orange™ Business Services

Service Description

Flexible Computing Advanced

Table of contents

1 Definitions

Complementary to the definitions as per General Terms and Conditions, the following specific definitions shall apply with respect to this Service Description.

Application Programming Interface (or **API**) refers to the programming interface that allows you to access vDC resources using a program.

Bandwidth refers to the data transfer capacity made available to the Customer for transferring data between the storage platform and the Internet or Intranet network.

General Terms and Conditions refers to Orange Business Services' general terms and conditions for Cloud Services.

Domain Name Service (or **DNS**) refers to the system used to establish a connection between an IP address and a domain name.

Infrastructure refers to a collection of resources (Virtual Machines, servers, firewall, load balancer, etc.) assembled by Orange Business Services to provide the Service.

Customer License(s) refers to Third-party Software licenses that a Customer subscribes to that are used in the Infrastructure.

DRaaS (Disaster Recovery as a Service) refers to a disaster recovery solution set up between the Customer's infrastructure and the Flexible Computing Advanced platform. In this document, DRaaS also refers to a billing method for computing power.

HADR (**High Availability Dual Room**) refers to a Feature allowing a vDC to have a very high level of availability thanks to a distribution of its resources over two rooms and the use of metrocluster.

Local Area Network (or **LAN**) refers to a local computer network in which connected terminals (computers, etc.) send and receive frames in the link layer without using an intermediary router. Local networks are interconnected with switches or other connecting devices.

Virtual Machine (or **VM**) refers to a software-based computer that runs an operating system and applications just like a physical computer. Virtual Machines have an array of specification and configuration files, supported by the physical resources of a host. All Virtual Machines have virtual endpoints, which do the same job as physical hardware, but are better in terms of portability, manageability, and security.

Organization (or **vOrg**) refers to a private virtual space provided by the VMware vCloud Director application, the software that underlies the Flexible Computing Advanced service. The Organization includes all Virtual Datacenters (vDC) created by the Customer to host their VMs.

Virtual Private Network (or **VPN**) refers to a local network extension that provides logical security within a local network. It is actually a way of interconnecting local networks using a "tunneling" technique. A VPN is used when an entity interconnects its sites using an infrastructure shared with other entities. These shared infrastructures come in two varieties: "public" shared infrastructures, i.e. the Internet and dedicated infrastructures created by operators to provide VPN services to businesses. "Tunneling" techniques were developed for IP infrastructures on the internet because they allow data moving from one end of the VPN to the other to be secured using cryptography algorithms.

Service refers to the "Flexible Computing Advanced" service provided for an Organization. Each Organization constitutes a separate Service.

Operating System (or **OS**) refers to a central set of programs used by a computing device as an interface between the hardware and software applications

vApp refers to a logical envelope within which VMs are created. This envelope helps to simply and coherently manage an array of VMs that are grouped together for some reason (functional or security). VMs can only be created within a vApp.

Virtual Central Processing Unit (or **vCPU**) refers to a virtual computer component that runs computer programs.

Virtual Datacenter (or **vDC**) refers to the VMware logical object of the same name. A vDC is a pool of computing resources (CPU power, RAM capacity), storage resources, and virtual networks (internet network and VPN access, firewall, load balancer) used to create a secure network architecture. An Organization includes one or several vDCs.

2 Purpose of the document

The purpose of the present Service Description is to define the "Flexible Computing Advanced" Service and to set forth the conditions under which it is provided by Orange Business Services, in application of General Terms and Conditions.

3 Service Overview

3.1 Overall description

The Service is a managed virtual Datacenter for Customers who wish to control the size and structure of their computing infrastructure and resources with as much flexibility as possible. It is an Infrastructure as a Service (IaaS).

3.2 Geographical footprint

The Service is available from the Val-de-Reuil and Rueil-Malmaison Datacenters in France.

These two Datacenters are about 100 km away from each other.

Each subscribed Organization is built using a given datacenter, in line with the Purchase Order.

The number of rooms available on the different datacenters is given in the table below:

Datacenter	Number of rooms
Val de Reuil	2
Rueil Malmaison	1

4 Terms of Use

4.1 Prices

The Service pricing are revisable, as per General Terms and Conditions.

4.2 Licenses

The Customer undertakes to use Software, including operating systems, in compliance with the article “Intellectual property” of the General Terms and Conditions.

4.2.1 Microsoft products

The Customer may either subscribe to Microsoft Software licenses from Orange Business Services 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).

4.2.1.1 Rental mode

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

4.2.1.2 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 the following operations:

- to have subscribed with Microsoft, when required by Microsoft, the "Software Assurance" (SA) which is an additional license to allow its mobility;
- for Mobility License, declare mobility to Microsoft, indicating ORANGE's references as a mobility partner, via a specific form published by Microsoft and provided to the Customer by Orange Business Services at the Customer's request;
- for QMTH, declare to Orange Business Services the number of Users for each Software concerned.

4.3 Scheduled maintenance

The recurring maintenance times are as follows: every first Wednesday of the month, from 0:00 am to 6:00 am. Exceptionally, maintenance may occur between 12.00 pm and 2 pm from Monday to Thursday. Should the Service be impacted, the Customer shall be notified as per General Terms and Conditions.

5 Service Access

5.1 Prerequisites

Resource administration and Virtual Machine management will be carried out using the vCloud Director administrator portal. The Customer must choose one of the following configurations for the computer they are using:

5.1.1 Windows Environment

Browsers and operating systems compatible with Microsoft Windows platforms

Platform	Google Chrome	Mozilla Firefox	Microsoft browsers
Windows XP Pro	Yes	Yes	IE 11.x

Windows Server 2003 Enterprise Edition	Yes	Yes	IE 11.x
Windows Server 2008	Yes	Yes	IE 11.x
Windows Server 2008 R2	Yes	Yes	IE 11.x
Windows Vista	Yes	No	IE 11.x
Windows 7	Yes	Yes	IE 11.x
Windows 8, 8.1	Yes	Yes	IE 11.x
Windows 10	Yes	Yes	IE 11.x, Edge

5.1.2 Linux Environment

Browsers and operating systems compatible with Linux platforms

Platform	Google Chrome	Mozilla Firefox
CentOS 7.x and previous	Yes	Yes
Red Hat Enterprise Linux 7.x and previous	Yes	Yes
Ubuntu 14.x and previous	Yes	Yes

5.2 Portals

5.2.1 VCD Portal

The administrative features of the Service are accessed using the vCloud Director (VCD) administrator portal. This technical portal requires knowledge of the network and security features to configure different networks and security rules.

The version of vCloud Director on each Datacenter is given in the table below:

Site	Current VCD release
Val De Reuil Datacenter	9.7
Rueil Malmaison Datacenter	9.7

The release notes and product documentation are available in the link below:

https://docs.vmware.com/en/VMware-Cloud-Director/9.7/com.vmware.vcloud.user.doc/GUID-D078FBD8-4704-4FB9-B112-C79349CC47DB.html

5.2.2 Accessing the VCD Portal and API

Access to the VCD portal and API is protected with an application firewall (WAF), which forbids access from the Internet by default. Access can be granted at the Customer's request during the initial order or through a change request in each Organization's Customer Space.

The VCD portal and API can be accessed without a WAF using the VPN Gallery access to which the Customer can subscribe.

5.2.3 Customer Space

The Cloud Store Customer Space is a Customer's personal space that allows them to manage their Flexible Computing Advanced account.

The Customer Space online documentation is available in French from this link: https://wiki.flexible-computing-advanced.orange-business.com/wiki/Fiches_pratiques

IMPORTANT

Communications about the Service are only made towards Users declared in the Customer Space. The Customer is in charge of adding the Users to be notified. Users must keep their information up to date (email, mobile number, fixed line).

