support for different environments, the incident ticket rate will be that of the highest ticket.

4.6 Price of Additional Service Units

The price of the service units ordered at the signing of the Contract is fixed during the Customer's commitment period.

Any order for service units different from the service units ordered at the signing of the Contract will be invoiced at the price of the service units in the price list in force at the time of this order.

4.7 Build and Run billing

4.7.1 Build billing

Customer billing by the Service Provider during the Build phase can be carried out in two manners:

1. For small projects, the Provider invoices 30% of the Build amount on receipt of the purchase order duly signed by the Customer, and invoices the remaining 70% on completion of the Build phase.
2. For customer projects of which the Build phase is spread over several months, the sales representative dedicated to Customer will define batches/due dates with his project manager, in agreement with the Customer. The Service Provider invoices the Build amount in batches, respecting the due dates agreed.

4.7.2 Run billing

Invoicing for the run starts on delivery:

1. Either the entire Build,
2. Or a defined batch, in the case of batch billing.

5 Price conditions

5.1 Minimum period

The minimum duration of the Service is one year. The duration of the Customer's commitment is specified in the Order.

A Managed Tenant may host several of the Customer's Projects, whose commitment end dates may be different.

5.2 Scheduled maintenance

Recurring timeslots for maintenance are stated in the CSQP.

In addition, some administration tasks, such as patches or security maintenance, are proactively performed by the Provider.

5.3 Reversibility

In line with the General Terms and Conditions, the reversibility conditions are defined as follows:

- The reversibility period shall not exceed 3 months.
- During the reversibility phase, the “Guaranteed Fault Repair Time” does not apply.
- The Provider undertakes in particular to provide all technical information about the service architecture (SCQP, SRF), provided that information requested is not considered protected know-how by the Provider.

Should supplementary assistance be required, in addition to that defined above, with steering requested of the Provider, the Customer shall receive:

- An offer for paid assistance specifying the conditions for assistance, personnel dedicated to reversibility operations, and the possible hardware and physical facilities required.
- The financial terms applicable to the implementation of this supplementary assistance.

The Customer, meanwhile, undertakes to provide any technical or human assistance, and where applicable, financial assistance needed to duly perform the service migration. The Contract's terms and conditions shall continue to apply up to the term of the Reversibility Period.

In all events, the Customer shall be solely responsible for its relationship with the buyer and its actions with the latter.

6 Access to the Service

6.1 Prerequisite

The “Managed Applications” Service relies on a IaaS service, to which the Customer must also subscribe. The Tenant subscribed by the Customer is a Managed Tenant, administered by the Provider.

The Customer must subscribe to the IaaS support level of his choice and will be invoiced for IaaS support as part of the corresponding contract. For the IaaS Flexible Engine, the level of support to be subscribed is "Managed Tenant».

The IaaS service corresponding to the Managed Tenant shall be billed as soon as it is put into operation, without waiting for the Managed Applications managed service acceptance.

For Managed Tenant, some IaaS functionalities will not be available to the Customer:

- ⇨ Change management, incident management, and releases (security rules, VM upgrades, etc.) are run under the “Managed Applications” service.
- ⇨ The IaaS console and reporting tools in the Cloud Store are available in read-only mode.
- ⇨ The Customer delegates to the Provider responsibility for selected management tasks on its Managed Tenant, in accordance with the provisions of the document herein.

6.2 Portal – Cloud Store Customer Space

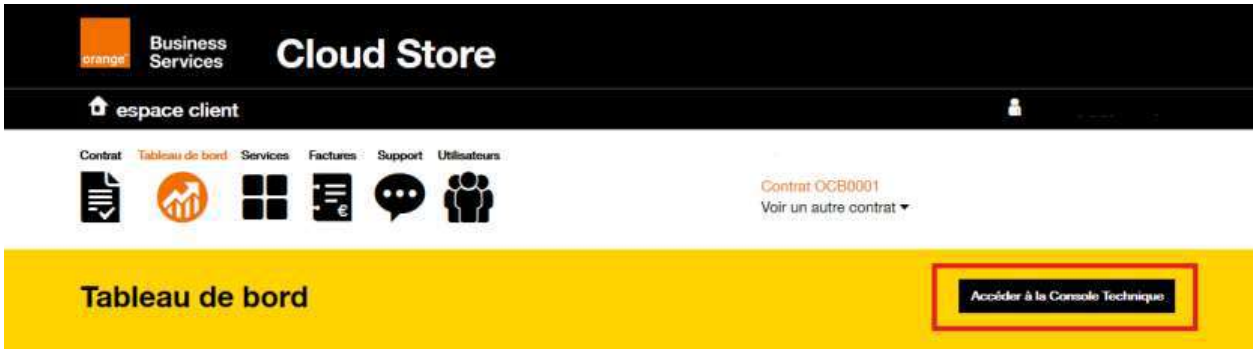


Figure 2 - The Cloud Store Portal

The Cloud Store Customer Area allows to manage all contracts to which they have subscribed, in particular via the following sections:

- Contract: this section offers viewing general information on contracts and orders made.
- Dashboard : enables Customers to access the IaaS console through SSO (Single Sign On), in read only mode.
- Services: enables Customers to order online services or access the change request tools.
- Invoices: enables Customers to view all invoices on-line and access the information needed to contact the invoicing department
- Documents; documentation management space allowing the Customer to access documents organized in five directories: User guides, performance reports, technical dashboards, meeting minutes, miscellaneous.
- Support: provides access to the incident reporting tool and information needed to contact the customer support centre.
- Users: enables Customers to manage user rights on each offer and on the customer space.

7 Content of the Service

7.1 Guidance and advice services

7.1.1 Service Delivery Manager

The Service Delivery Manager (or SDM) is the Customer's main point of contact for the proper functioning of the Managed Applications Service This service must be subscribed for each Project that includes at least one Premium Support Level Managed Tenant. This service is not available for Projects that include only Standard Support Level Managed Tenants.

The Service Delivery Manager provides the following services:

- Taking part in implementing upgrades / improvement to Customer Service during the run phase,
- Monitoring due functioning of Customer Service during the run phase,
- Advising Customer on possible upgrades to Services subscribed to,
- Servicing in escalation mode, either at the Customer's request, or at that of the Provider teams, or proactively,
- Implementing and steering the quality assurance process,
- In charge of capacity management on the Customer environment (Disk, CPU, RAM). Informing the Customer about upgrades to be taken into account to allow optimal functioning of the environment.

7.1.2 Contract Business Manager

The Contract Business Manager (CBM) is the main contractual contact for the Customer's IT department for Managed Applications Service.

This service must be subscribed for each Project that includes at least one Premium Support Level Managed Tenant. This service is not available for Projects that include only Standard Support Level Managed Tenants.

The Contract Business Manager provides the following services:

- He ensures that the Provider' contractual and commercial commitments to the Customer are respected
- It implements, monitors and updates the Customer's document repository
- He leads governance: Steering Committee and Strategic Committee

- He is the Customer's privileged contact for all matters relating to contractual developments in the life of the solution

7.1.3 Lead Technician

The Lead Technician is the Customer's main technical contact during the run phase of the Service. This service is recommended for complex projects.

The Lead Technician provides the following services:

- Organization of technical committees to improve the performance of the solution;
- Investigation of malfunctions and proposal of solutions;
- Study and implementation of changes.

7.1.4 Architectural design

The architecture design service consists in providing an high level design for the Customer's project at the end of a study based on the Customer's specifications. This service is recommended for complex projects.

7.1.5 DevOps expertise

The DevOps expertise service provides advice and technical assistance for the Customer's implementation of a continuous integration / delivery approach on its Managed Tenant.

A report containing the recommendations will be sent to the Customer at the end of each intervention.

7.1.6 The Service Reliability Engineer (SRE)

The Service Reliability Engineer (SRE) is a key player in managed services, particularly in the DevOps and Co-management models.

The SRE is a named expert, knowledgeable in operations and software engineering, participating simultaneously in the execution of the managed service within the Service Provider's operations team, and working closely with the Service Provider's development team.

The SRE works closely with the Customer's development team to identify and implement observability indicators, operations automation and infrastructure as code to meet business needs. He brings his expertise to the development team to provide the tools needed for reliable operation. In the longer term, the SRE contributes to the continuous improvement of the reliability of the business application and its operations.

The SRE participates (remotely) in regular meetings with application owners to align continuous improvements.

7.1.6.1 Deliverables

The SRE contributes, with the development team, to the following deliverables:

- Guidelines for DevOps automation (Infra as Code, integration, etc.) according to the maturity of the Customer's team.
- Infra as Code required to deploy / redeploy resources in the event of loss of service or misconfiguration.
- Identification and implementation of observability measures required to monitor business activity.
- Define and manage SLOs (Service Level Objectives) and SLIs (Service Level Information).
- Setting up automated dashboards to analyze metrics and trends. Advice on the tools needed to implement them.
- Identification of alarms/thresholds on metrics and alarm collection mechanism.
- Identification of backup procedures and security measures required for the application and data to meet customer requirements.
- Drafting of the main procedures needed to deal with known incidents. These procedures will be passed on to the level 1 and 2 operational teams.
    - Simple procedures are generally integrated into the infrastructure as code to speed up corrective action.

- Review/validation of technical procedures for changes proposed by the Service Delivery Manager for inclusion in the change catalog.
- Identification and implementation of log collection to detect anomalies and facilitate business application troubleshooting. Set up automated correlations and alerts based on log analysis.
- Cold analysis of dashboards and logs for on-demand preventive maintenance.
- Configuration of security tools and SIEM (Security Information & Event Management).
- Definition and drafting of recurring control procedures where necessary.
- Pre-production go criteria. RACI between Customer and Service Provider for pre-production deployment. Automation of deployment if necessary.
- Criteria for going into production, taking into account technical and business constraints (deployment time, special events, etc.). RACI between Customer and Service Provider for production deployment. Automate deployment if necessary.

7.1.6.2 Limitations

- Architecture is not the responsibility of the SRE. Rather, it is the responsibility of the customer or an architect, i.e. the Technical Design Authority (TDA).
- Disaster recovery design is not the responsibility of the SRE, but of a TDA.
- The build and design of the architecture, including disaster recovery, HLD and LLD, is the responsibility of the customer or an architect.

7.2 Managed OS

With this service, the Customer is provided with complete operating system management, including tasks connected with the VM (Virtual Machine). It is available only to the Customer's Managed Tenants.

7.2.1 Description

The description of the services provided under the Managed OS Service is:

Table 1: Description of "Managed OS" services

Phase	Activities
OS Server implementation	▪ Installing and configuring operating system ▪ Installing and configuring storage ▪ Configuring the network and access services ▪ Installing and configuring agents (DNS, NTP, Antivirus Sophos services, monitoring agent) ▪ Deploy and configure the Snapshot backup solution for customer servers on the IaaS ▪ Perform implementation checks of the Snapshot backup ▪ Configure the monitoring of the " Snapshot " backup ▪ Configuring access to the package repository ▪ Installing and configuring the IaaS security service
OS Server operation	▪ Administering and maintaining the configuration ▪ Evaluating, planning and executing requests for changes ▪ Patch services ▪ 24x7x365 supervision ▪ Incident upscaling ▪ Monitoring of "Snapshot" backups Client 24x7x365 ▪ Snapshot backup rescheduling in case of failure ▪ Restore(s) on customer request (by changes) ▪ Capacity management on the "Snapshot" backup platform

Customers may request specific retention policies and customized backup frequencies. Specific requests are submitted to the Provider for validation and quotation.

