Business

Service Description
Private Cloud Solutions

Table of contents

1. Sales summary / background foreword

For many companies, specific IT needs cannot be met by a usual public cloud solution. These are for example:

- Legacy applications that require a specific Operating System and a specific environment to run and be maintained,
- Data confidentiality and isolation,
- Maximum security of data and assets,
- Traceability, proximity, close and identified location of the data,
- Performance (dedicated servers),
- Compliance with regulations, European applicable law,
- Customer control of the maintenance/update schedule of the infrastructure,
- Ability to mix managed and IaaS usages.
- Need to outsource a part of the infrastructure management to a trusted partner

For such needs, the use of an IT infrastructure dedicated to the customer, physically and logically isolated from others, is required.

The Provider meets these needs by providing Private Cloud solutions, tailor made to address a large plurality of needs and delivering Customers with a wide range of services from IaaS to PaaS, managed or in self-service mode.

2. Definitions

All capitalized terms used but not defined herein have the meanings set out in the General Conditions or in the Specific Conditions for Cloud Services.

"Back End" refers to a zone isolated from the internet and intranet, hosting services or applications not accessible via the Internet,

"DMZ (Demilitarized Zone)" refers to a sub-network isolated by a firewall. This sub-network comprises machines located between an internal network (LAN – customer stations), an external network (Internet, usually) and applications exchange networks.

"Front End" refers to a front zone, hosting services or applications accessible from the Internet.

"High Availability" means a system that is continuously operational for a desirable period of time. Availability can be measured in terms of "100% operational" or "never fails".

"Legacy applications" refers to software that has been in place for a long time in the company and is therefore "inherited" from the past. Although potentially obsolete, they are still essential to the day to day running and business needs of the Client.

"vCPU (Virtual Central Processing Unit)" refers to a virtual component in a computer which helps executing IT programs.

"Virtual Machine" or "VM" refers to a software executable environment which emulates a hosting computer. Several Virtual Machines can be created in a single computer. Each User has the illusion of having a complete computer while each Virtual Machine is isolated from the others.

"VLAN (Virtual Local Area Network)" refers to an isolated logical local IT network. Many VLANs may coexist on the same switch.

"VPN (Virtual Private Network)" refer to an extension of local networks ensuring the logical security provided by a local network. It is the interconnection of local networks via a tunneling technique using cryptographic algorithms.

"Workload domain" refer to a logical unit that groups the nodes hosts managed by a central control plane with specific characteristics according to the best practices of the HCI solution editors.

3. Purpose of the document

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

The present Service Description is attached to the Cloud Specific Terms.

4. Overview of the service

4.1. Overall description

The Provider's Private Cloud Solutions deliver a tailor-made IT infrastructure-as-a-service or platform as-a-service exclusively serving a Customer in the datacenter that best suits its needs, either Customer datacenter on-premises or hosted by the Provider in 70 datacenters of Tier III+/Tier IV equivalent level, worldwide.

The Private Cloud infrastructure is dedicated to the customer (unlike Public Cloud) and is available on the customer's intranet, with the purpose to match the organization strong requirements for security, compliance, and localization. Based on hyperconverged technologies, the infrastructure is designed to support customer's critical workloads with the right level of performance, rapidity of deployment, service assurance and scalability.

In accordance with the configuration defined with Customer, the Service enables the Customer to set up the following functionalities:

- Hosting of applications and data on the Infrastructure.
- Using the Infrastructures as:
  - a development, test and integration platform,
  - a pre-production platform,
  - a production platform or,
  - for hosting an application in SaaS mode (Software as a Service).
- Designing a secure architecture by partitioning services using security zones in the "secure architecture".
- Accessing its applications via Internet and/or VPN Intranet in a secured and efficient manner.
- Changing the architecture according to Customer's requirements for:
  - Virtual Data Center resources (CPU power, RAM memory, Disk Space capacity),
  - Internet and/or VPN Intranet bandwidth or,
  - Secure architecture (Front-End, Back-end).

The Provider takes care of the design, build and run of the platform ensuring its 24x7 high-availability, data-protection, security, connectivity, technical assurance and evolution according to customer's requirements and following the governance put in place with the customer (within agreed SLAs).

The Provider Private Cloud solution offer consists in providing to the customer some or all of the following services:

- Co-design and build of the appropriate solution,
- Delivery of the infrastructure (HW and SW), worldwide,
- Hosting of the infrastructure in the Provider/Partner datacenter (when not on customer premises),

- Implementation/integration of the solution within customer IT,
- Security services: updates for security patches, antivirus, security audits,
- Maintenance of the Private Cloud solution in operational conditions (Service Management),
- Management of the solution according to different models:
    - IaaS (Infrastructure as a Service) is a cloud computing offer where Customer benefits from IT resources within a virtualised environment via a VPN or another secured connection. The Provider deploys and manages the infrastructure (physical compute/storage servers, virtualization, networks and security). The Customer installs and manages the operating system, the middleware and the applications. IaaS provides Customer and its own users/customers with the ability to autonomously provision virtual machines (VMs) with the associated VM storage and networking on demand in multiple regions.
    - With PaaS (Platform as a Service), in addition to the provision and the maintenance in operational condition of the Cloud infrastructure, the Provider implements the hosting environment configuration according to the customer's needs (virtual networks, VM hosting model, VM configuration profile for resources & storage), leaving Customer in control of the business applications that they can install, configure,,use and maintain themselves.
    - Various gradual levels of managed services are available for Private Cloud Solutions including the managed OS, the managed middleware, and the managed applications.
- Support (Service level)

Different levels of support are offered for Private Cloud solutions, with service level agreements that vary according to the level chosen. In addition to the predefined Standard and Premium support levels, there are customizable levels to meet the specific requirements of customers as part of a tailored offer.