5.3 Network

The VMs hosted on the Flexible Computing Advanced platform can be accessed in two ways:

- Over the Internet
- Using an Orange Business VPN with the Gallery option

These two access methods are not mutually exclusive. A vDC can handle an internet access and one or several BVPN accesses at the same time.

6 Service Content

6.1 Virtual Datacenter

A Virtual Datacenter (vDC) is an array of resources including:

- **Computing power**, expressed in GHz or vCPU, and with a quantity of RAM
- Storage capacity
- External network connections (internet or BVPN)

The computing power (CPU + RAM) and amount storage available varies across several service classes.

IMPORTANT

Each vDC has a service class and resource allocation mode (PAYG or Allocation Pool). A vDC's resource allocation mode cannot be changed after it has been created. If the Customer wishes to change the resource allocation mode for their vDC, they will need to order a new vDC and migrate their vApps/VMs over to it. However, the service class can be changed to any of the service classes available on the platform, outside of dedicated clusters.

6.1.1 vDC Specifications by Service Class

Service Class		Eco	Standard	High Perf.	VOIP
VM Limits (vCPU / RAM / Storage)		4 vCPU / 16G 4 TB	8 vCPU / 64G 4 TB	32 vCPU / 256G 6 TB	32 vCPU / 256G 6 To
Usage		Prod with low needs of CPU, Dev, test, labs	Prod, test, dev	Prod, Big Data, Real time	IPBX, Real Time
Allocation modes		PAYG and Allocation Pool	PAYG and Allocation Pool	Allocation Pool	Reservation Pool
One Room available		●	●	●	○
Dual Room available		●	●	●	●
HA Dual Room available		○	●	●	○
Available billing modes		PAYG, Mixed, Reserved and DRaaS	PAYG, Mixed, Reserved and DRaaS	Mixed and Reserved	Reserved
Frequency vCPU	PAYG or DRaaS	same as physical CPU	same as physical CPU	N/A	N/A
	Mixed	1.7 GHz	1.7 GHz	same as physical CPU	N/A
	Reserved	1.2 GHz mini	1.2 GHz mini	same as physical CPU	2.6 GHz

● = disponible sur demande

Note: the mention "same as physical CPU" refers to the physical frequency of the servers deployed on the infrastructure, which varies between 2.3 and 2.4 GHz depending on the generation of the hardware.

In the VOIP service class, the configuration implemented disables vMotion (the automatic movement of a virtual machine from one physical server to another) and VMware HA (the automatic restart of a VM hosted on a failed physical server on another physical server), in order to be compatible with the way most IP telephony solutions work.

6.1.2 Availability classes

On the Val de Reuil Datacenter campus, the Flexible Computing Advanced infrastructure is deployed in two rooms, each of which is totally independent of the other (energy, cooling, networks), making it possible to offer several classes of availability for a vDC:

- One Room,
- Dual Room
- HA Dual Room, also known as HADR.

6.1.2.1 One Room

This is the default configuration; vDCs are built on a single room, no matter which one.

This configuration is available for all performance classes, except for the VOIP class.

6.1.2.2 Dual Room

In this configuration, the Client wants to deploy VMs in two different rooms; the computing and storage resources are independent of each other.

To enable this configuration, the Client can order:

- Either two independent vDCs, one in each room (**One Room** vDC rates apply). Each vDC is assigned a different storage space, each located in a different room.
- Either a single vDC with two storage spaces, each located in a different room.

It is the storage, physically present in a single room, which ensures the location of the VMs in a given room.

Storage is also ordered for each room at the "**One Room**" rate.

In this scenario, if the application supports it, the loss of a room does not affect the availability of the application.

This configuration is available for all performance classes.

6.1.2.3 HA Dual Room (HADR)

In this configuration, the computing and storage resources are spread over the two rooms, thus providing the very high availability of the infrastructure (computing + storage). This is called HADR (High Availability Dual Room).

To enable this configuration, the Client must order a single vDC in **Dual Room** mode (Dual Room vDC rates apply), the ordered storage will be automatically provisioned in **Dual Room** mode, and the vDC gateways will also be deployed with the **HA option enabled**. Storage is written to both rooms simultaneously and is therefore always available.

In case of loss of a room, the VMs located in the failed room will automatically reboot on the ESXi of the other room.

This configuration is only available for **Standard** and **High Performance** classes.

The availability rates guaranteed by Orange Business Services for each of the availability classes are specified in the Quality of Service document.

6.1.3 vDC Resource Management

The Customer chooses how vDC resources will be allocated. Allocation can be configured when the vDC is ordered, can be modified through a change request, and may even change several times based on the Customer's needs.

vDC resource allocation is a "physical" limit that VMs will not go beyond when running.

6.1.4 Computing Power Allocation Modes

6.1.4.1 Allocation Mode PAYG

With this allocation mode, resources are expressed in numbers of vCPUs (= Limit in GHz / vCPU frequency) and in GB of RAM.

In a "PAYG" configured vDC, resources will be allocated to VMs on an individual basis. When the VM starts up, its vCPU and RAM allocation is subtracted from the total amounts allocated to the vDC. VMs cannot consume more resources than they are allocated. This is a limit.

The billing method used is usage-based payment (PAYG: Pay As You Go).

6.1.4.2 "Allocation Pool" Allocation Mode

With this allocation mode, resources are expressed in GHz and GB of RAM. These resources are a maximum usage limit with a guaranteed minimum reservation. Resource allocation for all VMs is done globally when creating the VDC. Unlike PAYG, there is no limit per VM and its consumption can be adjusted according to the needs and the total usage of the VMs in the VDC (without exceeding the total limit).

vCPU frequency is set:

- At 1.7 GHz and cannot be changed by the Customer in mixed billing mode.
- By the Customer in reserved billing mode, when the vDC is ordered, with a minimum of 1.2 GHz.

The physical processors used in the storage platform have variable frequencies depending on the physical server generation, ranging generally between 2.3 and 2.6 GHz. The "Allocation Pool" mode allows the vCPUs of initially configured VMs to consume up to the maximum processing power provided by a physical processor (e.g. 2.3 GHz). This "burst" effect will activate under certain conditions:

- A VM that is subject to heavy CPU loads may periodically use extra power.
- There are GHz available (not in use) in the vDC.

This allocation mode is recommended for vDCs whose VMs are permanently on.

6.1.4.3 "Reservation Pool" allocation method

In this allocation mode, resources are expressed in GHz and GB of RAM. But contrary to the "Allocation Pool" mode, it is a firm reservation and therefore a guaranteed minimum as well as a guaranteed maximum reservation. The allocation of reserved resources (therefore guaranteed minimum) of a VM is this time done individually VM by VM by the administrator of the organization throughout the life of the VDC. It is a fine and total control by the organization administrator of his resource.

The resources allocated to each VM are 100% guaranteed for the VMs, which requires an adapted dimensioning when defining the VDC so that all VMs intended to operate can start.

This principle of resource allocation is used for VOIP-type vDCs, which allows telephony or videoconferencing applications to operate with the maximum possible isolation from their environment.

6.1.5 Computing Power Billing Modes

There are four billing modes available.

Billing Plan	Usage-based	Mixed	Reserved	DRaaS
Resource allocation	PAYG	Allocation Pool	Allocation Pool Reservation Pool	PAYG
Billing	Resources allocated to running VMs	% of vDC resources (according to class of service) + resources allocated to running VMs	100% of vDC resources	resources allocated to running VMs

In Mixed mode, a portion of the vDC's resources is invoiced monthly, based on the average value of the resources allocated during the month. Depending on the class of service, this invoiced reserve is detailed in the Price List.