7.2.2 Specifications

The service applies to the following operating systems:

Table 2: "Managed OS" specifications

OS	Distribution and version
Linux	▪ CentOS ▪ Debian ▪ Ubuntu ▪ Red Hat Enterprise Linux ▪ Suse
Windows Server	▪ Versions supported by the editor

7.2.3 "Snapshot" backup and restore service

This service is included in the Managed OS service offered to Managed Applications customers.
The backup and restore service is provided to customers who already subscribe to the Managed OS services.

This Snapshot Backup Service allows the Service Provider to back up and restore at full disk level (system and data), the content of the Client servers deployed on their Managed Tenants.

The type of "Snapshot" Backup depends on the underlying IaaS on which the Managed Service subscribed by the Customer is deployed. When the Managed Backup and Restore Service is based on a backup system integrated into the IaaS, the cost of the service is borne by the Customer as part of the IaaS service it has subscribed to.

The backup policy is predefined in the "Snapshot" backup system of the managed OS service as follows A daily backup with 6 days retention and a weekly backup with 4 weeks retention.

The Customer can, via a change request, request a disk restoration since the last "Snapshot" backup.
The pricing of the "Snapshot" backup service for the iaaS part depends on the volume of data protected and the associated storage space.

7.2.4 Limitations

The following activities remain the Customer's responsibility:

- Verifying the proper operation of the infrastructure and of the OS'
- Making the decision to restore operating system
- Do not deploy OS updates
- Do not deploy an application not validated by the Provider
- Do not disable the antivirus
- Not joining an AD domain
- The Customer cannot refuse the basic "Snapshot" backup service proposed in the offer, as it ensures the Provider's SLA,
- In case of a change in the "Snapshot" backup policy at the request of the Customer, the Customer is responsible for the associated recovery capacity,
- The Customer is responsible for any decision to restore a file or a group of files,
- The "Snapshot" backup does not include specific backups (Active Directory, Messaging, ...). Other solutions of the Provider are proposed in the catalog.

The Customer shall not have root or administrator rights on the OS, and shall not be allowed to integrate a VM from the Managed Tenant into a Domain Controller not managed by the Provider.

7.3 Managed database

The Provider technically operates the Customer database(s) as well as optimisation and upgrading activities.

For managed DBaaS (DataBase as a Service), database software licenses are provided :

- ✓ as part of the IaaS service subscribed by the Customer.
- ✓ by the Provider, holder of the Licenses. In other cases, the licenses of the database software are subscribed
- ✓ or by the Customer, depending on the Software publishers' terms.

For managed DBaaS, the cost of the DBaaS service is borne by the customer as part of the IaaS service it has subscribed to.

7.3.1 Description

The managed database consists of the following services:

Table 3: "Managed database" description:

Phase	Activities
Database implementation	▪ Installing and configuring storage ▪ Installing and configuring the database(s) ▪ Setting up the network and access services ▪ Installing and configuring agents (DNS, NTP, Antivirus Sophos services, backup agent, monitoring agent) ▪ Installing and configuring the security service ▪ Multi-AZ Deployments (DBaaS only)
Database Operation	▪ Administering and maintaining the configuration ▪ Evaluating, planning and executing requests for changes ▪ Patch services (excluding DBaaS) ▪ 24x7x365 supervision ▪ Incident upscaling ▪ Back-up and restoration services ▪ Event management

7.3.2 Specifications

The service applies to the following databases:

Table 4: Specifications for "Managed database"

Databases	Products	
Database relational	▪ PostgreSQL ▪ MySQL ▪ MariaDB ▪ Microsoft SQL Server ▪ Oracle	
Database Non-relational	▪ MongoDB ▪ Cassandra ▪ Neo4j ▪ Couchbase ▪ Redis ▪ Elasticsearch	
Database DBaaS	▪ PostgreSQL ▪ MySQL ▪ Microsoft SQL Server ▪ Maria DB ▪ Oracle Database	☑ FE, Azure, AWS, GCP ☑ FE, Azure, AWS, GCP ☑ FE, Azure, AWS, GCP ☑ Azure, AWS ☑ Azure, AWS

☑ Availability according to IaaS: Flexible Engine (FE), Microsoft Azure (Azure), Amazon Web Service (AWS), Google Cloud Platform (GCP)

7.3.3 Limitations

The following activities remain the Customer's responsibility:

- Verifying the proper operation of the database
- Making decision to restore database
- Performing business tasks dependent on the Customer application

7.4 Managed middleware

The middleware are installed and set up by the Provider.

The operating system is always fully-managed by the Provider. It is mandatory that the Customer subscribe to the Managed OS service.

7.4.1 Description

The following chart lists the services supplied as part of the “Managed Middleware” services:

Table 5: Description of “Managed Middleware” services

Phase	Activities
Middleware Implementation	▪ Installing and configuring the middleware ▪ Compliance with safety recommendations
Middleware Operation	▪ Administering and maintaining the configuration ▪ Making minor upgrades ▪ Making major upgrades for some middlewares only ▪ Managing security (patches, access control, anti-virus, etc.) ▪ Back-up and restoration services ▪ Resource optimization ▪ Capacity management ▪ Event management

7.4.2 Specifications

The service's specifications are as follows:

Table 6: Specifications for “Managed middleware” service

Middleware	Distribution and version
Web server	▪ Apache server ▪ NGINX server ▪ IIS server
Proxy Server	▪ Squid server ▪ HaProxy server
Application server	▪ Tomcat server ▪ Microsoft IIS + ASP.NET ▪ PHP server ▪ SOLR server ▪ Web server + PHP server
DDI	▪ DNS server standalone ▪ DHCP server standalone
File server	▪ Samba server ▪ Microsoft File server ▪ Microsoft DFS server ▪ ProFTPD server ▪ CFT server
Manufacturing Operations And Management (MOM)	▪ Kafka ▪ Zookeeper ▪ RabbitMQ

7.4.3 Limitations

The following activities remain the Customer's responsibility:

- Verifying the proper operation of the middleware

- Performing business tasks dependent on the Customer application
- No client code review

7.4.4 Managed CFT

The "Managed CFT" service allows the Customer to exchange files via the protocols supported by CFT with one or up to 5 partners. This service is only available to Customers who have subscribed to the Managed OS service.

The offer includes:

- Integration of the CFT application with Windows or Linux servers.
- Deployment and validation of the licenses provided by the customer.
- Management and supervision of the deployed applications.
- The implementation of the necessary configuration to send/receive files.
- Management of patches and service packs installation for deployed CFT applications and their deployment frequency.
- Management of file transfer anomalies between the managed CFT application and the Axway Vision gateway.
- Deploy customer-provided certificates required for secure exchanges.

7.4.4.1 Prerequisites

This offer involves a mandatory analysis phase for:

- Validate the Customer environment, and the integration of the CFT application
- Validate the configurations provided by the Customer, in agreement with the partners (remote partners and Axway Vision gateway)
- Validate the implementation of the service and the proper functioning of the configuration deployed on the client side.

7.4.4.2 Description

The following table lists the services provided under the "Managed CFT" service:

Table 7: Description of the services "Managed CFT"

Phase	Activities
CFT Implementation	▪ Install and configure the CFT application for exchanges via the Axway Vision gateway. ▪ Test exchanges with the partner(s) ▪ Implement standard supervision of the application ▪ Validate compliance with security recommendations
CFT Operations	▪ Administer and maintain the CFT application ▪ Apply minor or major updates of patches and service packs. ▪ Manage antivirus security ▪ Supervise and analyze incident logs.

7.4.4.3 Limitations

- The Customer provides the license for the use of the CFT application in accordance with the subscription of its editor contract.
- The Customer is responsible for opening the flows.
- The remote third party(ies), partner(s) of the Customer, which are not managed by the Provider remain solely responsible for the proper reception of the files sent by the Customer.
- The GTR (Guaranteed Recovery Time) will be suspended in case of waiting for the return of the editor's support or the non-managed partner.

7.5 Managed container with CaaSCAD

The Managed Container service with CaaSCAD is an tthat allows you to delegate the container management of your applications.

The service consists of all or some of the following elements:

- The deployment of on-demand containers on managed Kubernetes clusters based on images, Dockerfiles and manifests provided by the Customer.

- 24 x 7 monitoring of the containers deployed in the Kubernetes clusters.
- Notification and intervention on incidents in the event of container malfunctions on the basis of procedures agreed with the Customer and formalized during the pre-sales phase.

On quotation, the Provider can provide container images (OS, and Middleware).

7.5.1 Description

The following table list the services provided as part of the "Managed container with CaaSCAD" service

Table 8: Description of « Managed container with CaaSCAD » service

Phase	Activities
Container Implementation	▪ Deploy containers on demand on managed Kubernetes clusters from images and deployment manifests provided by the customer and deposited in CaaSCAD directories and registries. ▪ Configure the supervision of containers on managed Kubernetes clusters.
Container Operation	▪ 24 x 7 supervision of containers deployed in Kubernetes clusters ▪ Creation of incident tickets, investigation and notification of the customer on incident. ▪ Redeployment of the current version N and N-1 of the containers from the images and manifests deposited in CaaSCAD*. ▪ Resizing of the quota allocated to containers at the POD level of the Kubernetes clusters*. ▪ Triggering support and troubleshooting of the Managed Kubernetes service in the event of a problem on the underlying Kubernetes cluster. ▪ Collection and storage of metrics and logs exported by Containers in the Managed K8S service with CaaSCAD. ▪ Access to metrics, logs and alerts of containers in the Managed kubertnetes service with CaaSCAD. ▪ Backup of the git containing the files linked to the containers in the Managed kubertnetes with CaaSCAD service.

(*) According to the procedures agreed by the Customer during the pre-sales phase.

Change requests (*) from the Client include:

- Redeployment of container versions on KKubernetes clusters from files stored in CaaSCAD tools
- The creation or modification of deployment chain routines in CaaSCAD tooling
- Verification of the proper functioning of the containers
- The modification of the export points of metrics and container logs
- The creation and modification of alerts in CaaSCAD dashboards.
- Adding or modifying exporters on containers, especially for application metrics.
- Creation and modification of reporting dashboards on metrics and logs in CaaSCAD tools.
- The structuring of the Git tools and the deployment chain (CD) for integration with the processes and the integration chain (CI) already used by the Customer.

(*) For an exhaustive list of changes, please refer to the exchange catalogue available in the Cloud Store portal.

7.5.2 Service requirements

- The Managed Kubernetes service with CaaSCAD ordered from the Provider
- Kubernetes clusters created, functional and managed by the Provider
- The provision by the Customer of Docker images, Dockerfiles, manifests, exporters sending metrics and logs and the deposit by the Customer in the CaaSCAD repository and registry.
- The validation by the Customer of the procedures to be applied on incident among the proposed procedures.

7.5.3 Limitations

The following activities remain the responsibility of the Customer:

- Updating container deployment files in CaaSCAD git
- Updating container images in the CaaSCAD repository
- Container application supervision
- Application performance commitments
- The commitments of good functioning between the containers and the Virtual Machine (VM)
- Stateful containers

7.6 Managed Kubernetes with CaasCad

The Kubernetes service managed with CaasCad is an the Provider service that allows the Customer to delegate the supervision and operation of the Kubernetes clusters used by its applications and to use the CaasCad tooling as a service for the operation of Kubernetes clusters, containers and containerized applications in DevOps mode.