4.2. Cloud Avenue [Private] solution

Besides a 100% tailor-made solution presented in this service description, the Provider offers its customers a standardized private cloud solution, called Cloud Avenue [Private]. Thanks to its rationalized and standardized architecture, Cloud Avenue [Private] offering is suitable for customers looking for the core characteristics of a private cloud solution but who want lower costs and faster delivery. This solution is presented in a specific Service Description.

4.3. Geographical footprint

Private Cloud Solutions can be implemented worldwide, in the customer own datacenters and\or hosted in the Provider datacenters (70+ datacenters worldwide).

Figure 1: Provider datacenter worldwide presence

5. Content of the service

The Provider Private Cloud offer is based on pre-standardized solution blocks mixing infrastructure and services.

5.1. Service components

5.1.1. Services included

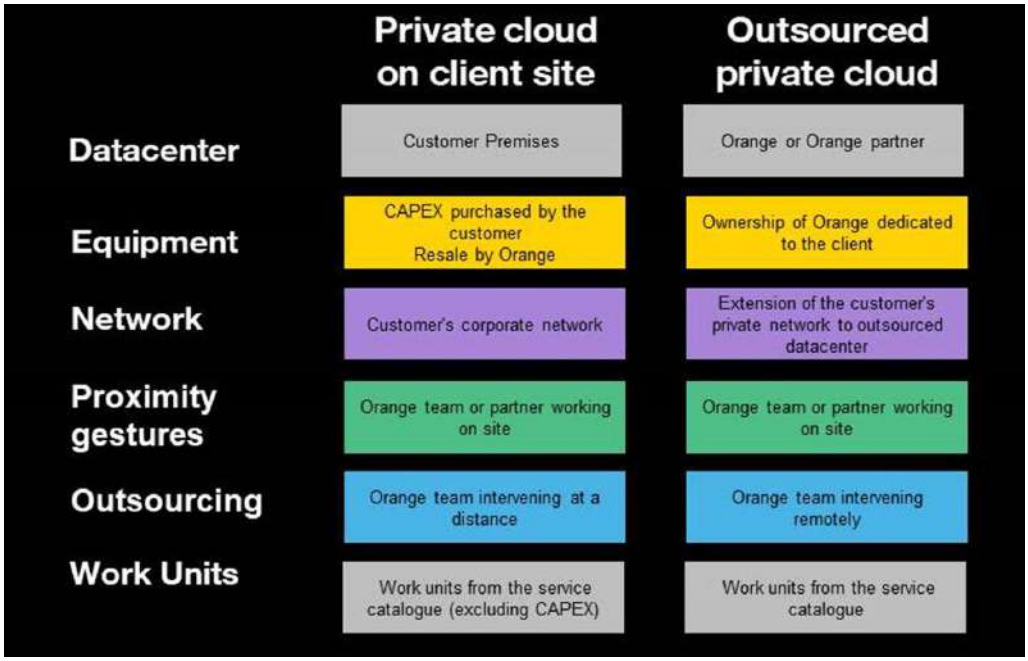
- Procurement and build of the private cloud infrastructure and any infrastructure required for the additional add-on services subscribed via the Provider.
- Hardware and software licenses for all in scope private cloud components up to the hypervisor layer.
- Configuration and management of the private cloud infrastructure and any infrastructure required for the additional services subscribed via the Provider.
- Solution management including operational management, monitoring and regular maintenance of the hardware and software components of the private cloud and any subscribed add-on services.
- If hosted by the Provider or partner, hosting space for the private cloud infrastructure (in two separate datacenters with inter datacenter connectivity if High availability / Disaster Recovery requirements) and any infrastructure required for the additional add-on services subscribed via the Provider
- Supply and management of OS images required for the management and monitoring of the private cloud IaaS platform (optional).
- Day 1 configuration of the IaaS platform with all its components as discussed, agreed, and validated with the customer.
- Regular monthly service reviews conducted and organized by the Provider customer service manager.

5.1.2. Additional services

Additional services require a specific quote, the validation of the Customer and an additional invoicing.

- Any operating system, database, or application licenses for customer virtual machines.
- Management of any customer OS, database, applications – unless subscribed as a service.
- Transition, migration and transformation of physical assets or customer data from current to future mode of operation – unless the Provider is responsible for providing this service.
- Application-level backup management.

Figure 2 : Examples of Models



5.2. Infrastructure components

The Provider provisions a Virtual Data Center on dedicated hardware (containing CPU, RAM, Disk Capacity and included backup service) and secure architecture resources (dedicated firewalls, load balancers and customer managed HSM key management appliances).

The Provider offer focuses on the Software-Defined Data Center approach called Hyper-Convergence. A hyper-converged infrastructure (HCI) consists of virtualizing computing, storage and networking. HCIs take advantage of the hypervisor to provide computing power (Compute), network, and shared storage from a single X86 server platform (means the servers used are no longer categorized by function – computing, network routers, firewall or storage – but are generic servers that perform these services through the datacenter's comprehensive virtualization software: Server Virtualization, Software Defined Network, and Software Defined Storage).

The Hyper converged integrated system (HCIS) tightly couples computing, network, and storage hardware, which dispenses with the need for a regular storage area network (SAN). Storage management functions — plus optional capabilities like backup, recovery, replication, deduplication and compression — are delivered via the management software layer, together with compute provisioning.

The Service is set up for Customer using standard validated components, as agreed with the Customer in the Order Form.

For Private Cloud requirements, the Provider provides solutions on three leading technologies, all hyper-converged.

- VMWare: the core components of VMware's hyper-converged solutions are VMware vSphere and VMware vSAN.
- Nutanix: the core components of Nutanix are AHV, Volumes, and Prism.
- Azure Stack HCI: it provides a Azure hybrid solution on Customer premises, ready to deploy according to customer requirement and same user experience than Azure.