6.1.5.1 "PAYG" and "DRaaS" Billing

PAYG & DRaaS	Compute	RAM
work unit invoiced (WU)	vCPU	GB
quantity invoiced	Number of vCPU allocated to each running VM X number of minutes / day	Quantity of RAM allocated to each running VM X number of minutes / day

Usage time is billed by the minute.

A vDC in DRaaS mode is used when setting up VM replication between the Customer's private infrastructure (On Premise) and the Flexible Computing Advanced platform.

6.1.5.2 "Mixed" Billing Plan

Mixed	Compute	RAM
work unit invoiced (WU)	vCPU	GB
quantity invoiced	(% of the total quantity of GHz allocated to the vDC X Number of days / month) + (Number of vCPU allocated to each running VM X number of minutes / day)	(% of the total quantity of RAM allocated to the vDC X Number of days / month) + (Quantity of RAM allocated to each running VM X number of minutes / day)

With this plan, the Customer is billed for:

- Allocated VM GHz and RAM based on usage (PAYG)
- A portion (30%) of GHz and RAM allocated to the vDC, lump-sum payment (reserved).

6.1.5.3 "Reserved" Billing Plan

With this plan, all of a vDCs GHz and RAM resources are billed on a lump-sum basis. This allows the Customer to take advantage of better rates.

Mixed	Compute	RAM
work unit invoiced (WU)	vCPU	GB
quantity invoiced	% of the total quantity of GHz allocated to the vDC X Number of days / month	Quantity of RAM allocated to each running VM X number of minutes / day

6.1.6 vDC "Dedicated Cluster" Class

6.1.6.1 Introduction

The Standard service class is based on shared resources, for which Orange provides Cloud licenses, i.e. usage-based payment licenses. However, when the Customer has certain requirements, or in order to adapt to some usage types (for example, needing to use Customer Licenses), Orange Business Services can offer a private group of physical servers within the shared platform.

Orange Business Services provides the necessary tools for the Customer to verify that their VMs were not able to function outside of the dedicated cluster, so that the Customer can ensure that they are in compliance with Customer License rules.

6.1.6.2 How does it work?

The Customer orders several physical servers to create a "provider vDC", dedicated to them, and on which a vDC is built, containing all of the resources available from the physical servers. It should be noted that the Customer can ask for several vDCs to be created on their cluster.

The resource allocation mode is the "Allocation Pool". This resource allocation mode has several advantages:

- Limits are set at the vDC level, and in our case, are the same as the physical cluster's capacity. This allows VMs to access more resources when they are available in the vDC ("burst mode").
- The percentage of guaranteed resources and the vCPU frequency can be configured when the vDC is created, allowing the Customer to manage the consolidation ratio themselves.

The following parameters can be set when the vDC is created:

- CPU reservation percentage
- RAM reservation percentage
- vCPU frequency in GHz

Besides these parameters, it is the number of VMs that the Customer chooses to create in the vDC that will determine the rate of overbooking.

6.1.6.3 High Availability

In order to not compromise application availability if a blade is lost, the Customer must size the cluster with enough capacity to make up for the loss of a blade. Defective blades will be replaced by Orange Business Services within 48 hours. However, during this time, VMs must be able to run on a cluster that is one blade short without significantly impacting the performance of the hosted applications. **This sizing is the Customer's responsibility**.

6.1.6.4 Capacity management

Capacity management is up to the Customer. Orange Business Services will provide the Customer with VMware indicators that will allow them to track overall cluster performance, as well as VM performance.

Note: it is the Customer's responsibility to decide whether or not to modify the size of the cluster.

Orange Business Services will install a blade within 1 month, maximum, from the date the Order is placed.

Any requests to add more than 2 blades will be handled within 3 months.

The initial installation of the dedicated cluster will coincide with a maximum output study done by the Customer, and approved by Orange Business Services.

Other resources (storage, network, etc.) are provided in line with standard Flexible Computing Advanced processes and will be billed based on the current price list.

6.1.6.5 Subscription to a Dedicated Cluster

The minimum size for a cluster is two servers of the same type.

Billing is done monthly based on the number of reserved physical servers and based on their specifications.

Orange uses "blade" type physical servers with the following specifications:

Specifications	
CPU	Intel Xeon
CPU Frequency	2.3 GHz
No. of CPUs	2
No. of cores/CPU	18
No. of vCPU / blade	36
RAM	512 GB
vDC allocation type	Allocation Pool

A blade that is added during a month is only billed for the number of days during which it was active.

For each subscribed blade, the minimum commitment is 6 months.

6.2 Orange template catalog

All VCD administrator accounts can access the public Orange catalog, which provides vApp templates that are ready to use. These vApps contain only one VM, which comes with an Operating System already installed and pre-configured.

The Customer can also manage their own template catalogs. Storing these private catalogs uses storage space from the available storage in the first vDC on the list displayed by vCloud Director.

All Windows and RedHat operating system licenses must be purchased through Flexible Computing Advanced. The price list provides the prices and billing methods for each license.

Note: when a Customer imports a VM using the VCD interface or API and this VM includes a Windows or Redhat operating system, the Virtual Machine will automatically be identified as carrying a billable license, and will be subject to normal invoicing the month following its import.

6.3 Network and Security

6.3.1 Organization networks

Organization Networks are created and configured by the Customer. It is important to choose the configuration parameters of these networks carefully because, once created and connected to vApp/VMs, they can no longer be modified, unless all vApp/VMs connected to them are disconnected.

The IP address ranges are chosen by the Customer, generally in non-routable address ranges.

6.3.2 Edge Gateway

Flexible Computing Advanced's network layer and security are managed by VMware's NSX solution. Implementation is carried out on two levels, based on the following:

- "Provider Edge Service Gateway" level, which includes the NSX gateways connected to various external networks (Internet, VPN Gallery, etc.). Gateways on this level are managed by Orange Business Services. A separate gateway is created for each external network.
- "vDC Edge Gateway" level, which includes Edge Gateways connected to vDCs and carrying different networks for the Organization. Gateways on this level are managed directly by the Customer using the VCD portal.

With this architecture, the Internet or VPN Gallery bandwidth subscribed to by the Customer for each Organization is set to be at the "Provider Edge Service Gateway" level and shared between different vDCs.

A vDC Edge Gateway makes it possible to create Organization networks that can be shared by all Organization vDCs. Each vDC Edge Gateway can be connected to a single gateway on the Provider Edge level.

The Customer can ask Orange Business Services to limit the bandwidth of a vDC Edge Gateway. For example, if several vDC Edge Gateways are connected to the same Edge Gateway on the Provider level, the bandwidth used by the various vDCs can be controlled.

Two levels of vDC Edge Gateway resilience are available:

- "Standalone" mode: resilience is provided by the VMware HA option, which makes it possible to restart a VM in less than a minute.
- High Availability (HA) mode: activates a second gateway, and the two work as a cluster, with a maximum 9 second delay to switchover from one to the other in case of a problem.

Two levels of vDC Edge Gateway interface management are available:

- **Standard** (default) – settings for the following features: Router, Firewall, NAT, DHCP, Load Balancer and IPSec and RedHat (point to point).
- **Advanced** – access to all VCD network features: Firewall, NAT, DHCP, (dynamic) Routing, Load Balancer, IPSec VPN, SSL VPN-Plus (remote access) and SSL Certificates (implementable in the Load Balancer), as well as:
  - A distributed firewall, which makes it possible to use the VMware NSX micro-segmentation mechanisms.
  - A complete Load Balancer based on HA proxy software that can, among other things, handle SSL offloading.