The service consists of all or part of the following elements:

- The deployment of on-demand Kubernetes clusters on a Container as a Service infrastructure provided by the IaaS provider from configurations provided by the Customer.
- The 24 x 7 supervision and the maintenance in operational conditions of the deployed Kubernetes clusters.
- Notification and intervention on incidents to restore or rebuild from the repository in case of malfunctions of Kubernetes clusters.
- Restoring Kubernetes clusters from a repository saved in CaasCad
- The CaasCad as a Service tool for the operation of Kubernetes clusters, containers and containerized applications.
- Change management on Kubernetes clusters and CaasCad tools.

Table 9: Description of « Managed Kubernetes with CaaSCAD » service

Phase	Activites
Kubernetes Implementation	▪ Creation of Kubernetes cluster(s) with Docker Engine and ETCD ▪ Storage installation and configuration ▪ Configuration of the network, access services and associated security groups ▪ Installation and configuration of the supervision service ▪ Installation and configuration of the backup service
Kubernetes Operation	▪ 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 Request for change*	▪ Creation and destruction of a managed Kubernetes cluster ▪ Resizing the cluster or underlying nodes

* according to the Change Management Policy in Chapter 7.4.

7.6.1 Service Requirements

- The CaasCad service for the operation of Kubernetes clusters, containers and containerized applications.

7.6.2 Service specificities

There is no distinction of price whether the managed kubernetes cluster with CaasCad is in production or not

7.6.3 Limitations

The following activities remain the responsibility of the Customer:

- Provision of the specification of the characteristics of the managed Kubernetes cluster and its location
- Container and application management. To benefit from this service, the customer must subscribe to an extension at the Managed Container and Managed Application level.

7.7 CaasCad Service

The CaasCad service provides a DevOps-oriented operations tool for co-management by the Provider and the Customer on multiple clouds. The Caascad service is offered in two versions:

- Dedicated Caascad called "Caascad" which includes all the tools listed below and whose instances are dedicated by Customer
- Caascad Shared which is a limited version (see section Limitations of the Caascad Shared service) and shared between several Customers

This tooling includes:

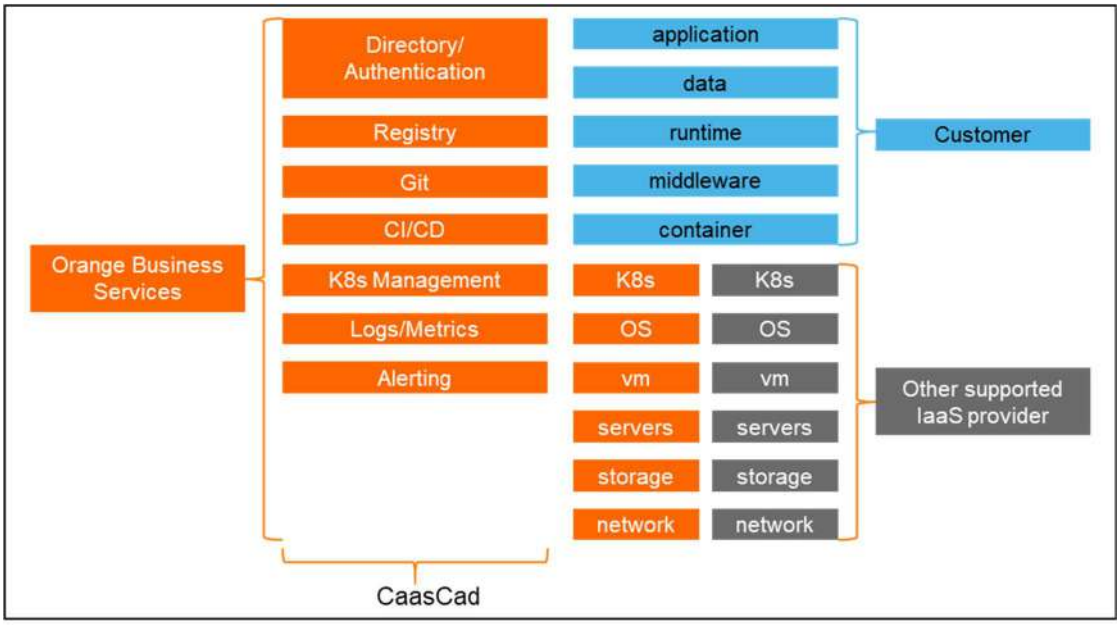
- a managed user directory and centralized authentication service

- a set of as-a-service managed tools to build, test and deploy applications in the managed Kubernetes cluster(s)
    - management of binary object repositories
    - GIT decentralized version management
    - Automation of builds/testing/deployment
- as-a-service managed tools for collecting, storing, and visualizing logs and metrics of infrastructures and applications
- an as-a-service application alerting managed tool configurable by the customer
- a portal summarizing the status of the system and facilitating navigation to the tools

This solution deploys and uses the services of the IaaS infrastructure of compatible service providers.

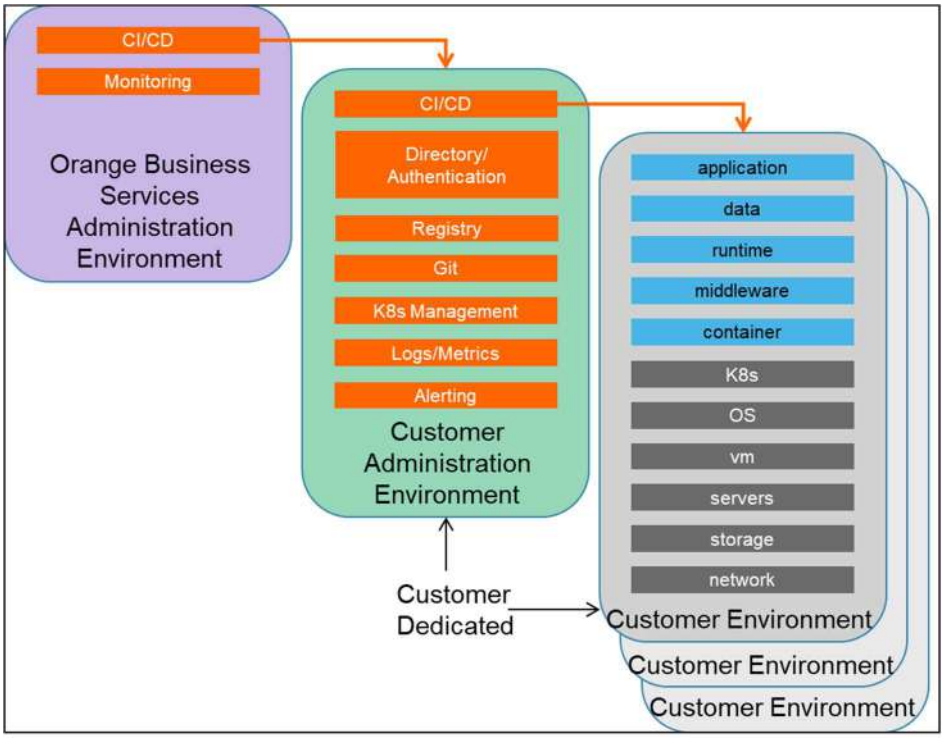
The following diagram represents :

- The Customer's containerized applications
- CaasCad services provided by the Provider
- The underlying Iaas services of the cloud provider



Responsibility matrix between Customer & the Provider

All the tools are open source tools deployed, integrated and maintained in operational conditions in an industrial way by the CaasCad Service. The following diagram describes the deployment model of the Service:



The different environments

7.7.1 Accès to the Service

7.7.1.1 Prerequisites

CaasCad services, Kubernetes Managed with CaasCad, Managed Container with CaasCad require mandatory governance with a Managed Services Manager.

The CaasCad Service is based on a supported IaaS and its services, which the Customer must subscribe to in advance with the third party cloud provider or the Provider. Cloud provider services are not part of the Service. In this context, the Customer and the Provider have Administrator rights on this Customer Environment.

IaaS supported :

- Flexible Engine from the Provider, Paris Region
- Cloud Container Engine (CCE) functionality is a prerequisite for the CaasCad service.
- The following Flexible Engine functionalities are also used (not exhaustive): ECS, EVS, CCE, VPC, NAT GTW, OSS, AK/SK.

The CaasCad Service requires a Kubernetes cluster in the managed client:

- An ECS s3.large.2 (2 vCPU/ 4GB RAM) with a data volume of 150G
- A t2.small ECS (1 vCPU/ 2GB RAM) with a public IP address
- A NAT gateway with an IP address

These elements that the Provider may determine changes over time to accommodate new features where changing performance requirements are not included in CaasCad pricing.

The CaasCad Service deploys probes in the Customer's Kubernetes clusters for administration and monitoring purposes, these probes consume a fraction of the computing power of the clusters.

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

The CaasCad service requires among others

- an Internet connection for the Administration Environment, used for updating the open-source software used in CaasCad.
- a connection from each Client Environment to the CaasCad Administration Environment, used for cluster administration.

- User access to CaasCad service URLs.

For incident investigation purposes, Customer authorizes the Provider to access the logs and metrics stored in CaasCad.

Customer must provide prior to installation and deployment:

- the list of "login" and "email" users authorized to access the Service
- the list of "login" and "email" users authorized to access Support (Incidents / Changes)
- the desired configuration of the managed Kubernetes cluster
- Log and metrics configuration retention periods.

7.7.1.2 Geographic location

CaasCad is deployed on the Provider' Flexible Engine infrastructure in the Paris Region with two Availability Zones located in St Denis and Pantin. The evolution of the CaasCad service is planned in an agile roadmap and includes compatibility with other cloud service providers.

7.7.1.3 URLs and CaasCad Portal

The various functionalities of the CaasCad Service are accessible through web service URLs that will be provided following the On-boarding phase.
One of them is the URL of the CaasCad portal providing a home page and navigation to other tools in SSO mode.
This Portal is hosted on the Customer Administration Environment.
The URLs and IP are public.

7.7.2 Support Services for CaasCad service

7.7.2.1 On-boarding

An On-boarding package of 3 consecutive days is provided at the initialization of the Service, which includes the creation of the Customer Administration Environment, the registration in the Identity Provider of the users authorized to the Service, the creation of the Kubernetes cluster and the provision of the access urls to the Service, the declaration of the named users in the Support ticketing system as well as the support of the Customer by an expert on the configuration and the use of the Service.
The service is renewed for the deployment of each Customer Administration Environment.
An additional service can be ordered by the Customer.

7.7.2.2 Cloud Expert Services

The Provider' Cloud Expert Services offer a catalog of DevOps expertise services to complement the CaasCad service.

7.7.3 User Directory and centralized authentication

The Service provides an Identity Provider (IdP) in order to authorize or limit user access to the Service. The set of Customer users authorized to use the Service is defined within the Identity Provider (IdP). The IdP allows the management of users, groups and associated roles.

Users can change passwords through self-service. All access to the Service tools is authenticated by the Identity Provider. The user has a Single Sign-On connection to access CaasCad tools.

The directory and the authentication service are hosted on the Customer Administration Environment.

During On-boarding, as standard, all users are placed by the Provider in the same group with the same maximum rights allocated to all Service tools based on the list of users and associated emails provided by the Customer.