Regardless of the technology and regardless of the Private Cloud sales model (whether or not the physical servers used by the Service Provider are owned by the Provider), all hosted data and applications provided by the Customer remain the property of the Customer

Figure 3 : Private Cloud Solutions Feature Sets

feature	VMWare	Nutanix (new portfolio 2022)	Nutanix	Azure Stack HCI
Hypervisor	vSphere / ESXi	AHV, vSphere, ESXi, KVM, Xen, Hyper-V	AHV, vSphere, ESXi, KVM, Xen, Hyper-V	HyperV
Cloud Management Platform	vRO / vRA	Intelligent Operations	Prism Pro	Azure Portal, Azure Arc
SDS tool	vSAN	AOS Storage	AOS	native
Block Storage	vSAN	Nutanix Kubernetes Engine	Volumes	native
Object Storage (S3)	Object Storage / Ceph	Objects Storage	Objects	native
Files Sharing	vSAN files services	Files Storage	Files	3rd party (Isilon)
SDN (micro segmentation)	NSX-T	Flow Network Security	Flow	native
Container orchestration	Tanzu	Nutanix Kubernetes Engine	Karbon	AKS
Database Management	vFabric	Nutanix Database Service	ERA	native
VM Image Management Service	Mirage	Intelligent Operations	Prism / Prism Pro	native
DR	Veeam / Zerto / vSphere replication /	Nutanix Disaster Recovery	Leap / Protection domain	Comvault
Automation Orchestrator	vRO / vRA	Self-Service	Calm	native
Life cycle application management	vRealize	Self-Service	Calm	native
Resource pool management	Resource pool	Projects	Projects	native
Analytics, Optimization	vRops	Cost Governance	Beam	native

5.2.1. Computing and storage capacity

The Provider provides computing capacity based on a yearly / monthly capacity plan established with Customer. Computing capacity includes CPU Power, RAM memory, and one or more levels of storage capacity. Those resources are used to create the Virtual Machines.

The CPU power is set out in vCPU values (per CPU cores) and the RAM memory is set out in GB values.

Disk types and capacity provided are divided into GB values (storage on the virtual machines). Any specific performance capability, if provided, will be documented in the Service Level Agreements governing the provided services.

With the Private cloud solutions, workload domains are defined. Services classes applied to computing capacity are defined per workload domain with the following parameters: vCPU/core ratio, vCPU/core (recovery) ratio, number of nodes for failure to tolerate.

Customer can modify its reserved resources via the Provider's change control process (assuming sufficient unreserved infrastructure capacity is available).

The services include:

- Servers and components acquisition,
- Equipment installation,
- Management tools providing, installation, setup and maintenance,
- Physical connectivity,
- Physical server (RAM, CPU, storage) initial configuration,
- IaaS Infrastructure configuration and deployment of physical/logical connection to LAN network,
- Server operation and support.

5.2.2. Firewall

The Provider sets up a secured Infrastructure with a high availability firewall configuration.

The firewall pair is located at the upstream of the Hosting Platform with restrictive rules for analyzing and filtering traffic going through the platform and the Customer's Virtual Data Center and VLANs.

The Customer is responsible for defining its own firewall rules between internal virtual instances/VLANs and external networks. These rules are defined during the design/onboarding phase and managed and updated through the Provider's change control process during the 'live' Service.

Depending on the option subscribed by the Customer, this dedicated firewall service gives access to up to 8 security zones/VLANs related to Customer traffic (traffic VLAN), load balancing traffic (virtual VLAN) and the Provider traffic (admin VLAN).

These security zones can be defined as:

- Front End security zones (internet zone, intranet/VPN zone with the VPN connection option);
- Back End security zones.

Each security zone contains private address subnets, defined with the Customer, which can be used for Virtual Machines.

The Customer can request the Provider to configure its filtering rules via the Provider's change control process. The Customer must have the required knowledge and expertise to understand the required firewall rules. Any addition or modification requested by the Customer to the filtering rules of the Virtual Machine is under the Customer's sole responsibility.

5.2.3. Load balancing

The Load Balancer allows maximizing the availability of the virtualized resources by improving the distribution of the network incoming traffic workload (HTTP, TCP) among a pool of virtual machines, containers or bare metal servers. The traffic distribution is done according to most usual algorithms (Round-Robin, Least Connection, IP Source). With this service the withdrawal / reactivation of unavailable / again available containers can be performed automatically. The Load Balancer service is the necessary tool to deploy and operate high availability architectures.

The Provider implements load balancing appliances by setting up redundant hardware for the Virtual Machines.

Virtual Machines availability and load balancing can be managed by the load balancer. The load balancing service is available to all secure zones.

Traffic management functionalities include:

- Intelligent load balancing (choice between two algorithms: Round Robin and Least Connection),
- IP source persistence.

NB: To activate the load balancing, the Provider and/ or the Customer imperatively authorize ping requests on the Virtual Machines pooled by the load balancer. Otherwise, the load balancer is not active on those Virtual Machines that are considered as switched-off.

The maximum number of load balancing rules is 10 in each security zone.

5.2.4. Security & identity

The Provider builds a security base. The offer includes a Managed Firewall service that can be completed with optional features such as intrusion detection, anti-DDOS, Security Operation Center.

The Edge Firewall monitors North-South traffic (between the data center and the rest of the network) to provide perimeter security functionality including firewall, Network Address Translation (NAT) as well as site-to-site IPSec and SSL VPN functionality.

The Provider secures data flows in each virtual machine and container and offers micro-segmentation of virtual networks based on NSX network virtualization and security principles proposed by our VMware.

Similar functionalities are provided with Nutanix solution (Flow) and with Azure Stack (natively embedded).

If needed, the Provider can define with the Customer how to assign the tasks among the various roles: IT security manager, users, administrators, and developers. This segmentation allows deployments to be automated within their scope of responsibility. Perimeters and permissions can be controlled optionally through the vRealize Automation™ interface (VMware), Intelligent Solutions interface (Nutanix), native interface (Azure Stack) and integrated with the client’s Advanced Directory to manage policies based on the groups the users belong to.