The complete documentation that describes the NSX features built into VCD 9.7 is available here:

https://docs.vmware.com/en/VMware-Cloud-Director/9.7/com.vmware.vcloud.tenantportal.doc/GUID-FA1B782D-7E76-4AB9-9EB9-E0A11401BEB0.html

Customers can switch from the standard level to the advanced level whenever they want to. It is not possible to switch from the advanced level to the standard level.

6.3.3 External Networks

Two types of connection are available in standard mode:

- Internet connection
- Connection to an Orange Business Services VPN Gallery

Connections to another network (third-party VPN, for example) is available through the Cross Connect option.

6.3.4 Distributed Firewall

It is possible for the Customer to set firewall rules directly at the Virtual Machines level. This is called micro segmentation. Unlike a perimeter firewall, which defines trust zones and filters flows between these trust zones, the distributed firewall implements filtering rules directly at the Virtual Machine "VM Kernel" level, which allows virtual trust zones to be built, even though the VMs are on the same network (same "subnet").

These filter rules are set via the VCD portal, from the context menu of a vDC.

The advantages of using the distributed firewall:

- The security rules remain valid after the VM has moved to another vDC
- The protection is valid in the “east-west” direction; even if a network machine located after the perimeter FW is compromised, the security rules continue to protect the other network machines.

6.3.5 Intranet Access

FCA Organization “Intranet” connections are connections to an Orange Business BVPN Gallery WAN belonging to one or several of the FCA Organization’s vDCs. No matter the platform (OCP or NUP), the Customer must first enter into an Orange Business VPN contract with the Gallery option (“BVPN Gallery”).

Once the prerequisites have been met (BVPN Gallery contract signed with reserved bandwidth), the Customer must purchase one of the three Gallery Access Virtual Port (GAVP) options in connection with their Flexible Computing Advanced Contract:

GAVP type	Capacity
Type 1	1-200 Mbps
Type 2	201-500 Mbps
Type 3	501 Mbps to 1 Gbps

These virtual ports are configured for unlimited traffic and are billed as monthly subscription services.

6.3.6 Internet access

The proposed internet access is a shared access for all FCA platform customers located on a Datacenter.

The Internet connection can be shared by all the Organization's vDCs (see diagrams 1 and 2). Orange Business Services is setting up an NSX Edge gateway in the Provider Edge area. This gateway, called the Provider Edge Service Gateway Internet (PESGi) operates in two billing modes:

- PAYG
- Reserved (legacy model)

Only outgoing bandwidth is charged.

6.3.6.1 PESGi in PAYG mode

The outgoing bandwidth is not limited. The bandwidth value invoiced is the 95th percentile of all values sampled every 5 minutes during the month (value such that 95% of the measurements are lower and 5% higher).

In this subscription mode, the incoming bandwidth limit is set at 1 Gbps ; this limit can be fine-tuned on demand.

6.3.6.2 PESGi in reserved mode

Bandwidth is limited and reserved. The value of bandwidth invoiced is the one reserved by the Customer. It does not include an automatic burst mechanism.

This bandwidth can be modified via a change request in the Customer Area. Bandwidth is billed monthly according to the number of Mbps reserved. In case of bandwidth adjustment during the month, the billed bandwidth is calculated prorata temporis..

In this subscription mode, the outgoing bandwidth value is aligned with the incoming bandwidth value

6.3.6.3 Public IP Addresses

Public IP address ranges are billed by the day, starting on the date the Customer's configuration is put into place. IP addresses can be made public with a change request. These addresses are no longer billed once they are no longer part of the Customer's configuration.

Public IP addresses can be ordered from the change request management portal.

By default, a public IP address is configured in double NAT. Other configurations are possible, and can be set up on request

See the wiki for a detailed description of the different possibilities.

6.4 Storage

6.4.1 Overview

Two types of storage are available:

- "Datastore" storage for VMDK files
- Network storage, with NFS protocol

The different types of storage and their classes of service are specified in the Price List and described on the Storage page of the Service Catalog on the wiki.

6.4.2 Datastore storage

The "datastore" storage is made available to the VMs in a vDC in the form of storage profiles, from which the VMs can draw to provision their disks. The size of a VMDK file is limited to 2TB. When a VM needs to have storage greater than 2TB, add multiple VMDK files to the VM to reach the target size.

External storage is made available to the VMs via IP addresses and according to the protocols chosen by the Customer.

"Datastore" type storage is provided in two ways:

- Shared storage (by default),
- Dedicated storage, with guaranteed performance.

6.4.2.1 Classes of services

For each vDC performance class, one or more storage performance classes can be associated; the compatibility matrix describes them in the following table:

Service Class	Limit IOPS	Availability by vDC			
		Eco	Standard	High Perf	VOIP
Silver	600 IOPS / To	●	●	●	●
Gold	1000 IOPS / To	●	●	●	●
Platinum 3K	3000 IOPS / To	○	●	●	●
Platinum 5K	5000 IOPS /To	○	●	●	●
Platinum 10K	10.000 IOPS / To	○	○	●	●

Certain service classes are available in Dual Room to offer the choice of room, and in HA Dual Room on the storage Metrocluster, spread over two rooms in Val de Rueil. The characteristics and availability of these service classes are detailed in the following table:

Service Class	Limit IOPS	Availability by vDC		
		One Room	Dual Room	HA Dual Room
Silver	600 IOPS / TB	●	●	○
Gold	1,000 IOPS / TB	●	●	●
Platinum 3K	3,000 IOPS / TB	●	●	●
Platinum 5K	5,000 IOPS / TB	●	○	○
Platinum 10K	10,000 IOPS / TB	●	○	○

Several storage profiles can be associated with a single virtual machine. The IOPS resources are shared between all the VMs using the Datastore on which the Customer deploys his VMs.

6.4.2.2 Billing

6.4.2.2.1 Shared datastore PAYG

Billing covers the maximum disk space used throughout a day by:

- Each VM, including the space used by the VM and any snapshots taken by the Customer
- ISO images and templates in the Customer's private catalog

VM technical files such as the vmware swap file also consume space, but are not charged.

The sizing of the storage of a vDC ordered by the Customer must take into account:

- The virtual disks of the VMs that will be created in this vDC
- The RAM of the VMs
- Possibly the space to make a snapshot.

6.4.2.2.2 Shared datastore by subscription

Billing covers the observed average storage allocated to the vDC during the reference month.

6.4.3 Network storage

6.4.3.1 Overview

Network storage is shared between the VM of a Customer organization. Network storage is always provided through a dedicated datastore.

6.4.3.2 Classes of service

Service Class	Limit IOPS	Availability by vDC		
		One Room	Dual Room	HA Dual Room
Silver	600 IOPS / TB	●	○	○
Gold	1,000 IOPS / TB	●	○	○
Platinum 3K	3,000 IOPS / TB	●	○	○

The quantity of IOPS actually supplied corresponds to the volume of storage ordered times the number of IOPS / GB of the class of service subscribed.

Example:

500 GB of Platinum 3K network storage allows for permanent use of 1500 IOPS, regardless of the number of VMs using that storage.

6.4.3.3 Billing

Billing covers the observed average storage allocated to the Customer during the reference month.

The quantity of IOPS actually delivered corresponds to the storage volume ordered times the number of IOPS/Go of the service class subscribed.