7.7.3.1 Description

Phase	Activities
Directory / SSO Implementation	▪ Keycloak ○ keycloak.ocb-Projet.CaasCad.com
Directory / SSO Operation	▪ Minor and major updates ▪ Security management (updates, access control) ▪ Service supervision 24/7 ▪ Event management ▪ Log management

Phase	Activities
Directory / SSO Request for change*	▪ creation of groups and roles to refine rights ▪ creating or deleting users after On-boarding

* according to the Change Management Policy in Chapter 7.4.

7.7.3.2 Limitations

The following activities remain the responsibility of the Customer:

- Definition and change of password
- Provision of the list of users and associated emails

7.7.4 Kubernetes cluster inventory service

The Service provides an inventory and visualization tool of the status of Kubernetes clusters to allow the Customer to know the details of the container deployments in the clusters. This service is based on the Rancher utility available in read-only mode for the user. The Rancher component carries the authorization of the users on the Kubernetes clusters, the authentication is managed by the IDP.

7.7.4.1 Description

Phase	Activité
Build / Registry Implementation	▪ Dépôt de code : Gitea ○ git.ocb-Projet.CaasCad.com ▪ Build: Concourse ○ ci.ocb-Projet.CaasCad.com ▪ Registry: Quay ▪ Docker.ocb-Projet.CaasCad.com
Build / Registry Operation	▪ Minor or major updates ▪ Security management (updates, access control) ▪ Service supervision 24/7 ▪ Event management ▪ Log management

7.7.4.2 Limitations

The following activities remain the responsibility of the Customer:

- Provision of the specification of the characteristics of the managed Kubernetes clusters and their location by exchange of mail or constituted file.
- Management of its application code
- Container Deployment Management integrating application updates

7.7.5 Code Repository, Build Chain and Application Container Storage

The Service provides a code repository (git) to allow Customer to manage its code by itself. The Customer is free to organize his code as he wishes. This service is dedicated to the Customer and uses resources from the Customer Administration Environment.
The Provider team is the administrator of this service and also uses it for operations on the Customer Environment(s). Dedicated repositories are made available for the generation and maintenance of Grafana dashboards and Prometheus alerts (see Collection, storage, visualization of logs and metrics).

The Service provides a Continuous Integration (CI) tool to allow the Customer to create its containerized applications (build, test and packaging). Work is organized in a pipeline to automate tasks. The CI tool enables the Customer to perform the usual tasks of Build (compilation, script execution), testing (unitary, functional, integration, loading) and packaging (Docker). The Customer is free to configure the pipelines he wants.
The IC is installed in the Customer Administration Environment. The IC agent is installed in the Customer Environment and the jobs managed by the IC are performed in the Customer Environment.

The Service provides a Docker Registry to allow the Customer to store all of its application images. This service is dedicated to the Customer and uses resources from the Customer Administration Environment.

The Provider team has administrator rights on all of these tools. Access is authenticated and centralized through the Identity Provider (IdP) service, in SSO.

By default, following On-boarding, all users have the maximum rights available (excluding the administrator).

7.7.5.1 Description

Phase	Activities
Build / Registry Implementation	▪ Code deposit : Gitea ○ git.ocb-Project.CaasCad.com ▪ Build: Concourse ○ ci.ocb-Project.CaasCad.com ▪ Registry: Quay ○ Docker.ocb-Project.CaasCad.com
Build / Registry Operation	▪ Minor or major updates ▪ Security management (updates, access control) ▪ Service supervision 24/7 ▪ Event management ▪ Log management

7.7.5.2 Limitations

The following activities remain the responsibility of the Customer:

- Updating of the application code and storage in the code repository
- Control of the Build chain
- Deployment of applications on Kubernetes clusters

7.7.6 Application secrets manager

The Service provides a secret manager (Vault by Hashicorp) that allows the Customer to manage its own application secrets.

The integration of Vault into the Caascad service provides a generic secret organization model to cover a maximum of use cases:

- access by all applications on all clusters
- access by applications of a particular namespace on all clusters
- access by all applications on a particular cluster
- access by applications of a particular namespace on a particular cluster

Deployment of the Vault Injector component is required for applications that do not natively integrate with the Vault Secret Manager. The Vault Injector component is deployed by the Service Provider's team at the Customer's request in the environments of their choice.

The Service Provider's team has administrator rights to the secret manager. The access is done in an authenticated and centralized way through the Identity Provider (IdP) service, in SSO.

7.7.6.1 Description

Phase	Activities
Build / Registry Implémentation	▪ Secret Manager : Vault ○ Vault.ocb-Projet.caascad.com
Build / Registry Operation	▪ Minor or major updates ▪ Security management (updates, access control) ▪ 24/7 service monitoring ▪ Event management ▪ Log management

7.7.6.2 Limitations

The following activities remain the responsibility of the Customer:

- Updating application secrets
- Adding annotations in the application manifests to allow the recovery of secrets

7.7.7 Collecting, storing, viewing logs and metrics

The Service provides for each managed Kubernetes cluster, a metrics collection service (based on Prometheus) and logs (based on Promtail). These collection services are installed, configured and managed by the Provider.

Upon installation, these services are configured to collect:

- All metrics provided by Kubernetes components (node-exporter, cAdvisor)

- Logs of all applications running in the Kubernetes cluster and logging at standard and/or error output
- Logs of all components running on the Kubernetes cluster nodes

The Provider provides the Customer with a way to define additional endpoints for collecting application metrics. They are defined in the Code Repository and must be deployed by the Customer in the Kubernetes cluster to be taken into account.

The Collection Services retrieve, process and store the metrics and logs from each managed Kubernetes cluster centrally in the Customer Administration Environment.

For log processing and storage, the collection service uses the Loki tool that consumes the IaaS S3 service as a long-term storage back-end.

For metrics, the collection service uses the Thanos tool, which also consumes the S3 service of the IaaS as a long-term storage back-end.

The retention periods for logs and metrics are defined during On-boarding. Thereafter, the Customer can request a change to modify them. (Cf Change Management)

The Service provides a managed tool for viewing metrics and logs (Grafana). The visualization tool is configured by default with a set of dashboards and allows the Customer to configure its own dashboards.

7.7.7.1 Description

Phase	Activities
Logs/Métrics **Implementation**	▪ Installation and configuration of collection services ▪ Installation and configuration of processing and long-term storage services ▪ Retention configuration ▪ Installation and configuration of the visualization service ○ grafana.ocb-Project.CaasCad.com ▪ Added default dashboards
Logs/Metrics **Operation**	▪ Administration of services ▪ Minor or major updates ▪ Security management (updates, access control) ▪ Service supervision 24/7 ▪ Event management ▪ Log management
Deployment **Request for change***	▪ Change in metric retention period (global) ▪ Modification of the log retention period (global)

* according to the Change Management Policy in Chapter 7.4.

7.7.7.2 Limitations

The following activities remain the responsibility of the Customer:
- Specification of endpoints for collection of application metrics
- Configuration of metric and log collectors through the code repository
- Configuration of the Grafana dashboards specific to the customer applications through the code repository

7.7.8 Collecting, storing and viewing VM metrics

For each Customer environment, the Service Provider provides the Customer with a way to define endpoints for collecting application metrics from virtual machines. The informations on the VMs application exporters are defined by the Customer in the Code Repository and are deployed through the Provider's automatic CI/CD pipelines.

The metrics collection services from the virtual machines retrieve, process and store the metrics in a centralized manner in the Customer Administration Environment.

The retention periods for VM metrics are the same as those for managed cluster metrics.

7.7.8.1 Description

Phase	Activities
Metrics **Implementation**	▪ Installation and configuration of collection services ▪ Installation and configuration of processing and long-term storage services ▪ Installation and configuration of CI/CD pipelines

Phase	Activities
Metrics **Operation**	▪ Collection Services Administration ▪ Pipeline updates ▪ Security management (updates, access control) ▪ 24/7 service monitoring ▪ Event management ▪ Log management

7.7.8.2 Limitations

The following activities remain under the responsibility of the Customer:

- Installation of OS/application exporters on virtual machines
- Specification of the endpoints to collect OS/application metrics
- Opening network flows between the managed clusters and the monitored virtual machines
- Configuration of the dashboards of the applications installed on these VMs

7.7.9 Alerting

This Alerting service allows the Customer to:

- Manage its own set of alerting rules based on the collected application metrics
- View alerts set up by the Provider by default
- View the status of alerts in real time via the managed tool Karma

7.7.9.1 Description

Phase	Activities
Alerting **Implementation**	▪ Installation and configuration of the service ▪ Default alert configuration ▪ Viewing alerts ○ karma.ocb-Project.CaasCad.com
Alerting **Operation**	▪ Administration of services ▪ Minor or major updates ▪ Security management (updates, access control) ▪ Service supervision 24/7 ▪ Event management ▪ Log management

7.7.9.2 Limitations

The following activities remain the responsibility of the Customer:

- Configuration of application alerts and the Karma tool through the code repository
- Saving the alert configuration in the code repository

7.7.10 Backup and Restore

The GIT code repository is backed up daily. These backups are kept for 7 days, then a weekly backup is kept for an additional month in the Customer Administration Environment.

The configuration elements of all the Service tools (dashboards, alerts, etc.) must be stored by the Customer in the code repository in order to be backed up and preserved during updates and incidents.

The backups of the code repository are exclusively provided for the restoration of the Service by the Provider in the event of an Incident. The Service restoration mechanism consists of restoring the GIT repository from the backup and redeploying the tools and their configuration from the restored repository.

Logs and metrics are stored in the standard Object Storage of the Customer Administration Environment. They are not replicated or backed up additionally.

7.7.10.1 Description

Phase	Activities
Git Code Repository Backup **Implementation**	▪ Installation and configuration of the code repository backup

Phase	Activities
Git Code Repository Backup **Operation**	▪ Administration of services ▪ Minor or major updates ▪ Security management (updates, access control) ▪ Service supervision 24/7 ▪ Event management ▪ Log management

Phase	Activities
Restoration of Code Git repository and service on incident **Implementation**	▪ Restoration of the code repository from version N-1 onwards ▪ Redeployment of Service tools from the code repository
Restoration of Git Code Deposit and Service on demand **Request for change***	▪ Context of a change request from the Customer ▪ Restoring the code repository from the desired saved version ▪ Redeployment of Service tools from the code repository

* according to the Change Management Policy in Chapter 7.4.

7.7.10.2 Limitations

Configurations made by the Customer on all the tools and collectors of the Service other than through the code repository are not saved. They are therefore lost when the Service is restarted following an incident or update.

7.7.11 Specifics of CaasCad Service Updates

The Provider does not provide software development services or feature patches on open source software deployed for the Service. The Provider uses the evolutions updated by the opensource community. The so-called "minor" updates and security patches will be automatically deployed without Customer notification.

The major updates will be notified to the Customer with a notice period of 2 weeks before going into production. The Provider will inform the Customer of the end of support for obsolete versions.

The application of the major updates will be the subject of a service invoiced to the Customer.

The Provider ensures the traceability of all interventions in production thanks to an operating tool used by the Customer Support Center. This data is kept by the Provider for the duration of the Agreement and is deemed authentic between the Provider and the Customer.

7.7.12 CaasCad Service Limitations

The Managed Application Reporting Service does not apply to CaasCad.

The Managed Application Antivirus Service does not apply to the CaasCad service that does not manage servers.