Regular updates to patch security flaws in the underlying infrastructures are included in the private cloud service. The Provider also extends this service to any additional outsourcing that may be entrusted to the Provider.

5.2.5. Backup

With the Private Cloud Solution, the Provider proposes managed backup and business continuity plans to protect companies against the risk of data loss.

The Provider integrates, operates, automates and monitors the solution 24x7.

The backup service allows to save Customer's data on a daily or weekly basis and to restore it when necessary, at a chosen date within the backup history limits.

The Backup policy proposes 2 standard modes:

- Weekly-6 (a weekly backup with 6 weeks backup), by default mode,
- Daily 15 (A daily backup with 15 days backup).

Customized backup policies can be addressed and subject to validation.

A wide range of technical solutions are proposed depending on customer requirements (stored data, virtual machines, operational databases, etc.), quantity, retention time, destination (local, remote or cloud), partial or complete Recovery Time Objectives (RTOs), tolerable or intolerable Recovery Loss Objectives (RLO), and the flexibility of the recovery process.

Basically, the Provider management scope covers the following areas:

- Customer backups monitoring,
- Storage repository profile definition,
- Backup restart in case of failure,
- Restoration proceeding at customer's request,
- Capacity planning on the backup platform.

The managed data protection solution with Veeam Backup and Replication Suite™ provides efficient and powerful backup of the Virtual Machines, a fast and flexible restoration as well as advanced features for Virtual Machines replication. The compatibility is well recognized for VMware vSphere™ environments leveraged in the Private Cloud Solutions as well as for Microsoft Hyper-V environment.

Similar solutions are available with Nutanix (Xi Leap) and Azure Stack (CommVault).

The Provider proposes four scenarios with different RTO/RPO (Recovery Time Objective/ Recovery Point Objective):

- Single Availability Zone (AZ): no protection against site failure.
- Dual AZ, same site: dual room, protection against room failure.
- Dual AZ, different sites: protection against site failure.
- Dual Region: management stack and production stack fully separated, which places workload closer to customer.

Datacenters are chosen based on distance and network available between them.

Infrastructure hosting in Tier III+/IV equivalent data centers close to the enterprise and its affiliates (70+ Provider data centers worldwide).

5.2.6. High Availability

Private Cloud Solutions propose a high availability service based on a redundant multi-site architecture.

High availability relies on a redundant multi-site architecture. The entire system is designed by the Provider, according to validated benchmark architectures: certified datacenters, redundant and reliable inter-site networks, low latency between main sites, certified equipment, high availability datacenter virtualization architecture for everything (computing, storage, network, virtualization, security or portal). The Provider’s teams adjust the design of private clouds to meet application performance and data access requirements.

In the event of hardware failure, the fault-tolerant system continues to operate without interruption or hindrance to service on redundancy hardware. Through its outsourcing support, the Provider intervenes quickly to repair the defective hardware and restore nominal service in order to avoid a double breakdown.

2 different resilience profiles are proposed: synchronous replication (Active/Active) or asynchronous replication (Active/Passive).

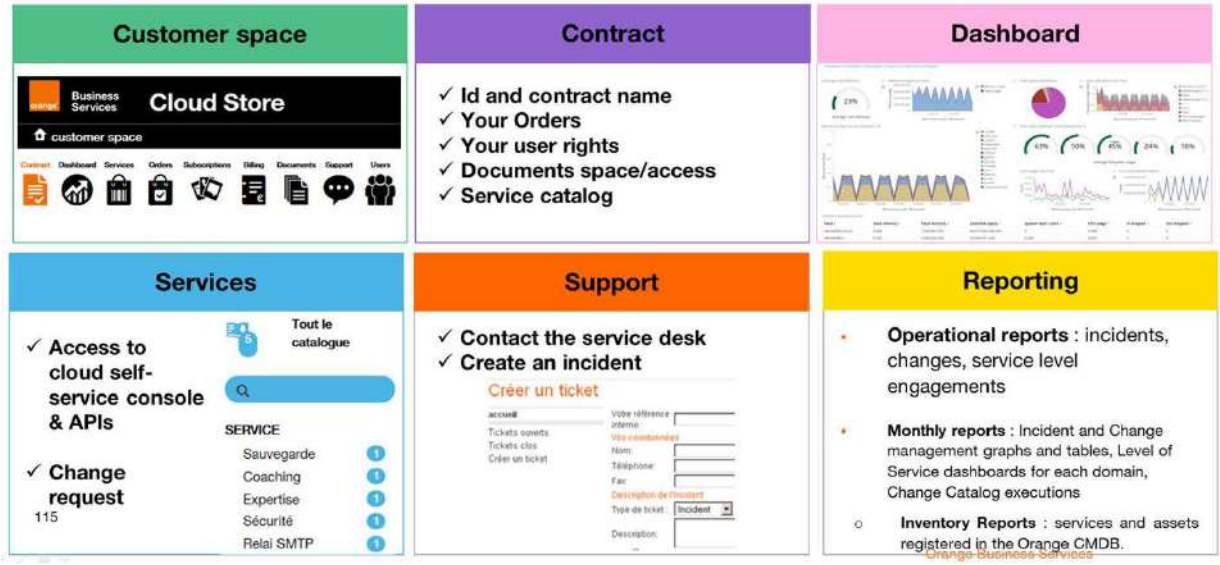
A maximum 5ms latency between both sites is required for synchronous replication.

5.2.7. Self-Service portal, Orchestration, Hybridization

With the Provider's Private Cloud offer and according to the chosen solution management mode, Customer can access to a self-service console, embedded in a unified web portal.

Through this console, Customer IT department presents a service catalogue to its users.

Figure 4 : Customer Web Portal



Users can activate and deploy services depending on their access accreditation.