6.4.3.4 Backup

The Customer can set up himself the snapshot policy for its network storage. The space used by the snapshots is deducted from the quota subscribed by the Customer. Depending on the policy chosen, the Customer must reserve between 10 and 20% of the total subscribed storage quantity for snapshots.

6.4.3.5 Management portal

A self-service portal is provided to make the Customer autonomous in the management of network storage. With the help of the portal, the Customer can:

- Adjust the quotas of its shared volumes
- Set up rights, manage the list of VMs with access to a shared volume
- Restore all or part of a backup snapshot

6.4.4 Dedicated datastore storage

6.4.4.1 Overview

A datastore is dedicated to a Client. In other words, only the VMs that the Customer has chosen can use this storage space.

The datastore works with a QoS rule that constraints the number of IOPS that the volume can draw from the storage.

This type of storage is available;

- In One Room, and for some classes in Dual Room (on a storage Metrocluster).
- With or without encryption.

6.4.4.2 Classes of service

It is possible to order a dedicated datastore for all the following service classes:

Service Class	Performance	Minimum size	Availability by vDC			Encryption available
			One Room	Dual Room	HA Dual Room	
Silver	600 IOPS / TB	8 TB	●	●	○	●
Gold	1,000 IOPS / TB	6 TB	●	●	○	●
Gold Metrocluster	1,000 IOPS / TB	6 TB	○	○	●	●
Platinum 3K	3,000 IOPS / TB	4 TB	●	●	○	●
Platinum 3K Metrocluster	3,000 IOPS / TB	4 TB	○	○	●	●
Platinum 5K	5,000 IOPS / TB	4 TB	●	●	○	○
Platinum 10K	10,000 IOPS / TB	4 TB	●	●	○	○

The quantity of IOPS actually delivered corresponds to the storage volume ordered times the number of IOPS/Go of the service class subscribed.

Important: For a dedicated Datastore, the deduplication mechanisms embedded in the storage equipment benefit the Customer. That is, if the Customer deploys multiple VMs based on the same template, this will significantly increase the rate of deduplication, and therefore limit the total amount of storage charged to the Customer.

6.4.4.3 Billing

Billing covers the observed average storage allocated to the Customer during the reference month.

6.5 SUO Tools services

6.5.1.1 Overview

The SUO Tools zone (Services for Unmanaged Offer) is a service area that can be accessed by VMs through a specific Organization network that covers the entire Organization and provides several services:

- Sophos Antivirus
- Windows and Redhat license activation
- Windows and Redhat OS updates

- Access to backup servers (for using an agent to backup/restore VMs)
- Access to e-mail relay gateways
- NTP Server

Availability of these procedures avoids VM internet exposure.

Note: All virtual machines of the same Organization (vOrg) can be connected to this service area via an Organization network shared between all the vDC of the Organization. The connected virtual machines have a second IP interface (virtual Ethernet card) and share the same IP addressing scheme. They can technically communicate with each other. If the Customer wishes to keep on this SUO Tools network the zones of trust set up on the other Organization networks, is the Customer must configure security rules using the configurable distributed Firewall for each vDC of the Organization.

6.5.2 Antivirus

Every Windows template includes a Sophos agent, which automatically updates its signature database from the central console, which the Customer cannot access.

6.5.3 License Activation

The SUO Tools area has a KMS server that helps activate Windows licenses. Windows templates in the Flexible Computing Advanced public catalog are pre-configured and are easy to activate. For imported or "from scratch" VMs, the Customer is given a procedure to follow to manually make the system activated from the SUO Tools area.

The SUO Tools area has an RHN infrastructure for Redhat VM, which makes it possible to activate and update the operating systems.

6.5.4 OS Updates

The SUO Tools area has a WSUS server that helps to update Windows VMs. For Redhat VMs, the SUO Tools's RHN infrastructure provides access to the Redhat repository.

6.5.5 Accessing Backup Servers with the NetBackup Agent

If a NetBackup agent has been installed on a VM, it can be accessed using SUO Tools.

6.5.6 Accessing SMTP Gateways

The SUO Tools area also has a complete SMTP e-mail relay server infrastructure. These servers are protected with antivirus software.

With a simple change request, the Customer's servers can also benefit from this infrastructure.

The service is:

- **Paid** and billed to the server IP address of this service's "customer"
- **Limited** to 200 e-mails sent per day and per IP

This service cannot be used for mass mailing type usages.

6.6 Backup Service

6.6.1 Overview

The FCA service's backup option is a self-service backup option provided by the NetBackup Self-Service solution. This option has several features:

- Web portal control of the solution (NSS portal)
- VM backups based on several pre-defined policies. Backups are local, i.e. the data are saved to the same Datacenter that hosts the VM.
- VM restoration, file restoration via the NSS portal
- Backup externalization, with replication to a remote site (only for the OCP platform)
- Backup and restoration in agent mode (not the NSS portal) using the local interface
- Service forecast (daily report)

This feature is activated when the Customer's Organization is created, and in VM mode only. A change request is needed to activate the agent mode.

6.6.2 NetBackup Agent and NSS Portal Features

	Without agent	With agent
Envelope backup (VMDK)	●	○
Backup of a file, a system file, or a partition	○	●
Total VM restoration (including the envelope)	●	○
Restoration of a file, a system file, or a partition	○	●

6.6.3 VM Backups and Restoration

Using the NSS portal, you can:

- View your Organization's protected / non-protected VMs
- Protect VMs by applying a pre-defined backup policy to them
- Restore a locally backed up VM (completely or partially)
- Remove protection from a VM
- Back up a VM immediately
- View the backed up data volumes by VM and the total volume used by your backups

Policies have different settings:

- Local backup frequency
- Local retention duration
- Backup range
- Off-site option (replication to a remote site)

Backup modes, frequency and available retention values are as follows:

Backup policies	Description
Policy #1	[**DAILY-6**] 1 backup / day – Retained for 6 days
Policy #2	[**DAILY-30**] 1 backup / day – Retained for 30 days
Policy #3	[**WEEKLY-4**] 1 backup / week – Retained for 4 weeks
Policy #4	[**MONTHLY-3**] 1 backup / month – Retained for 3 months
Policy #5	[DAILY-6] + [WEEKLY-4]
Policy #6	[DAILY-6] + [WEEKLY-4] + [MONTHLY-3]
Policy #7	[DAILY-6] + [MONTHLY-3]
Policy #8	[DAILY-30] + [MONTHLY-3]
Policy #9	[WEEKLY-4] + [MONTHLY-3]
Policy #10	[**MONTHLY-12**] 1 backup / month – Retained for 12 months
Policy #11	[DAILY-6] + [MONTHLY-12]
Policy #12	[DAILY-30] + [MONTHLY-12]
Policy #13	[WEEKLY-4] + [MONTHLY-12]
Policy #14	[DAILY-6] + [WEEKLY-4] + [MONTHLY-12]
Policy #15	**[DAILY-60]** 1 backup / day – Retained for 60 days
Policy #99	[SPOT] 1 backup operation at the customer's discretion – Retained for 31 days
Policy #nX	Same as policy #n (except for #99), but with an extra replication of the local backup to a remote site, fulfilling the need for **off-site backups**.

Backup policies	Description
Policy #nZ	Same as policy #n (except for #99), but with encryption of the backup

A daily (preferably generic) report, called the "Service Forecast" is e-mailed to the Customer every day, listing the status of the previous night's backups.

Note: By default, the NSS portal allows VM restoration without an agent. For a more granular restoration (of a file, directory), a NetBackup agent will need to be installed on the VM. The Customer will install the agent, with help from the user guide provided with the FCA reference documents.

6.6.4 NSS Backup Execution Window

By default, backup jobs (except for "backup now", i.e. policy #99) are run between 10 pm and 6 am.