The CaasCad Service does not include IaaS and Customer Environment services that Customer must purchase separately from the IaaS provider at its then current rates.

7.7.13 Limitations of the Caascad Shared service

The following features do not apply to Caascad Shared

- Code repository, build chain and container storage
- Log and metrics collection, storage and visualization
- VMs metrics collection, storage and visualization
- Alerting
- Backup and restore (GIT)
- Secret management
- Self-service user management in the centralized directory

To get the full Caascad service, the customer must migrate from the "shared" offer to the "dedicated" offer. This migration is possible at any time at Customer request.

7.8 Managed application

The “Managed Application” management level makes it possible to provide the Customer with the following services:

- Application server installation
- Application operation and administration
- Reporting and application statistics
- Application supervision
- Application back-up

The Provider can take on responsibility for all customer application management tasks, as an additional service, giving rise to a separate estimate.

7.8.1 Managed business application

The Provider will provide the following services:

- Production environment maintenance,
- =Application management in other environments (interaction between different environments, such as development, integration, etc.)
- Application management with dependencies connected to other environments (interaction between different environments such as development, integration, etc.

The Provider defines a complexity coefficient depending on the criteria below. These criteria are taken into account to produce the quotation.

- Number of users,
- Application maturity,
- Party in charge of release management
- Number of interfaces with other applications,
- Number of servers.

By drawing upon the application functioning thresholds set with the Customer, the administrators may diagnose a problem and advise the Customer on corrective action.

The functioning thresholds are determined with the Customer from the very deployment of the customer application management service. However, the components subject to proactive monitoring are enhanced throughout the customer application’s life cycle, as it is by tracking them day-by-day that the administrators become familiar with the Customer's applications and their behaviours.

7.8.2 Managed SAP

SAP managed services aim at either setting up a new SAP application or migrating an existing SAP application for the Customer and operating the corresponding Environments.

7.8.2.1 The service phases

For each SAP application, the Customer must subscribe “SAP run” activities and either “SAP setup” or “SAP migration”.

Table 10: Description of « Managed SAP » service

Phase	Deliverables
SAP setup	▪ A project management phase delivering: ○ Collecting customer needs ○ Sharing the transition plan and methodology with the Customer ○ Architecture and sizing ○ Test plan ▪ Validation of installation and test plans with the customer ▪ Setting up an infrastructure platform ▪ Installation of SAP applications and databases ▪ Verification and reporting phase ▪ All documents necessary for the Customer's use of the Service (e. g. user guide)

Phase	Deliverables
SAP migration	▪ A project management phase delivering: o Collecting customer needs o Migration plan o Data migration plan o Test plan ▪ Validation of migration and test plans with the customer ▪ Setting up an infrastructure platform ▪ Migration of SAP applications and databases ▪ Verification and reporting phase ▪ All documents necessary for the Customer's use of the Service (e. g. user guide)
SAP run Operating activities	▪ Incident management ▪ Performance Management ▪ Management of recurring change requests (configuration, database patches, kernel updates, transport, EWA) ▪ Backup and recovery management (including cloning for refreshing and managing backup policies) ▪ Management of package supports ▪ Database management (tablespaces, reorganization, refreshes, indexes...) ▪ Printer management (in SAP) ▪ Client management (creation, copying, deletion) ▪ Transport management (routes, system, EO) ▪ Creation of market place messages (technical problems) ▪ Application of OSS scores (technical) ▪ EWA analysis ▪ Analysis of daily reports ▪ Technical acceptance tests
SAP run Follow-up activities	▪ A reporting portal (GUI) ▪ Alerts - information, settings ▪ Response times - low, medium, high, high, extreme ▪ Engine - ok / nok ▪ External alerts - snmp ▪ Track tablespaces, database activity, backups, SAP events, batch work, SAP spools, blocking entries, SAP queues, SAP logs, updates. ▪ Monthly reports
SAP run Infrastructure management activities	▪ Database management ▪ Operating system and virtual machine management ▪ Storage and backup management

7.8.2.2 SAP Hana Trial

The Service offers two SAP Hana Trial test scenarios to allow the Customer to test the use cases before going into production or in parallel with the production workload. The options are "Prototyping" and "Sandbox":

- Prototyping allows you to test a new application
- Sandbox is intended to test the evolutions of an existing SAP application.

Assistance is provided during working days and French business hours (9am-6pm).

- ***SAP Prototyping***

In this scenario, the Provider creates a new environment, based on the Customer's needs.
The Service includes the implementation of an application platform for the Customer according to his needs. The customer's needs must be described beforehand during configuration.
The Service includes the following deliverables:

- Access to a technical platform containing all the applications and specificities agreed at the Client's request (The Prototype)
- All documents necessary for the client's use of the Service (e. g. user guide)

- ***SAP sandbox***

In this scenario, the Provider replicates an existing Environment provided by the Customer into a dedicated Sandbox Environment.

The service includes configuring a SAP sandbox environment based on SAP HANA® for the customer. All documentation allowing the installation and settings of the application must be provided by the Customer.

The Service includes the following deliverables:

- Access to a technical platform containing all applications and data provided by the Client (the Testing Environment)
- All documents necessary for the client's use of the Service (e. g. user guide)

7.8.2.3 Specifications

The following tables list the applications provided as part of the "SAP Managed" services

Table 11: Description of "SAP Managed" applications

SAP services	Application
Business Suite, S4	▪ ECC ▪ CRM ▪ SRM ▪ SCM ▪ PLM / S4
Application Server	▪ AS ▪ CI ▪ PAS
BO-BI	▪ BusinessObjects BI
BW (abap & java)	▪ Business Information WH
APO & Live Cache	▪ Advanced Planner/Opt & Live Cache
APO Optimizer	▪ Advanced Planner and Optimizer
GRC	▪ Governance ▪ Risk ▪ Compliance
Solman (technical)	▪ Solution Manager – Technical
BC	▪ Business Connector
BFC	▪ BO Financial Consolidation
BPC	▪ BO Financial Consolidation
Solman (ChaRM)	▪ Solution Managed – ChaRM
Portal	▪ Technical, no apps
HCM	▪ Human Capital Management
T-REX	▪ Text Retrieval and Info Extraction
ADS	▪ Adobe Document Service
Webdispatcher	▪ Webdispacher
Content Server	▪ Content Server
BW (abap)	▪ Business Information Warehouse

SAP services	Application
PI	▪ Process Integration
WECM	▪ Web Channel Experience Management

7.8.2.4 Limitations

The following activities remain the responsibility of the Client:

- Verification of the proper functioning of the SAP application
- Make the decision to restore the database or environments
- Perform sales tasks based on the customer application

Project management services or professional services, unless otherwise specified in the technical and financial proposal, are not included in the service.

7.8.3 Non-production environments

The Customer may subscribe to Non-Production Service Units in addition to its Production Service Units, under the conditions specified in the Fee Schedule. The Customer's non-production environments will be installed by default in the same Tenant as the one of its production.

A service of management of nonproduction environments can be included, on quotation, in the service of the Managed Service Manager. It may cover, according to the Technical and Financial Proposal, all or part of the following services:

- Centralize deliveries and validate deliverables
- Industrialize the installations in such a way as to facilitate and secure production start-ups
- Test the installations and application in an environment equivalent to production
- Provide advice and assistance to the Customer on deliverables related to new versions, processes, and possibly on some technical choices

7.8.4 Description

The following table lists the services provided as part of the "Managed Application" services.

Table 12: Description of "Managed Application

Phase	Activities
Business Application Implementation	▪ Install and configure website ▪ Install and configure Client application ▪ Compliance with safety recommendations
Business Application Operation	▪ Administer and maintain the configuration ▪ Backup and recovery services ▪ Event management

7.8.5 Limitations

The following activities remain the responsibility of the Client:

- provisionning of a documentation for installation and configuration of the application
- verification of the proper functioning of the application
- provisionning of procedures for the management and operation of the application
- decision to restore the application
- business tasks depending on the Client's application

7.9 Native Hyperscaler Services

7.9.1 Managed and Co-Managed Services Strategy

The Provider can support Customers in 3 different ways in their use of the Cloud.

1. The Fully Managed model is a model in which the Service Provider is responsible for the deployment, monitoring and operation of the Customer's application scope. The Customer is responsible for providing a fully tested functional environment.

2. The "Co-Managed" model is a model in which the Customer and the Service Provider share the responsibilities of deployment, monitoring and operation of applications and workloads. In this model, the Customer takes responsibility for the development and testing of its application(s). The Customer may propose deployment procedures based on its own change processes. The Service Provider is responsible for 24x7 monitoring and maintenance including non-working hours and days and/or 8x5 for less critical workloads. The Provider and the Customer collaborate using a Git repository, a continuous integration and deployment chain (CI/CD) and shared tools for monitoring, logging, alerts, dashboards and communication. The Provider can offer in this model, via a specific contract, a Cloud Center of Excellence or Expertise.

3. The "Full DevOps" model is a model in which the Customer's development team is fully responsible for the development, deployment, monitoring and operation of the Workload. In this model, the Provider may offer professional services to the Customer, via a specific contract, in the form of a Cloud Center of Excellence or Expertise to help the Customer set up DevOps pipelines, tooling, landing zone and Build to Run activity. In this model, no managed services are offered.

The Service Provider's service commitment applies to both Fully Managed and Co-Managed models. During the pre-sales or consulting phase, the Client and the Service Provider will agree on the required managed services model and adapt the RACI accordingly if necessary.

7.9.2 Service Description

The Provider provides technical operation and monitoring of the Customer's AWS, Azure or GCP Native Services, as well as optimization and upgrade activities through the implementation of a network interconnection between the Provider's "service area" and the Provider's Cloud Platform.

At the beginning of the Client project:

- An audit is required to determine the inventory of resources to be managed, their Transition Class, the scope of work remaining to be completed to be ready for operation, the RACI and the limitations of the service to be managed.
- The construction of a landing zone is required. Infrastructure deployment is modeled as Infrastructure as Code (IaC) for quality, repeatability and disaster recovery. Native Services, AWS, Azure or GCP are deployed using this IaC.

The definition of Transition Classes for resources to be transferred and then managed by the Provider are specified in the AWS, Azure or GCP Technical Annex.

The rates listed in the AWS, Azure or GCP Native Services pricing sheet are for the service delivered by the Provider only. Pricing for the IaaS resources of the relevant hyperscalers are not included in the Service Provider's service, and appear on the Customer's IaaS invoice.

The price of the services referred to in this paragraph and applicable to the Customer is calculated by taking into account the following elements

- The number of Native Service Units managed or for which the managed service is subscribed after validation with the Customer through a HLD (High Level Design). The Service Provider's service and price commitment is based on the native services indicated in the HLD as well as the underlying micro services, middleware, application, database.
- The Transition Class applied, following the inventory of the resources to be managed, that the Provider will perform during the audit. For some services, the Provider's responsibility may be limited to the maintenance of the IaC and the management of changes only, or may include the supervision.
- SRE (Site Reliability Engineering), which corresponds to the maintenance of the infrastructure as code or to a proactive recommendation for improvement of the IaC by the Provider. An SRE share is included as standard in the Managed Service operated by the Service Provider, a provision is provided beyond that which will be invoiced as a controlled expense by the Customer.
- The support chain used:
    - Standard" via our support chain located in Cairo for the L0/L1 service desk
    - Full France", in which the Customer can have a Full France channel or a Full France channel with reinforced security, via our support channel located in France. The incidentology (number of monthly tickets L0/L1) will be defined with the Customer and the Service Provider according to its needs.
- The number of days related to governance via :
    - the Managed Services Manager for the monitoring of monthly kpi/reporting,
    - the Managed Contracts Manager for contractual follow-up and billing.
- The number of managed tenant(s) that host(s) the Customer's environment, administered and supervised by the Provider's teams,

- The number of token(s) per unit or per pack subscribed by the Customer for the "change management " necessary to the starting of the Customer project or in life of solution.