Clicking on a service launches a deployment validated alongside a reference pattern (IT practice, security, support).

When the Provider provides optional managed services, the launch triggers automatically the deployment of management agents (monitoring, backup, etc.).

The range of supported platforms is broad (multiple private cloud DC, various IT equipment, applications, OSS-ITSM, public clouds).

Responsibilities:

- The Provider is responsible for the infrastructure and implementation of the services.
- The Customer is responsible for user management.

5.2.8. Cloud Automation

The Provider has defined 3 stages within the Private Cloud offer, with an inceasing level of automation:

- On demand: Virtualization of the compute/storage resources allocated by the administrator.
- Automated cloud: Automation of User APIs and orchestration.
- Micro-segmentation: with the micro-segmentation, it is possible to reinforce and complete the global security of a cloud system by adding an East-West lateral security level (inside the system, between its different components). The micro-segmentation defines secure zones within the cloud system allowing to isolate workloads and protect them individually by bringing more granular security rules that can apply directly on each VM or each container.

5.2.9. Containers, Kubernetes & PaaS

Customer developers can use Kubernetes™ clusters, a standard platform with open APIs conceived for the deployment of third generation applications (Cloud native) based on containers.

Kubernetes™ orchestrator enables containers high-availability, load balancing, auto-scaling, easy upgrades without loss of service. It eliminates many of the manual processes involved in deploying and scaling containerized applications. Kubernetes can run on various cloud platforms.

Docker™ containers are portable from one environment to another. Containers embeds OS and dependences, which make them independent from the host OS and from other containers, facilitating the integration.

The Provider guarantees a production grade Kubernetes integrated and maintained by our operations team.

The Provider puts at customer's disposal container automation solutions with all Private Cloud technologies (VMware, Nutanix, Azure Stack Hub):

- Tanzu Kubernetes distribution is supported by VMware.
- Nutanix KubernetesKarbon (Nutanix) is embedded within core solution.
- Azure Stack HCI gives access to AKS.

5.3. Managed services

The Provider provides optional progressive levels of managed services on top of the Private Cloud infrastructure:

- Managed OS: operating system management including server-related tasks and additional upgrade activities.
- Managed database: complete management of the customer's database(s), including server-related tasks, optimization and upgrade activities.
- Managed Middleware complete management of all software offered in the catalogue of the following components: Web Server, Application Server, File Server, Directory Server, Proxy Server. The co-management of the Middleware is possible but will be subject to a Customized Offer.
- Managed Application: management of the Customer's Business Applications (web e-business, ERP, CRM, Finance, HR ...).

As these levels of managed services are progressive, the subscription to a service will require the subscription to the lower levels (i.e. for the Managed Database and Managed Middleware management levels, the Customer must obligatorily subscribe to the Managed OS management level).

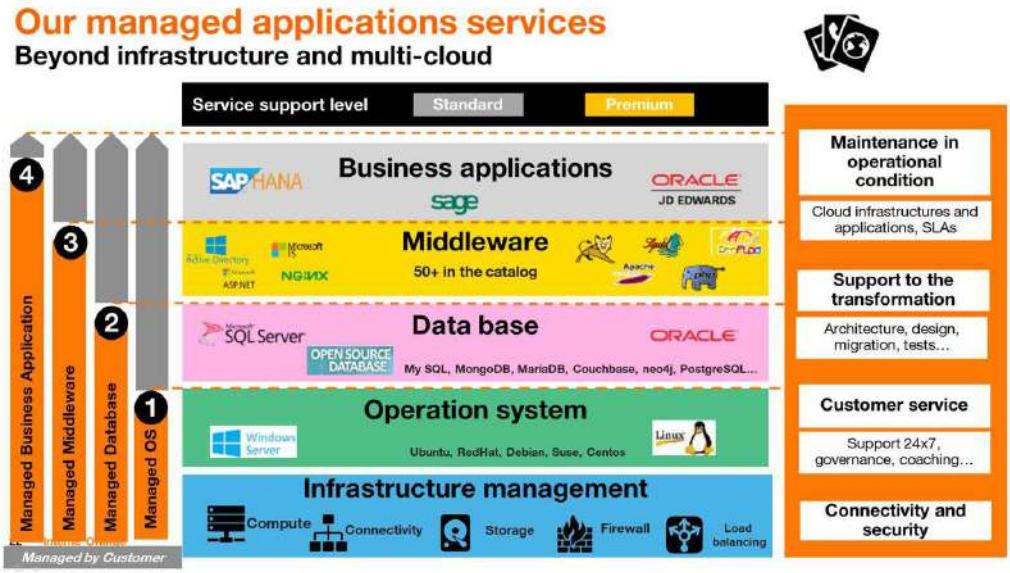
The Provider reliably runs the Customer's infrastructure and applications with a high level of expertise.

The Provider maintains The Customer's applications in production, inclusive of SAP.

The level of reporting available to our customers around application performance features:

- Performance monitoring of the services.
- A 360°map of the IS components: clouds, workloads, systems, middleware, business applications, and services.
- Performance views over cloud infrastructures and applications.
- Service usage and events reporting.
- Monitoring of data flows between applications.

Figure 5 : Managed Services



5.4. Colocation

With Private Cloud solutions, colocation is possible for needs not covered by virtualization.

The Provider can host the Customer's specific equipment in the same datacenter.

The hosted equipment can be managed by the Provider on a case-by-case basis.

6. Terms of use

6.1. Pricing

Except for Cloud Avenue [Private], a Private cloud solution is always fully tailor made. It means the quote of a private cloud solution requires a pre-sales phase taking into account the dimensioning, the required functional level and the managed services.

With the Private Cloud as a service model,

The Provider purchases the equipment and all the elements necessary to create the service and resells the service in the form of work units of a catalogue of services covering:

- The equipment (CAPEX either paid upfront at delivery or integrated within work units)
- The build
- The exploitation
- The support
- The commitments
- The governance

With Resale of equipment + service model,

The Provider resells the main equipment to the customer.