In certain instances, the Customer may want some of these backup jobs to run during a shorter window (2 hours), to make more time in the production plan. That is why Orange provides custom policies that allow the Customer to choose the time slot that best fits their needs.

6.6.5 Backup encryption

Policies suffixed with a Z are policies whose backups are encrypted directly on the backup storage. This functionality makes it possible to meet certain security requirements attached to the Customer's obligations towards its own end customers.

6.6.6 Off-Site Backups

Backup policies with an 'X' after their number have their backups replicated at a remote site. This means that there are two restoration sources: one local and one remote.

Data replicated at this remote site cannot be restored using the self-service NSS portal, but Orange Business Services can activate this feature at the Customer's request.

6.6.7 Policies in Agent Mode

In some instances, the Customer can use the NetBackup agent to back up their VMs. The Customer controls how frequently backups are made, based on a schedule created by the Customer in the VM's operating system, or with a third-party tool. The different retention policies are listed in the table below:

	Frequency	Retention
Agent Policy #1	1 on-demand backup	6 days
Agent Policy #2	1 on-demand backup	1 month
Agent Policy #3	1 on-demand backup	3 months
Agent Policy #4	1 on-demand backup	12 months

Note: Backups and restorations in agent mode are executed directly from the agent's VM and not through the NSS portal.

The agent has two operating modes: command line and graphical interface.

6.7 VM Replication between two Flexible Computing Advanced sites

6.7.1 Overview

This feature provides the Flexible Computing Advanced service with the ability to resume activity after an accident by replicating VMs from the Flexible Computing Advanced primary site to a Flexible Computing Advanced backup site. This solution uses Zerto software (Zerto Virtual Replication, or "ZVR"). The replication technology used may change at a later date.

This solution has a self-service portal, which is made available to the Customer.

This feature makes it possible to:

- Protect all or some of your virtual machines
- Manage the switchover and the restoration between the primary site and the backup site

This feature also has the following advantages:

- The Customer is able to freely switch environments on their own schedule
- Agnostic data protection for the application and infrastructure, since the virtual machines are protected in the hypervisor layer

Note: Zerto does not protect against data corruption, since it replicates even corrupt data from the source VM. The only way to restore data from before a corruption event is to restore a backup.

6.7.2 Self-service Protection

The Customer can change the number of protected Virtual Machines whenever they want. Orange adjusts the fees it charges based on how many VMs are protected.

The smallest protection unit is the vApp. The Customer can add and remove VMs from vApps whenever they want. Any VM that is added to a protected vApp is also automatically protected.

The Customer can configure their vApps using the provided web portal, which is based on the Zerto Self-Service Portal (ZSSP).

Orange Business Services does not provide any services within this feature to help select VMs for protection or to help implement these protections. These tasks are the exclusive responsibility of the Customer. However, Orange Business Services may offer complementary services by request to meet the Customer's support needs.

6.7.3 Testing for Recovery and Restoration after an Incident

The freely available Zerto portal allows the Customer to test and execute switchover drills for protected applications.

The Customer is responsible for organizing and running post-incident recovery tests and primary site activity restoration tests. The Customer will incur no further costs for testing this feature, unless there are cost overruns for using the Flexible Computing Advanced service itself.

Orange Business Services may also, by request, assist the Customer in organizing, running, and analyzing these tests. The Customer nevertheless remains generally responsible for configuring the tool, running the test, and confirming the ability to recover and restore after an incident according to their needs.

6.7.4 Recovery Environment

The recovery environment is configured by the Customer, using the site-dedicated VCD web portal. The Customer can organize their backup vDC as they want.

The Customer will be able to access the backup administrator portals and virtual machines (provided with public IP addresses) directly over the Internet.

The storage profile chosen for the recovery environment may be different from the profile chosen for the primary environment. For example, data stored in a Gold storage environment may be replicated in a Silver storage environment.

6.7.5 Physical Servers

VM replication only protects vApps from the Flexible Computing Advanced primary site, and not any co-located physical servers that may be associated with Flexible Computing Advanced.

If the Customer wants a DRP for their collocated spaces, it is their responsibility to deploy the required tools and organize a DRP. However, Orange may offer complementary services by request to meet the Customer's specific needs.

6.7.6 Activating the VM Replication Option

In order to use the VM replication feature, the Customer must have at least one Organization at the primary site and one Organization at the backup site.

The VM replication option is one of the Flexible Computing Advanced primary site services.

After the feature has been activated, Orange will send the Customer their login information for the Zerto self-service portal, along with a user guide.

Note: This "VM replication" option must be purchased for each of the primary Flexible Computing Advanced Organizations covered by the DRP that the Customer wishes to put into place.

6.7.7 Billing

This option is billed using 3 billing units:

- A monthly fee for each protected VM.
- A monthly fee for protection storage, i.e. how much storage is actually used by the protected VM that is replicated at the backup site.
- A fee for the bandwidth used each month to replicate modified data from the primary VM.

6.8 Flexible Recovery Advanced

6.8.1 Description

Flexible Recovery Advanced provides the Customer with a solution to protect its business on its private infrastructure. Flexible Recovery Advanced enables the Customer to respond to failures and disasters affecting applications or infrastructure at the Customer's nominal site.

Flexible Recovery Advanced is based on replication of the customer's VMs and associated data to the Orange Business Services Flexible Computing Advanced platform. The customer then has the means to recover, and to test the recovery, of its activity, using Flexible Computing Advanced as the test and recovery site.

Orange Business Services provides customer support for the deployment and getting started with Flexible Recovery Advanced. However, the Customer remains solely responsible for maintaining the protection of its activity in operational conditions and for switching its activity to the recovery site.

Logs of recovery points are at the disposal of the Customer, who sets the retention period. In the event of data corruption, if the recovery logs date back to a time prior to the corruption, Flexible Recovery Advanced allows to restart activity based on the data prior to the corruption.

This activity protection solution is now based on Zerto's virtual replication software. However, the replication technology may evolve.

6.8.2 Perimeter and limits of protection

Flexible Recovery Advanced allows to protect, at a Customer site, only the servers that are virtualized using VMware (version 5.0 or higher). The Customer chooses the VMs he wants to protect.

Flexible Recovery Advanced is neither a disaster recovery plan nor a business continuity plan, but it's a tool that can be used by the Customer to implement its own disaster recovery plan.

Flexible Recovery Advanced does not include:

- the selection of VMs to be protected;
- the implementation of these protections;
- the end-to-end supervision of the protection;
- the activation of the recovery environment;
- the restoration of activity at the nominal site.

These tasks are the sole responsibility of the Customer. However, Orange Business Services may offer, upon request, services to support the Customer.

6.8.3 Prerequisites

The prerequisite for Flexible Recovery Advanced is that the Customer subscribes to a vDC in DRaaS mode and that he connects the Flexible Computing Advanced platform to its own network. These connections can be made at the Customer's discretion:

- by Business VPN Galery
- by Internet, in IPsec
- by any other method of connection, validated by Orange Business Services, on request

6.8.4 Performance

Orange Business Services does not make any commitment on RPO (Recovery Point Objective) or RTO (Recovery Time Objective). In order to benefit from the best performance offered by the solution (RPO of a few seconds and RTO of a few minutes) the Customer is responsible for:

- The dimensioning of its resources according to the load of its applications;
- The sizing of the bandwidth between its nominal site and the recovery site;
- The design and implementation of the fail-over process;
- The multi-annual fail-over tests.

The Customer can view the freshness of the replicated data on the recovery site via the Zerto Self-Service Portal (ZSSP).