6.9.2.1 Description

The following table lists the services provided as part of the "Native Hyperscaler Services":

Table 13: Description "Native Hyperscaler Services"

Phase	Activities
Native Hyperscalers Services Implementation Phase	▪ Review and validation of the RACI of the Azure, AWS or GCP Customer's application services by the Service Provider ▪ Creation of the infrastructure as code: according to the transition class ▪ Review and adjustment of the reflex cards (MOP on incident) provided by the Customer's company to the Service Provider (When applicable in transition where the Customer's environment exists and in case of managed applications) ▪ Takeover and/or elaboration of the documentation for the use of the Provider's teams ▪ Co-definition and/or revision of alarms and application thresholds ▪ Creation of accesses for the Provider's administrators ▪ Configuration of the VPN operation (if necessary) ▪ Configuration and testing of alarms in the Provider's centralized monitoring system ▪ Training Customers on the Cloud Store for access to change/incident requests.
Native Hyperscalers Services Operation Phase	▪ Supervision and operation o Reading and analysis of alarms o Maintenance of the IaC (excluding changes) according to the transition class o Correction of faulty configurations o Joint review and update of security groups and access controls o Event management (changes & incidents) and interfacing with Azure, AWS or GCP support if necessary and application operations o Supervision of the service 24/7

7.9.3 Spécifications

The Provider provides operation/supervision and foreign exchange management of the Native Services mentioned in the attached list. All the Native Services not present in the list available via the following url will be treated as a customized offer by the Provider's teams.

6.9.3.1 Managed Service on Azure

Table 14: « Azure Native Services » Service Specifications

The list of Azure Native Services is available at the link:

- ✓ https://cloud.orange-business.com/wp-content/uploads/2021/10/managed-applications-list-of-supported-native-services.pdf

6.9.3.2 Managed Service on AWS

Table 15: « AWS Native Services » Service Specifications

The list of AWS Native Services is available at the link:

- ✓ https://cloud.orange-business.com/wp-content/uploads/2021/10/managed-applications-list-of-supported-native-services.pdf

6.9.3.3 Managed Service on GCP

Table 16: « GCP Native Services » Service Specifications

The list of GCP Native Services is available at the link:

- ✓ https://cloud.orange-business.com/wp-content/uploads/2021/10/managed-applications-list-of-supported-native-services.pdf

7.9.4 Prerequisite

To benefit from the various "Native Hyperscaler Services" the prerequisites are as follows:

- Customer must have defined an HLD compliant architecture. (Provider may optionally provide professional services for architecture definition).
- Customer must have a subscription, resources, and support level to an Azure, AWS, or GCP account. Subscription and IaaS resources are not included here, the Provider may provide this subscription via a specific contract.

- ❖ The Customer must create at least one VPC (Virtual Private Cloud) at its Cloud provider or give the means of delegation to the Provider.
- ❖ The Customer must create as many accounts as necessary for the Provider's administrators as defined during the audit phase,
- ❖ The Customer must set up a network interconnection between the Azure, AWS or GCP platform and the Service Provider's service area. The connection may be simplified when the Provider does not provide a managed operating system, middleware and application and native Azure, AWS or GCP tools are used (to be determined in the Pre-Sales phase).
- ❖ Customer's platform must be urbanized according to Azure, AWS or GCP landing zone best practices,
- ❖ The Customer must have a precise inventory of the resources to be operated by the Service Provider: micro services, middleware, applications, databases, ..., so that the transition perimeter and the list of services to be managed can be established by the Service Provider teams.
- ❖ The Provider will apply by default its standard RACI. A RACI between the Provider and the Customer can be established beforehand if there are Customer specificities to take into account.
- ❖ The Customer and the Provider must agree on the tooling used for GIT, the CI / CD chain, the monitoring, logging and alerting solution.

7.10 Log As A Service (LaaS)

The Log As A Service managed with ECE (Elastic Cloud Enterprise) components is an Provider Service. It is a complete end-to-end log analysis solution that helps in deep search, analysis and visualization of logs generated by different machines.

The service consists of all or part of the following elements:

- A secure administration platform, shared by all Clients, instantiated within the Log As A Service platform
- The instantiation of the Clients in the secure shared Allocators,
- Elastic license management provided by the Provider
- The 24 x 7 supervision of the deployed Elastic clusters
- Installation and maintenance in operational conditions of all or part of the components (Kafka, Logstash, APM, Machine Learning, Kibana) for the Customer
- The implementation of the following services on estimate:
  - Customized data collection for :
    - The addition of new data sources in your Elastic cluster
    - The accompaniment in the update of the architecture (addition of node) if needed according to the volume of data added
    - The creation of custom dashboards for the creation of dashboards adapted to the use of the Customer
  - Deployment of machine learning for the customer
  - Coaching on the use of Elastic and the solution for the Customer's teams on the use of the Elastic suite

7.10.1 Description

The following table lists the services provided as part of the "Log As A Service" service:

Table 17: Description «Log As A Service»

Phase	Activities
Log As A Service Implementation Phase	▪ Installation of the ECE platform ▪ Creation of Elastic Cluster ▪ Adding Allocator(s) on the ECE platform ▪ Snapshot Configuration ▪ Restore Snapshot data ▪ Supply and Installation of licenses on the Customer environment ▪ Provision of an Elastic version on the ECE platform according to Elastic recommendations ▪ Installation of Logstash and KafKa options ▪ Installation/configuration of LDAP ▪ Deployment of Machine Learning nodes in the Customer cluster

Phase	Activities
Log As A Service **Operation Phase**	▪ Administration of the ECE platform (IaaS + Software) ▪ Update of Elastic Clusters versions ▪ Administration of installed services ▪ Minor or major upgrades ▪ Supervision and Operation o Alarm reporting and analysis o Correction of faulty configurations o Security management (updates, access control) and platform compliance o Event management (changes & incidents) o Log management o Supervision of the service 24/7

7.10.2 Limitations

To benefit from the various "Log As A Service" services, the Customer must perform the following actions:

- Adding logs to the cluster, creating indexes, managing Kibana spaces, managing users and roles, querying logs, reading access logs, creating a lifecycle policy, creating "beats" pipelines, creating a dashboard on Kibana,
- Installation and configuration of a software/agent on the application servers to transfer the logs to the ECE cluster using for example filebeats and https protocol
- Installation of Beats for data injection.

7.11 Managed Big Data

Managed Big Data is a service that allows customers to generate value from their business data (such as predictive maintenance, fraud detection or customer knowledge).

This service is composed of different solutions that are all managed by the Provider (Infrastructure and Big Data Components). These solutions work with the same philosophy: Collect data in batch or streaming mode, Store data, process the data and visualize data.

The service consists of all or part of the following elements:

- A secured administration portal provided with the Big Data platform,
- A dedicated tenant to ingest, store, process and visualize the Customer data,
- A 24 x 7 monitoring and alerting solution,
- /Installation, configuration and RUN (maintenance in operational conditions) of the Big Data solutions components by the Provider,
- The implementation by the Provider of the following services on quote:
  - Data and security Assessment and Architecture proposal,
  - Migration from an existing Big Data solution to the Provider environment,
  - Development of business use cases with the internal partners of the Provider,

The following Big Data software solutions are proposed and managed by the Provider. Each solution can be selected depending on customer needs (see next chapters for more details):

- Big Data with Cloudera CDP / CDF
- Big Data native services with Flexible Engine
- Big Data native services with Google GCP
- Big Data native services with Microsoft Azure
- Big Data native services with Amazon AWS.

For the Big Data Services proposed in self-service by the public Cloud Provider (Flexible Engine, GCP, Azure and AWS), the Provider manage for the Customer the infrastructure and the Big Data components.

7.11.1 Access to the Service

6.11.1.1 Prerequisite

- The Managed Big Data Service is based on a supported IaaS and its services, which the Customer must subscribe to in advance with the third-party cloud provider or the Provider. IaaS services are not part of the Service.
- The Customer shall subscribe necessary network access to the IaaS Service.
- Big Data native services from Public Cloud provider (FE, GCP, Azure and AWS) can only run on each IaaS
- The Tenant subscribed by the Customer is a Managed Tenant, administered by the Provider.
- For Big Data with Cloudera, Cloudera CDP/CDF software licenses must be purchased by the Customer from the Provider.

The following phases are optional to the service: Data and security Assessment and Migration.
The following phases are mandatory to the service: Installation, configuration, operation, supervision, monitoring, backup and change management.

The following chart lists the services supplied as part of the "Managed Big Data" services:

Table 18: Description of "Optional Managed Big Data services"

Phase	Activities
Data and security Assessment	**A project management phase managed by the Provider to** ▪ Drive workshops, ▪ Define scope of work, ▪ Evaluate Customer data and jobs, ▪ Assess data policies and network prerequisites **Evaluation of ETL Data** ▪ Purpose of data ▪ Volumetry, criticality of the flow ▪ Description of treatments ▪ Location and format of original data **Evaluation of security constraints** ▪ Data Confidentiality and sensitivity ▪ IAM organization roles ▪ VPN or interconnection solution
Migration	**A project management phase managed by the Provider to** ▪ Manage the migration from an existing Big Data solution to the Provider environment, ▪ Prerequisites: The Data and security Assessment phase has to be done **Collect customer needs** **Definition of the functional and technical architecture (macro and detailed)** **Establish the migration plan and test plan considering** ▪ The integration of existing database assets and structures ▪ Security and encryption ▪ The actual pipelines and workloads **Operate the migration** ▪ Install and configure the Big Data solution (detailed in next sections) ▪ Configure the Customer pipeline ▪ Migration the Customer data and workloads ▪ Test the migration

Table 19: Description of "Managed Big Data services"

Phase	Activities
Installation	**Installation tasks under the Provider's responsibility** ▪ Sizing definition, ▪ Big Data Software (including VM provisionning) ▪ ITSM software installation ▪ Cloudera CDP/CDF, Software licenses installation Depending on the complexity and size of the clusters, Big Data experts (junior/senior) will carry out the installation. **Installation tasks requested by the Customer and carried out the Provider** ▪ Additional VMs to run applications
Configuration	**Configuration tasks under the Provider's responsibility** ▪ Creation of initial user accounts and roles policies ▪ Configuration of the monitoring and supervision ▪ For "Big Data native services with Flexible Engine", when the "Advanced Security" option is subscribed, configuration of the Environment to use Kerberos and/or LDAP for authentication of users ▪ Configure the security policies ▪ Install & configure third party software if need be. **Configuration tasks defined by the Customer and carried out the Provider** ▪ Configuration and tuning of all VM and components depending on customers application
Operation	The Provider alone has root or administrator access on the servers in the Managed Tenant. The Customer will be granted access to relevant applications as a User only, to perform the tasks which are under his responsibility. **Administration tasks under the Provider's responsibility** ▪ Review Nodes performance and perform tuning, ▪ Configure the storage, ▪ Manage start and stop of Hadoop services, ▪ Add/Remove nodes, ▪ Ensure availability of Hadoop jobs and task logs **Administration tasks defined by the Customer and carried out by the Provider** ▪ Create scheduled jobs and tasks ▪ Manage Data Retention policies ▪ Management of Customer user accounts ▪ Execute/implement Minor or Maintenance Releases specific to a 3rd party component ▪ Terminate running jobs in Hadoop ▪ Management of ingestion flows and Kafka topics **Complex Administration tasks defined by the Customer and carried out by the Provider** ▪ Execute/implement major releases specific to a 3rd party component is considered an additional service and will be invoiced as such to the Customer.