- The equipment

The Provider provides integration services and operations separately:

- The build
- The exploitation
- The support
- The commitments
- The Governance
- The services

6.2. Minimum commitment

The usual duration of a private cloud contract is 3 or 5 years.

6.3. Reversibility

Pursuant to the General Terms and Conditions, the conditions of reversibility are defined as follows:

- The duration of the reversibility period is limited to 3 months.
- During the reversibility phase, the "Guarantee Time to Repair" does not apply.
- The Provider commits in particular to provide technical information on the architecture of the service, provided that the information requested is not assimilated to know-how protected by the Provider.

In case the Provider is requested to provide additional assistance to the assistance defined above and to manage the service, the Customer shall receive:

- A proposal for paid assistance specifying the conditions of assistance, the personnel dedicated to the reversibility operations, the possible material and physical installations necessary.
- The financial conditions applicable to the implementation of this additional assistance.

For its part, the Customer undertakes to provide all the technical, human and, where applicable, financial assistance required to successfully complete the migration of the service. The terms and conditions of the Agreement will continue to apply until the end of the Reversibility Period.

In any case, the Customer shall be solely responsible for its relationship with the transferee and for the latter's actions.

6.4. Microsoft licenses

The Customer may either subscribe to Microsoft Software licenses from the Provider in rental mode or bring licenses subscribed by him directly to Microsoft or a third-party reseller in mobility mode, according to the terms of use applicable to each Software, available at the following address:

https://www.microsoft.com/en-us/licensing/product-licensing/products

The Customer's use of Microsoft Software must comply with the terms of use associated with Microsoft's SPLA (Service Provider License Agreement). The Customer is the sole responsible of non-conformities in using Microsoft software and services and he is liable of the consequences decided by Microsoft in such cases.

6.4.1. Rental mode

The Microsoft licenses offered by the Provider are in rental mode, the Customer must not use the corresponding licenses for any purpose other than the Service subscribed to from the Provider.

6.4.2. Mobility mode

Microsoft license mobility, for previously acquired software, is possible in accordance with the "License Mobility" or "Qualified Multitenant Hoster" (QMTH) add-on of the SPLA contract, depending on the Software concerned.

Among other conditions, the Customer is responsible for having subscribed with Microsoft, when required by Microsoft, the "Software Assurance" (SA) which is an additional license to allow its mobility,

Microsoft licenses from a Customer's SPLA or SPLA Academics contract are eligible to mobility. In order to enable this capability, an "Outsourcing Company Agreement" contract have to be signed between the Customer and the Provider as stated in §7 of the Customer's SPLA contract.

7. Support and service/operation management

7.1. Organisation

The Provider sets up a governance team responsible for the implementation and execution of the Contract and therefore responsible for the performance of all the Provider's commitments to the Customer and guaranteeing customer satisfaction throughout the performance of the Contract.

Figure 6: Operation Team Managing the Service

Figure 7 : The Service Desk

- Non CET/CEST business hours requests will be addressed case per case to see if the service can be covered by existing 24x7.
- French and English language support depending on the choice of delivery model

7.2. SLA / Commitments

Service Commitments depend on the proposal. They include:

Guaranteed availability:

- Monthly guarantee of the Private Cloud Service availability.
- Commitment according to the selected service class and defined architecture.
- Up to 99.99% depending on the chosen architecture.

Guaranteed time to repair (GTR):

- Service 24x7.
- Commitments according to Incident Severity.
- Example: GTR less than 2h for the highest level of service.

Change execution

- Non-business hours change execution.
- Commitments according to the complexity of the change.

Backup

- The Provider's commitment only if the backup is managed by the Provider
- Restoration: commitment to 100% successful completion of backup requests, no commitment to restoration quality.

With the Private Cloud solutions service, 3 levels of support are available: Standard, Premium and Custom.

They are selected according to the criticality of the Customer's applications to which the service is dedicated.