6.8.5 Tariff structure

This section describes the various costs that the Customer has to consider when implementing activity protection using Flexible Recovery Advanced.

6.8.5.1 Protection infrastructure costs

The following table shows the costs incurred by the Customer in the context of a DRaaS:

Mode : / Incurred costs	Protection	Test	Recovery	
The protection of the concerned VMs	●	●	●	Flexible Recovery Advanced own costs
A Zerto Cloud Connector per subnetwork to be protected	●	●	●	
Release management of the protection solution	●	●	●	
Storage of protective data on Flexible Computing Advanced	●	●	○	Additional costs on Flexible Computing Advanced to be taken into account
The Flexible Computing Advanced outward connection subscription	●	●	●	
CPU/RAM/Storage activity of test or production VMs at the recovery site	○	●	●	
OS licenses used on test or production VMs at the recovery site	○	●	●	

6.8.5.2 Initial costs

In order to support the Customer in the deployment and the getting started with Flexible Recovery Advanced, support services must be subscribed to by the Customer. At the time of the study, Orange Business Services will determine the number of Flexible Expertise packs to be subscribed to, depending on the complexity of the Customer's configuration and the number of people to be trained.

6.9 Cross Connect

This option is only available from the Val de Reuil Datacenter and allows a Customer's hardware located in an Orange Flexible Computing Advanced Datacenter to be connected.

Orange offers several connection types:

- One 1 Gbps connection
- Two 1 Gbps connections, primary/backup
- Two 1 Gbps connections, primary/backup with link aggregation, bringing nominal speed to 2 Gbps
- One 10 Gbps connection
- Two 10 Gbps connections, primary/backup
- Two 10 Gbps connections, primary/backup with link aggregation, bringing nominal speed to 20 Gbps

6.9.1 Prerequisites

The Customer must:

- Already have operational storage space in one or several rooms of the Datacenter
- Have the network hardware needed to connect to the Orange Business Services infrastructure
- Provide the information needed to make physical connections (room / bay / hardware name / port)
- Provide the routes that need to be entered into Orange Business Services' configuration (no dynamic routing, static routing only)
- Provide the necessary configuration elements for the proper functioning of the entire link chain.

6.9.2 Activating the "Cross Connect" Option

The Customer and Orange Business Services' technical teams will need to collaborate to activate this option and configure the entire connection route. This option may be requested in the initial purchase order, or requested from the Customer Space.

6.10 Quality of service Appliance (QoSa)

6.10.1 Overview

The quality of service, or QoS (quality of service) designates a mechanism making it possible to ensure the prioritization of the most important flows in a limited bandwidth.

Customers who use their BVPN access to connect to their information system hosted on FCA may encounter contention problems when the bandwidth subscribed to on the site's BVPN access is limited.

"Real-time" type applications, most of the time communication applications (telephony over IP, videoconferencing, etc.) will suffer greatly from this contention and have a significant drop in the quality of sound and image.

To avoid this, it is necessary to put in place Quality of Service mechanisms, in order to prioritize the most critical ones.

6.10.2 Proposed solution

Flexible Computing Advanced offers an "Appliance" to fulfill this task of prioritizing the most critical flows. Each "QoS Appliance" is dedicated to an Organization, and one QoSa per BVPN link is required.

There are three models of "QoS Appliance", sized to be able to process all flows within the limit of a maximum bandwidth.

Model of QoS Appliance	Appliance maximum throughput
Small	50 Mbps
Large	500 Mbps
X-Large	2 Gbps

6.10.3 Prerequisites

The Customer must have a GAVP (Gallery Access Virtual Plug), as well as an Orange Business VPN Gallery contract taken out with his usual Sales Agency.

Customer applications must use DSCP marking of network packets.

6.10.4 Billing

Invoicing is carried out monthly, in proportion to the number of days of the month during which the QoS Appliance has been active, on the basis of the tariff sheet in force.

6.10.5 Deployment

The implementation of the QoS Appliance is done from the Customer Space of the Cloud Store. It is hosted in a secure area on the Flexible Computing Advanced platform and maintained in operational conditions by the Operations teams of Orange Business Services.

The Cloud Store Customer Space provides dashboards to monitor indicators allowing the Customer to view:

- The correct sizing of the subscribed bandwidth on the Orange BVPN side
- The distribution of the various flows and the processing of these carried out by the QoS Appliance

These elements are in no way binding on Orange Business Services but allow the Customer to ensure that his service is functioning correctly.

6.10.6 Limitation of liability

Orange Business Services is committed to the availability of the QoS Appliance, in the same way as the rest of the Flexible Computing Advanced infrastructure made available to the Customer. See the Quality of Service appendix for details.

Orange Business Services cannot be held responsible for poor quality of service if the bandwidth subscribed by the customer for his Orange BVPN access is undersized.

6.11 Use IT Cloud Portal

6.11.1 Overview

Use IT Cloud is a web portal developed by our technology partner Prologue, which allows you to manage the majority of public Cloud offers (multi-cloud functionality) in a single portal, with an interface that is simple, unified and powerful. It is also a PaaS (Platform as a Service) engine and orchestrator.

6.11.2 Proposed solution

Flexible Computing Advanced provides a virtual Appliance dedicated to each Customer, containing the latest version of Use IT Cloud validated by our teams.

6.11.3 Prerequisites

To be a Customer of Flexible Computing Advanced.

6.11.4 Billing

Billing for the Service is based on two indicators:

- The pro rata of the number of days of the month during which the Use IT Cloud Appliance has been active.
- The number of virtual machines (VM) created on Cloud offers other than Flexible Computing Advanced and Flexible Engine.

Invoicing is established monthly, on the basis of the Price List in force.

VMs created on Orange offers (Flexible Computing Advanced and Flexible Engine) are not billed.

6.11.5 Deployment

La mise en place de l'Appliance Use IT Cloud est faite à partir de l'Espace Client du Cloud Store. Elle est hébergée dans un espace sécurisé de la plateforme Flexible Computing Advanced et maintenue en conditions opérationnelles par les équipes Opérations d'Orange Business Services.

6.11.6 Limit of liability

Orange Business Services s'engage sur la disponibilité de l'Appliance Use IT Cloud, au même titre que le reste de l'infrastructure Flexible Computing Advanced mise à disposition du Client. Voir l'annexe Qualité de service pour les détails.

7 Support

The following table describes the support provided with the Flexible Computing Advanced Service.

Orange Business Services offers no support commitments for Beta Features.