Phase	Activities
Supervision (Alerting, Monitoring)	**Supervision tasks under the Provider's responsibility** ▪ Preventive Monitoring of metrics and KPIs ▪ Monitor availability, and alert the Customer ▪ Monitor performance, and alert the Customer ▪ Monitor capacity (including disk), and alert the Customer ▪ Monitor Service Status ▪ The alarms generated are raised to the central console of monitoring managed by the operations teams of the Provider to go through the incident management process. **Monitoring tasks defined by the Customer and carried out by the Provider** Monitor Customer specific jobs to detect long running, errors, etc.
Backup	The Provider operates backup policies in order to protect the Customer's Platforms in case of loss of configuration of a component, allowing restoration of a Node or rollback. However, slave Nodes are not backed up: in case of service failure, a new slave Node is deployed by the Provider. Customer's data are not included in backup policies. For all other VMs, Backup solutions implemented are: ▪ Hot File backup for master and edge Nodes ▪ Dumps for databases ▪ Snapshots when possible
Change Management	The service provides the Customer with the possibility to log: 1. Standard changes 2. Custom changes **Standard catalog : see a separate document for more details** The Customer can request for any of the current operations such as: ▪ stop / restart a service (maintenance mode) ▪ add / remove a Node ▪ backup / clone / restore the configuration of a component ▪ configure OS: groups, users, directories (system and/or HDFS, and/or webUI). ▪ delete data permanently ▪ create / modify / delete a database ▪ request an infrastructure modification (except datalake) ▪ request an infrastructure information ▪ add / modify / remove a Software component ▪ run a system command ▪ configure networks and security **Custom requests** In addition, when the Customer needs for more specific / custom services, he has the possibility to raise custom requests which are qualified by the Provider Big Data teams and lead to a proposal on quote to the Customer.

7.11.2 Specifications

The service consists of the following solutions and components

6.11.2.1 Cloudera CDP / CDF managed by the Provider

The Cloudera CDP/CDF solution includes the components listed below.

Table 20: Specifications for "Managed Big Data with Cloudera CDP/CDF Components"

Module	Components
Core	**CDP (Cloudera Data Platform)**
	Dataiku Studio DSS
	Airflow

Module	Components
Ingestion	CDF (Cloudera Data Flow)
Processing	Spark
	Hive
	Druid
Storage	Druid
	Hue
Visualization	JupyterHub
	Zeppelin
	Dataiku Studio DSS
	R Studio
	Tableau

6.11.2.2 Big Data native services with Flexible Engine managed by the Provider

Flexible Engine Native Services proposes a set of Big Data components as listed below.

Table 21: Specifications for "Managed Big Data with Flexible Engine Components"

Module	Components
Ingestion	DIS (Data Ingestion Service)
	DMS (Distributed Message Service pour Kafka)
Processing	CSS (Cloud Stream Service)
	MRS (MapReduce Service)
	DLI (Datalake Insight)
	MLS (Machine Learning Service)
	CS (Cloud Stream)
Storage	OBS (Object Storage Service)
	DWS (Data Warehouse Service)
Visualization	MRS (MapReduce Service)
	CSS (Cloud Stream Service)

6.11.2.3 Big Data native services with Google GCP by the Provider

Google GCP Native Services proposes a set of Big Data components as listed below.

Table 22: Specifications for “Managed Big Data with GCP Components”

Module	GCP component
Ingestion	Cloud Pub/Sub
Processing	Cloud Dataflow
	Cloud Dataprep
	Cloud Dataproc
	Cloud Datafusion
	Cloud Composer
Storage	Data Catalog
	Cloud SQL
	Cloud spanner
	Big Query
	Cloud Datastore
	Cloud Bigtable
Visualization	Data Studio

6.11.2.4 Big Data native services with Amazon AWS managed by the Provider

AWS Native Services proposes a set of Big Data components as listed below.

Table 23: Specifications for “Managed Big Data with AWS Components”

Modules	AWS component
Ingestion	Kinesis Streams
Processing	EMR
	Kinesis Analytics
Storage	S3
	Aurora
	RDS
	Redshift
	DynamoDB
	Elastic Search
	Kinesis Streams
Visualization	QuickSight

6.11.2.5 Big Data native services with Microsoft Azure managed by the Provider

Azure Native Services proposes a set of Big Data components as listed below.

Table 24: Specifications for "Managed Big Data with Azure Components"

Modules	Azure component
Ingestion	**Event Hub**
Processing	**HDInsight**
	Data Factory
	Databricks
	Stream Analytics
	Analysis Services
	Machine Learning
Storage	**Data Lake Storage**
	Cosmos DB
	Synapse Analytics
Visualization	**PowerBI**

7.11.3 Limitations

The following activities remain the Customer's responsibility:

- Sizing of the environment in coherence with the components requested by the Customer,
- Performing business tasks related to the Customer applications and use cases,
- Verifying the proper functioning of his business applications and use cases, on top of the Big Data softwares
- Produce and maintain a documentation for installation and configuration of his applications and use cases.
- Making decision to restore big data Nodes and databases,
- Project management, unless otherwise stated in the Technical and Financial Proposal

The execution/implementation of Major releases specific to a 3rd party component is not included, available through additional professional services only and a specific project.

7.12 Managed Computer Vision

7.12.1 Description

Managed Computer Vision is a service employing artificial intelligence for video analysis and allowing customers to gather insights and trigger alerts which are shown through a dedicated customer dashboard.
The service includes the following blocks:

- A Computer Vision software,
- A Cloud hosting solution managed by the Service Provider,
- An implementation service and a managed service for keeping the Computer Vision software solution up and running.

The implementation and managed services include the following items:

- Development of Managed Computer Vision use cases and their configuration to make them operational:
  - Dataset and tools deployment (labelling, training etc.),
  - Artificial Intelligence system design (internal framework, training, data processing etc.),
  - Design and implementation of key parameters and their visualization on a dashboard,
  - Application installation and configuration based on technology vendor best practices.
- System management, administration and 24 x 7 support for production and non-production environments,

- Monitoring and maintenance of the deployed system,
- Application maintenance as a third-party provider over the data lifecycle
- Incident, change and security events management.

The Service Provider can take care of full application stack management as an option on quote.

The Service Provider integrates ISVs (Independent Software Vendors) and experts into the Managed Computer Vision system according to customer needs.

7.12.2 Data privacy and security

Managed Computer Vision relies on camera footage at the customer premises and employs Artificial Intelligence methods for processing data.

The customer has the ultimate personal data processing responsibilities including the declaration of such technology to national entities responsible for personal data protection such as CNIL (Commission Nationale de l'Informatique et des Libertés) in France or equivalent institutions where the system is deployed.

The Service Provider proposes, within the Managed Computer Vision offer framework, end-to-end support on impact analyses on data protection for the CNIL institution. Potential equivalent activities in other countries can be offered upon a feasibility study carried out by the Service Provider.

7.12.3 Description

Here are additional details on the implementation and move to run phase for Managed Computer Vision.

Infrastructure implementation phase:
- Infrastructure and associated services deployment (middleware, network, DNS, NTP, backup, storage, antivirus, and monitoring),
- Infrastructure testing and validation.

Transition to run phase:
- Application design and data processing framework,
- KPIs collection, user dashboard creation,
- Development and integration of APIs,
- Application configuration,
- Data quality and data lifecycle testing,
- Monitoring system deployment and hardening,
- Move to maintenance stage,
- Activation of L1, L2 and L3 support teams.

Table 25: Description " Computer Vision "

Phase	Activités
Computer Vision Implementation phase	▪ Infrastructure and associated services deployment (middleware, network, DNS, NTP, backup, storage, antivirus, and monitoring), ▪ Infrastructure testing and validation.
Computer Vision Run phase	▪ Application design and data processing framework, ▪ KPIs collection, user dashboard creation, ▪ Development and integration of APIs, ▪ Application configuration, ▪ Data quality and data lifecycle testing, ▪ Monitoring system deployment and hardening, ▪ Move to maintenance stage, ▪ Activation of L1, L2 and L3 support teams.

7.12.4 Limitations

- The customer manages cameras infrastructure including initial implementation and maintenance,

- The customer provides the necessary workforce to monitor the Managed Computer Vision dashboard and act on alerts,
- Processed data is not backed up nor stored to be used as proof for legal actions. The main purpose of the service is to deliver a live KPI analysis and alerting solution.

7.13 Managed backup and recovery service

This Service allows the Customer to back up and restore **at the file level** the content of servers deployed in **physical environments** or in the **Cloud.**

The Customer can also benefit from the Office 365 Managed Backup. It allows to backup data from Office 365 applications: Exchange Online, SharePoint Online, OneDrive for Business and Team. It also provides full management of granular recovery of Office 365 data by application and backup policy.

This Service is based on a BaaS backup solution (integrated into the Provider's infrastructure). The cost of the BaaS Service is borne by the Customer as part of the underlying IaaS offer.

7.13.1 Description

The backup and recovery service includes the following services:

Table 26 : Backup & recovery description

Phase	Activities
Backup & restore Implementation	▪ Install and configure the agent on customer servers ▪ Configure the central backup platform to perform backups and restores on customer servers ▪ Perform an acceptance test
Backup & restore Operation	▪ Monitoring of client backups ▪ Restart backup in case of failure ▪ Perform restores on customer request (via change) ▪ Monitor the backup platform on a 24x7x365 basis ▪ Evaluate, schedule and execute system change requests ▪ Capacity planning on the backup platform

7.13.2 Caractéristics

The Backup and Recovery Service can be provided to Customers who already subscribe to the Managed OS, Managed Database, Managed Middleware, Managed Container, Managed Application services. This Service can also be provided to Customers who have on-premise or cloud-based data backup/recovery needs.

The following frequency and retention policies are predefined in the Provider's backup system.

The first backup in file mode or for Office 365 performed by the Service Provider is a full backup, the following backups are incremental according to the backup policy chosen by the Customer.

Table 27 : Standard retention policy

Retention policy	Policy Details	File / Office 365	
WEEKLY-1	Weekly backup with 1 week retention	✓	
WEEKLY-2	Weekly backup with 2 weeks retention	✓	
MONTHLY-1	Monthly backup with 1 month retention	✓	
MONTHLY-3	Monthly backup with 3 months retention	✓	✓
MONTHLY-6	Monthly backup with 6 months retention	✓	✓

Retention policy	Policy Details	File / Office 365	
MONTHLY-12	Monthly backup with 12 months retention	✓	✓
MONTHLY-36	Monthly backup with 36 months retention		✓

Customers may request specific retention policies and customized backup frequencies. Specific requests are submitted to the Service Provider for approval and will be quoted to the Customer.