Figure 8 : Incident Management SLA

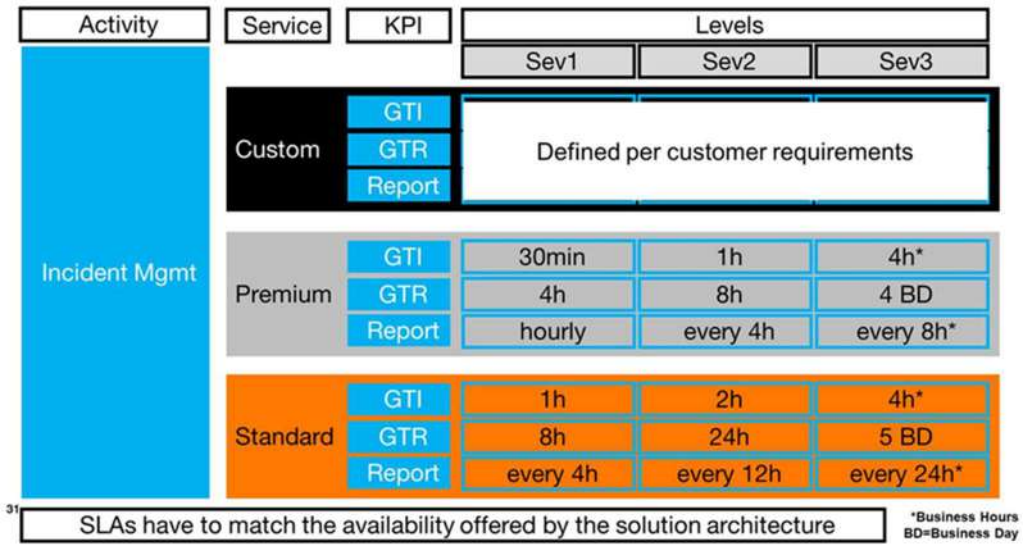


Figure 9 : Problem Management SLA

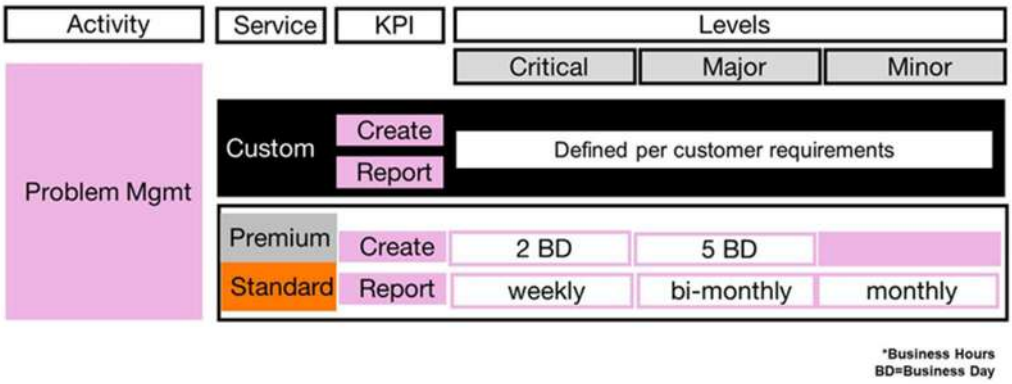
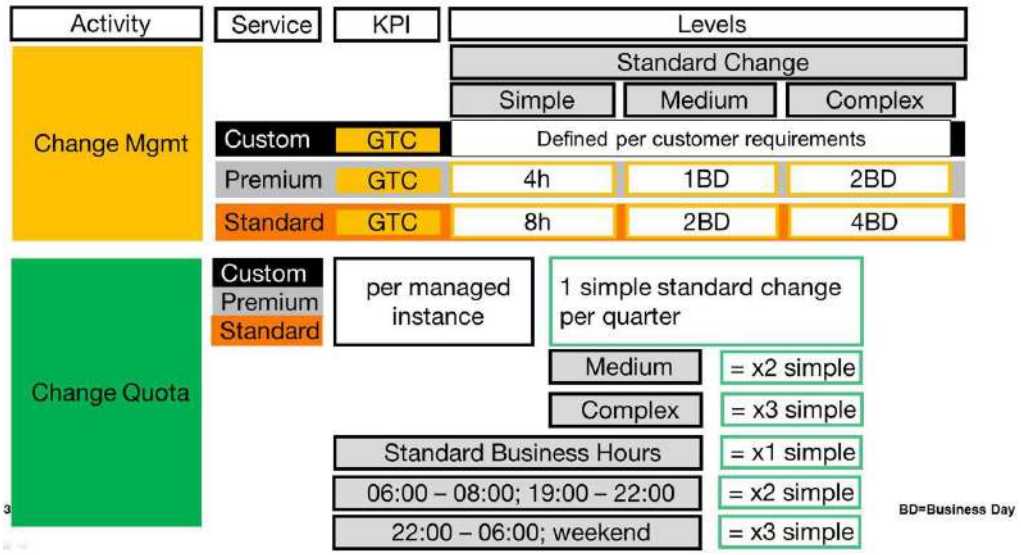


Figure 10 : Change Management SLA



7.3. Operation & Governance

7.3.1. Release management

The release management of the Customer's infrastructure is done by the Provider in coordination with the client, according to the agenda and constraints of the Customer.

It concerns security and maintenance patches and the Service packs proposed by hardware and software suppliers.

The Provider and the Customer agree on a regular maintenance window for all planned works:

- The Provider informs the Customer of new updates/application packages availability.
- The Provider installs patches/update application packages upon Customer's approval according to agreed rollout plan e.g. development systems in week 1 and production systems in week 2 after the Customer has performed satisfactory tests in the development environment.
- Emergency patches and application package updates can be installed via the standard change management process.

It possibly covers OS, database and Middleware for managed instances (if managed services option is subscribed).

The Provider ensures the traceability of all updates on the Provider's perimeter in a dedicated operating tool. This data is kept by the Provider over the duration of the Contract.

7.3.2. Alarm management

Thanks to a range of tools collecting alarms on the infrastructure, the Provider detects the different error codes and centralizes them in the Provider Event Manager. Error codes are prioritized according to 2 categories of severity: warning and error. The resulting alarms are transmitted to Level 2 (L2) and addressed according to ITIL process and compliance.

7.3.3. Incident and problem management

The Provider monitors the datacenters (if hosting provided), the whole hardware (compute, storage, network, backup), the software components (virtualization layer) in order to prevent any incident at infrastructure and cluster levels.

Incident management concerns incidents that may occur on all elements of the Customer's IT infrastructure and services under responsibility of the Provider.

The Provider integrates an incident management process which objectives are to intervene as quickly as possible in the event of actual or potential failures, to maintain communication between the Provider and the Customer regarding the situation and to evaluate the potential recurrence of an incident.

Incident monitoring and management are provided 24x7x365.

The Provider handles incidents:

- In proactive mode, following detection by monitoring tools, by an administration of the patches concerted with the Customer and by life cycle management.
- In reactive mode, following an incident reported by the Customer. Incidents are managed for resolution according to the Provider's standard Incident management processes, incident classification and service levels targets set based on the associated level of support.

Regardless of the origin of the alert, the Provider appoints an Incident Manager, in accordance with ITIL recommendations on incident management:

- Acknowledgment of incident
- Classification of the incident according to its severity
- Analysis and diagnosis
- Resolution by application defined instruction and resumption of operations
- Close incident case after Customer agreement

7.3.4. Service change management

As part of the Private Cloud solution Services, the Provider manages the Customer's service change requests based on the Provider's tools and processes.

The Provider provides the Customer with an access to the Managed Services Changes portal which allows the Customer to send online requests for technical changes to be performed by the Provider. The Customer may access the Service Changes portal using a secured link.