Support provided with the Flexible Computing Advanced Service	STANDARD	BRONZE	SILVER	GOLD
Customer Service				
FCA documentation in the Cloud Store document space	Included	Included	Included	Included
Account and billing questions	Business hours	Business hours	Business hours	Business hours
Technical Support				
24x7 Datacenter Supervision	Included	Included	Included	Included
Ticket from the Cloud Store Customer Space	Ticket received 24x7	Ticket received 24x7	Ticket received 24x7	Ticket received 24x7
Ticket by Telephone	yes	yes	yes	yes
Special access to experts (e-mail or telephone)	no	Yes, the first three months	yes	yes
Number of hours of consulting included in the plan	N/A	2 hours / month, the first 3 months	2 hours / month	4 hours / month

8 Support and Guidance

Orange Business Services offers support, and consulting for virtualization, systems, and networks. These services can be ordered using the Customer Space portal and are described in the table below:

Guidance service	vCloud Director on FCA guidance service: level 1	vCloud Director on FCA guide service: level 2	VCD API on FCA guidance service
Duration	2 hours of theory + 4 hours of assistance/coaching	2 hours of theory + 2 hours of assistance/coaching	2 hours of theory + 2 hours of assistance/coaching
Content	Explore the VCD interface Organization configuration VM deployment Network connections Catalogs Using vApps Deploying vApps User and Rights Management Basic Edge Gateway Configuration Connecting with CSSA administrator tools	New features of VCD 9.5+ Advanced Edge Gateway Configuration (NSX) Distributed FW (micro-segmentation) & vDC design VPNs Load Balancing Importing with OVFTool tools Individual connections with CSSA administrator tools	Introduction to API Using API in RESTful Learning by example Introduction to using an SDK Example of a project that uses API
Audience	New customers	Existing FCA/FCO customers	All customers
Type	webinar	webinar	webinar
Prerequisites	Understand the basics of virtualization and network, and ideally VMware	Understand VCD	Understand VCD

Trainings	Zerto on FCA	NSS on FCA
Duration	3 hours	3 hours
Content	Prerequisites Introduction to using the portal Implementing protection groups Switchover test Switchover	Introduction to using the portal Backup policies Protecting a VM Restoring a VM Granular restoration of files Installing the NetBackup agent

Trainings	Zerto on FCA	NSS on FCA
Audience	All customers	All customers
Type	webinar	webinar
Prerequisites	None	None

Support / Consulting Services	Description
Solution Development (POC)	Includes vCloud Director guidance service Weekly 1 hour follow-up phone call Technical expertise plan of 4 hours / month
Dedicated Solution Manager	Personalized assistance and advice from a virtualization expert. (2 days / month minimum)
Flexible Expertise	Assistance with becoming a virtualization expert Assistance with deploying your complex solution on Flexible Computing Advanced Assistance with performance optimization
Scheduled Maintenance	Expert made available during an operation usually carried out by the Customer alone
On-Call Expertise	Expert on call during an operation usually carried out by the Customer alone

9 Service limitations

9.1 VCD Access Security

The vCloud Director portal is accessed over the Internet. The standard (default) security level is password protection.

When the first administrator account is created by Orange Business Services, a password is created that meets the password security requirements set by Orange Business Services (e.g. 14 characters, etc.). However, the Customer can create new VCD accounts whenever they want.

We recommend that you set secure passwords:

- By following your security policy
- Or by referring to the password security guide published by ANSSI (French National Information Systems Security Agency, or Agence nationale de la sécurité des systèmes d'information): https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf

Password configuration and security are the responsibility of the Customer's administrators.

9.2 Increasing VCD Portal Access Security

The vCloud Director portal includes a feature for delegating authentication to an external identity provider, managed by the Customer. Orange recommends using this feature for security reasons.

Some "identity provider" software can also provide "strong authentication", which may be necessary in some cases to satisfy the Customer's general security policy requirements.

The Customer can control these settings in their Organization's configuration. The documentation on this topic is described in detail in the "Allowing your organization to use a SAMLv2 access provider" chapter of the user guide:

https://docs.vmware.com/en/VMware-Cloud-Director/9.7/com.vmware.vcloud.tenantportal.doc/GUID-1F1F3EFD-55C5-4BF7-8683-FD93184A402F.html

Some of our customers are already successfully using the following software:

- In-Webo
- Microsoft ADFS

9.3 VM Sizing

A VM's number of vCPUs must be a whole number (a VM may not have, for example, 1.5 vCPUs). In PAYG mode, vCPU frequency is aligned with physical CPU frequency, in line with VMware best practices, to provide the Customer with the best possible performance.

Note: Virtual machines created by the Customer **must** respect the limitations given in the "vDC Specifications by Service Class" section. VMware best practices recommend avoiding large VMs, because they can have trouble obtaining their resource quota compared to smaller VMs. Orange Business Services recommends creating several VMs rather than one large VM, when application architecture permits.

If the Customer does not respect these limitations, Orange Business Services cannot provide support under the conditions stipulated in the Contract.

When a Customer wishes to host a very large VM (> 8 vCPUs), they must provide a "high performance" vDC or a vDC built on a dedicated cluster.

9.4 VM Storage

VMs are created with the minimum amount of storage space needed to support the Operating System, called the "root drive" This minimum storage space cannot be modified or deleted and is linked to the Operating System installed on the VM. If the vDC does not have enough disk resources to provide this minimum space, no Virtual Machine can be created.

9.5 Limit of a virtual disk (vmdk)

The virtual disk of a VM must not exceed 2 TB. Beyond this limit, the VM will continue to operate normally, but the effectiveness of the high availability and load sharing mechanisms will be affected, or even seriously disturbed. The backup will also work normally. However, restorations will not work. This is why "oversized" VMs can only benefit from "Best Effort" type support.

9.6 Supported Operating Systems

The current version of the FCA Service is based on ESXi, version 6.5 U3 or later.

The following link will allow the Customer to check “Guest OS” compatibility.

https://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=16

9.7 VM Size and Backups

The backup system offered with Flexible Computing Advanced is meant for VMs under the authorized limit of 6 TB. These are the maximum allowed values. If a VM's storage exceeds this limit, the VM may not be backed up during the reserved backup time window (10 pm - 6 am).

Any VM that is backed up and whose size exceeds the limit will not be included in the service-level agreement calculations. The Customer may be asked to remove its protection, since backing up such a VM might have negative consequences for other VM backups.

9.8 Mandatory up to date "Vmware tools" software

The backup mechanisms (except backup agent) are based on the vmware layer and require that the VM embed an up to date version of the "vmware tools" software. Most of backup failures are due to outdated versions of vmware tools. It is therefore the Customer's responsibility to maintain the vmware tools software up to date.

In the event of repeated failure to back up a VM linked to an obsolete version of vmware tools, despite several reminders to the Customer by the platform's operating teams requesting this update, Orange Business Services shall disable the protection attached to the virtual machine, which will then appear in the list of unprotected VMs in the NSS console.

Orange Business Services cannot be held responsible for a loss of data if the VM is not properly backed up due to an obsolete version of the "vmware tools" software.

9.9 Network storage (NFS)

The minimum value of a NFS volume is 500 GB.

The maximum value of a NFS volume is 8 TB.

9.10 Hardware Features not supported in VMs

The virtual servers provided with Flexible Computing Advanced do not support the following hardware:

- Graphics card (GPU)
- Sound card

These pieces of hardware are often needed to use a virtual machine as a workstation (VDI), but this feature is not currently available from FCA.

9.11 Edge Gateway

When using an IPsec VPN or L2Sec VPN with an Edge Gateway, an SSL Plus VPN cannot be used with the same gateway (VMware limitation).

9.12 Encryption Computation (SSL Offload and IPsec)

Orange Business Services does not have physical equipment dedicated to encryption computation, which is used for the Advanced Encryption Standard New Instructions (AES-NI). Encryption computation is handled directly by NSX Edge virtual appliances, which has an impact on the overall performance of these gateways.

9.13 Security Rules on the Administration Network (SUO Tools)

By default, the VMs of the same Organization connected to the SUO Tools administration network are all in communication with one another, even if trusted zones have been set on the other network interfaces. It is the Customer's responsibility to set up the filtering rules for the administration network using the distributed Firewall, so that no data is accessible to an unauthorized User. It is the responsibility of the Customer to make this setting correctly.

9.14 Dual Room

The Dual Room Feature is only available on the Val de Reuil site.

9.15 Data localization

By default, all of a Customer's data is located on a single Datacenter. To obtain an outsourcing of its data to another Datacenter, it is up to the Customer to subscribe to one of the following services, depending on the desired RTO:

- Off-site backup policies
- VM replication service (Zerto)