7.13.3 Limitations

The following activities remain the responsibility of the Customer:

- Full acceptance tests which will be recorded in an acceptance report.
- Decision to restore a file or a group of files

7.14 Infrastructure services included

7.14.1 Antivirus service

This solution is composed of antivirus software installed on each server (Endpoint Protection) and an administration panel (Enterprise Console) positioned in the IaaS platform's service zone.

The panel manages upgrade distribution as well as deployment strategies and agent settings.

7.14.2 Managing patches and “service packs”

The Provider provides the Customer with patches and “service packs” for 3 management levels:

- Managed OS
- Managed database:
- Managed middleware

The upgrades are tested and validated by the Provider before being authorised for platform use.

The Customer validates or rejects the use of patches thereafter.

In the event of any problems stemming from the deployment of the Service Pack, the Provider may not be held liable. The Customer may request that the last image of the virtual machine be restored.

7.14.3 Supervision Service

The Provider undertakes to test the Customer solution infrastructure and application components to ensure smooth operation 24/7 and 365 days a year, at each management level (OS, database, middleware and Application) for which it is responsible. Any dysfunction alert confirmed by the supervision teams will give rise to an incident report with the Help Desk.

7.14.4 DNS Services

The Provider will provide two DNS services to respond to the following needs:

- Internet address resolution
- Customer Public DNS entry management

7.14.5 NTP Services

The Provider makes an NTP server available as the default time server

7.15 Managed Security Service

The Managed Security Service is a service provided by the Provider that allows the management of the following security components:

• Management of third-party Firewall(s) hosted on the Provider's infrastructure or Hyperscalers (Azure, AWS, GCP)
• Management of native Firewall(s) hosted on the Provider's infrastructure
• Management of third-party Load Balancer(s) hosted on the Provider's infrastructure or Hyperscalers (Azure, AWS, GCP)

The services provided as part of the Managed Security Service are described in detail in the document accessible through the link: https://cloud.orange-business.com/wp-content/uploads/2023/07/Managed-Applications-Technical-Service-Description-Managed-Firewall-and-Load-Balancer.pdf

The pricing of the security components of the Managed Security Service, as well as the technical description of the security components, are an integral part of the contractual package of the Managed Applications offering.

8 Support

The items below describe how the service is managed, as operated by the Provider, for all services provided.

Services are organised as follows:

- The Services Center, and more specifically, the Customer Support Center,
- Services Support, with the following processes:
  - change management,
  - incident Management,
  - problem management,
  - Configuration management,
  - Release management.
- Services provision, with the following processes:
  - service level management,
  - availability management,
  - continuity management,
  - capacity management,

8.1 Organisation of Support

The Services Center establishes 2 contact points via which the Provider can gather Customer demands (e.g.: change, modifications, dysfunctioning, etc.) in order to provide responses.

The two contact points are as follows:

- The Provider **Customer Support Center** (CSC), available 24/7, throughout the year. Each CSC enjoys visibility on the entirety of the service and customer applications hosted,
- The **Managed Services Manager** (or SDM, for Service Delivery Manager), as part of Premium Support.

The purpose of the Provider support is to manage Requests and Incidents, by carrying out the following actions:

- Take charge of the Requests and Incidents, and processing and resolving them;
- Communicate the appropriate, up-to-date information to the Customer regarding the processing of the Incidents and Requests which have been duly reported;

8.2 Customer obligations

The Customer establishes and maintains a nominative list of contacts authorized to report incidents and to contact the Service Provider's Service Desk. The Service Desk responds only to duly designated persons in possession of their login and access codes.

The customer's main contact guarantees that contact information is up-to-date and valid.

8.3 Support plans

The Provider offers the following 3 levels of support, depending on the criticality level of the applications for which the Service is intended: Initial, Standard and Premium.

Table 28: Service package by level of Support

Managed Applications	Initial	Standard	Premium

Support Service	Service opening	8x5	24x7	
	Through the Cloud Store Portal	✓	✓	
	By mail	✓	✓	
	By telephone. Limited to 5 named contacts.	✓	✓	
Managed OS		Initial	Standard	Premium
Supervision	Infrastructure supervision	✓	✓	✓
	Operating system supervision	✓	✓	✓
Capacity management	Reporting on infrastructure use (VM)	✓	✓	✓
	Reporting on resource use by VM (ram/cpu/disk)	✓	✓	✓
Managed Database		Initial	Standard	Premium
Supervision	Database supervision	✓	✓	✓
Capacity management	Reporting on resource use by database			✓
	Capacity review (using history and trends)			✓
Managed Middleware		Initial	Standard	Premium
Supervision	Middleware supervision	✓	✓	✓
Capacity management	Reporting on resource use by middleware			✓
	Capacity review (using history and trends)			✓
Managed Application		Initial	Standard	Premium
Supervision	Application supervision	✓	✓	✓
Version management	Max. number of versions per month	1	2	4
	Execution scripts delivered by the Customer for deployment automation	✓	✓	✓
	Previous versions maintenance			1 month
Capacity management	Reporting on resource use by Application (ram/cpu/disk)			✓
	Capacity review (using history and trends)			✓

Support service subscriptions are taken out for a minimum of 6 months. The Customer may modify its order only to move to a higher-range support offer during the commitment period. It then commits once again for 6 months at the new subscription level.

Changes in support level come into effect at the start of the calendar month.

8.3.1 Level 0 Support (Service Desk)

The Service Desk represents level 0 of the Customer Support Center and provides the following services:

- a single point of contact for customer-designated representatives
- a single telephone number and a single e-mail address,
- exchanges in French ou English,

- handling and processing of customer telephone calls,
- identification of the caller and his commercial offer,
- the opening of an incident ticket or exchange ticket relating to the handling of customer calls,
- redirecting the ticket to the appropriate level 1 team,
- transferring the customer call to the Level 1 team.

The Service Desk operates 24 hours a day, 7 days a week.

Customer requests are recorded in tickets in the Service Provider's repository. Information is entered into the ticket in accordance with the procedures described in the documentation produced after service initialization.

8.3.2 Level 1 Support

Level 1 Support provides the following services:

- ticket classification,
- initial processing of tickets
- incident recovery management (request for Level 2 teams),
- customer communication,
- management of customer requests,
- alerting to trigger the major incident and crisis management procedure,
- closing tickets.

Proactive management is carried out by a Level 1 Monitoring team (standard process). This team is responsible for events affecting infrastructure and service elements. For events corresponding to impacts or risks of impacts on the service, the team opens a ticket in the Océane incident management application and carries out the initial diagnosis (standard process).

Level 1 Support operates 24 hours a day, 7 days a week.

Tickets stored in the Service Provider's repository are used to record all customer contacts and actions taken, and to activate (if necessary) Level 2 teams.

Tickets remain the responsibility of Level 1 until the ticket is closed and a ticket closure notice is sent to the customer.

8.3.3 Level 2 Support

Level 2 Support is available 24 hours a day, 7 days a week. During French non-working hours, Level 2 support is provided by off-site staff on call.

Level 2 Support ("Technical Management") provides the following services:

- change management: under the supervision and responsibility of the SDM, and after analysis of technical impacts, contractual commitments, completeness of procedures and feedback, and after risk assessment, carries out "change management" actions,
- event management: handles Warning-type events and, if necessary, triggers incident, problem or change management for these events. N2 monitoring support configures monitoring tools and hypervisor.
- Incident management : Level 1 Service Desk support: provides support in resolving incidents that do not fall under the responsibility of level 1 (complexity, new problem, risk of non-compliance with contractual SLAs),

- problem management: under the guidance and responsibility of the SDM, participates in problem management, analysis, follow-up and proposal of technical/functional corrective and/or remedial action,
- production launch: under the guidance and responsibility of the SDM, implements changes,
- ticket management: under the guidance and responsibility of SDM, manages support teams and relations with partners in the context of incident resolution, problem management and/or change management,
- manages on-site interventions by local teams,
- production performance monitoring: Capacity Planning,
- support to SDM: for incident reports, dashboards, operational customer meetings,
- application of escalation procedures,
- operational maintenance of technical components and associated procedures: for example, updating the procedures used by the Service Desk and Level 1 Support.

These documents evolve throughout the life of the project, under the responsibility of the RUN teams.

8.3.4 Level 3 Support

Level 3 Support provides its services during French working hours.

Level 3 Support (or Engineering) provides technical support to Level 2 Support, and may contact the Service Provider's suppliers and partners if necessary.

Level 3 Support also covers the following activities :

- industrialization and documentation of technical platform components (hardware, operating system, application products, databases, etc.),
- proactive monitoring of technical developments (hardware and operating system upgrade proposals, etc.),
- integration of major application releases.
- management of support access authorizations
- management of access to publisher support (Microsoft, etc.)
- definition of business rights and associated restrictions (access to Cloud, AD, CyberArk)

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.

8.4 Incident Management

The Provider includes an incident management process, including the opening of tickets towards the Customer's IaaS supplier by the Provider. The aims of this process consist of:

- Responding as soon as possible in the event of actual or potential breakdown in Customer applications hosted,
- Maintaining communication between the Provider and the Customer regarding the situation stemming from the incident,
- Assessing the incident to determine the risk of its reoccurring or whether it is a sign of a chronic issue.

The Provider addresses incidents:

- proactively, when an incident has been detected by the supervision tools,
- In response mode, when an incident has been reported by the Customer via the CSC.

The incident management stages (whether reported proactively or in response mode) are as follows:

- Incident taken into account,
- Incident categorised by degree of Priority,
- Analysis and diagnostic review,
- Resolution and resumption of activity,
- Incident case closed following Customer agreement.

8.5 Change management

The entry points for a request for change are as follows:

- The Cloud Store Portal
- The Customer Service Center,
- The Managed Services Managers, for Customer contracts benefiting from the Business or Premium support levels

Any non-standard request for change is submitted to the Provider validation and may be rejected.

The list of persons authorised to submit requests for change is updated by the Customer and addressed to the Customer Service Center or to the Service Delivery Manager so that the modifications can be incorporated.

If the request for change is originated by the Provider, the Customer's explicit agreement is sought before implementation can begin. An exception will be made to this procedure where the change was required in response to an Incident of Priority level 1, as defined in the Service Level Agreement. In that event, the Provider notifies the Customer as promptly as possible following implementation of the change.

Through the Cloud Store Portal, the customer can access to the change catalogue for raising the change request. An act of change during standard business hours will be charged the equivalent costs of number of Tokens as indicated in the catalogue. When performed outside the Business Hours or the Business Days of the delivery centres, an act of change accounts for the double (x2) of the number of Tokens indicated in the change catalogue.

The Customer may purchase Tokens on demand or subscribe one or more monthly Token packs, which must be purchased until the end of the commitment period. Tokens not consumed from a pack are not carried over to the next month.

8.6 Release management

The Provider incorporates upgrades offered by hardware and software suppliers. This includes minor updates - patches, corrections, service packs - as well as major upgrades.

Major upgrade application is considered an additional service and will be invoiced as such to the Customer.

When the Provider decides to produce a new component, the production launch procedure is treated like a request for change, in line with the rules set out for change management.

The Provider ensures that all production servicing is traceable, thanks to an operation tool used by the CSC. These data are stored by the Provider throughout the Contract period and shall be considered as authentic by the Provider and the Customer for execution of this contract.

8.7 Configuration management

The Provider manages the reference bases containing the configuration for all elements included in the Service.

9 End of document