Two types of change requests:

- Standard service change requests: concern requests which execution are fully documented in a change service catalogue and have been tested and approved by the Provider's operations. Standard service requests are submitted and managed according to the Provider's Change Request processes using the Provider's Change management tools (ECE portal).
- Non-standard service change requests: on project mode and subject to the Provider's validation. The entry point for this request is the CBM (Contract Business Manager) or the Customer Service Center.

7.3.5. Capacity and performance management

The Provider provides a pool of resources with associated capacity which is limited by the resilience engineering rules (consistent capacity planning).

The Customer benefits of its capacity usage status through the reporting.

The Provider proactively brings capacity planning information as part of the alerting process when the capacity used by the Customer is about to reach a certain limit.

Capacity management monitors and acts mainly on:

- CPU/RAM resources,
- Network resources,
- Storage and backup resources,
- Software licenses.

The validation of additional resource requests is made by the Provider since the physical hardware resources are under its responsibility.

By default, all the elements of performance of the Customer's infrastructure are collected by the Provider.

As from the managed OS level, the Provider can optimize the cluster performances.

The Provider's capacity and performance management scope:

- Maintain the optimal performance of the servers over time,
- Analyse servers and hypervisors statistics performance periodically,
- Recommend needed changes configurations (servers and hypervisors),
- Analyse and make recommendations following any significant degradation of response time.

7.3.6. Reporting & Monitoring

The Provider collects permanently the whole technical metrics of the platform, either VMs or objects hosted on the platform (infra and virtual instance metrics).

Infrastructure metrics are then processed and a comprehensive range of information and statistics are made available to the Customer through the shape of dashboards or reports:

- Dashboards (ex: via vROPS web access with VMware technology) with real-time cluster health status and VMs metrics,
- Operational reports (alert, change, capacity) automatically generated and sent by email.
- Monthly reports (graphs and tables of incidents and changes, summary table of service level indicators by perimeter, number of work units consumed over the period
- Inventory reports: including services and assets from the Provider's CMDB.

Optionally, specific monitoring tools provide metrics on Managed services (OS, Middleware, DDB, applications).

The Customer accesses to the monitoring/reporting tools via the CloudStore.

Figure 11 : Customer Web Portal

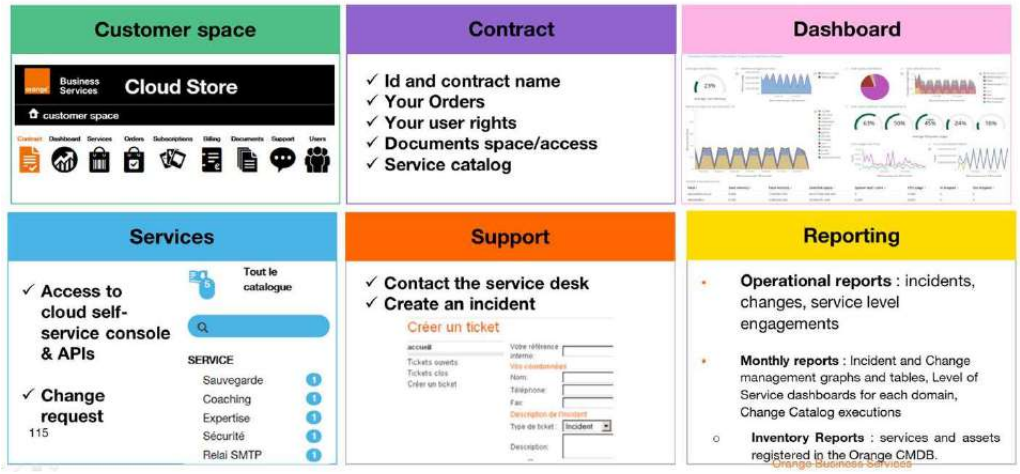
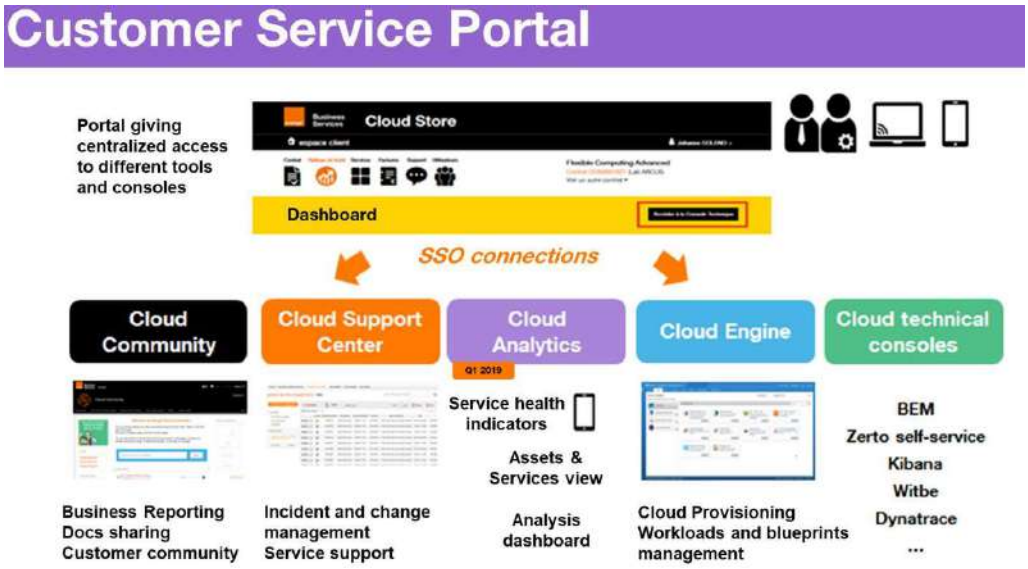


Figure 12 : Customer Service Portal



8. List of figures