SPECIFIC CONDITIONS – HOSTED PRIVATE CLOUD PREMIER

Latest version: 15 July 2020

DEFINITIONS

Terms beginning in upper case in these Specific Conditions are defined below, as well as in the Contract to which these Specific Conditions relate, and in the OVHcloud Glossary available on OVHcloud website. The definitions below supplement definitions in the Contract.

"Client Network": *Resources external to OVHcloud Infrastructure used by the Client in order to communicate with Resources provided by OVHcloud. These may be the Client's own resources, resources provided and/or hosted by third parties on the Client's behalf.*

"Hosted Private Cloud PREMIER": *All of the Virtual Datacenter hosted on OVHcloud Infrastructure. The Hosted Private Cloud PREMIER is managed by the Client through its Management Interface and the Virtualisation Interface. Host Servers and Storage Resources provided to the Client as part of the Hosted Private Cloud Premier Service are reserved for the Client.*

"Host Server": *Dedicated server deployed in a Client's Hosted Private Cloud Premier. This server provides additional capacity through its processor (CPU) and memory (RAM) in the Hosted Private Cloud Premier that can be managed using VMware® User Interface.*

"Infrastructure": *Structure established by OVHcloud to host the Client's Hosted Private Cloud Premier, including notably the network, bandwidth, physical resources and Virtualisation.*

"Management Interface": *The "Manager" space accessible to the Client after login with a Client ID and corresponding password.*

"OVHcloud Connect": *Connectivity to the OVHcloud internal dedicated network ("Backbone"), provided to a Client at one or more OVHcloud Points of Presence. OVHCloud Connect allows the Client to connect to its own Client Network (i.e. its own infrastructure and computer resources and/or third-party infrastructure and resources that it uses) to its OVHcloud Connect.*

"Pack": *Contains the minimum physical resources required to operate a "Virtual Datacenter" of Hosted Private Cloud Premier:*

- *A "Premier Private Cloud" Pack consists of a minimum of:*
  - *Two identical Host Servers (contributing CPU and RAM for Virtualisation) dedicated to compute, the Client must ensure that he has at all times two identical Host Servers (i.e. same technical specifications). In case the Virtual Datacenter includes different pair of Host Servers, the lowest pair in term of CPU and RAM will be considered in the "Pack" for the Virtual Datacenter. For the sake of clarity, should the datacenter contain 2 Host Servers Premier "48 RAM" and 2 Host Servers Premier "96 RAM", the "Pack" considered will be made of the 2 Host Servers Premier "48 RAM".*
  - *Two datastores resources. In case the Virtual Datacenter includes different pair of datastore resources, the lowest pair in term of capacity will be considered in the "Pack" for the Virtual Datacenter. For the sake of clarity, should the datacenter contain two datastore resources of 2TB and two datastore resources of 3TB, the "Pack" considered will be made of the two data resources of 2TB.*
  - *the VMware vSphere interface, known as vSphere Web Client, is the management interface as provided by VMware, to administer the resources provided to the*

Client. This interface will provide logical access to the platform usually made out of 1 vCenter, 1 virtual Datacenter and 1 Cluster, plus at least 2 datastores and the software-defined networking resources.

- *A "Premier Private Cloud" vSAN Pack consists of a minimum of:*
  - *Three identical Host Servers (contributing CPU, RAM, locally provisioned storage for Virtualisation) dedicated to compute, the Client must ensure that he has at all times three identical Host Servers (i.e. same technical specifications). In case the Virtual Datacenter includes different number of Host Servers, the lowest 3 hosts in term of CPU, RAM and vSAN storage will be considered the "Pack" for the Virtual Datacenter. For the sake of clarity, should the datacenter contain 3 Host Servers vSAN Premier "192" and 3 Host Servers vSAN Premier "384 RAM", the "Pack" considered will be made out of the 3 Host Servers vSAN Premier "192 RAM".*
  - *Two datastores resources. In case the Virtual Datacenter includes different pair of datastore resources, the lowest pair in term of capacity will be considered in the "Pack" for the Virtual Datacenter. For the sake of clarity, should the datacenter contain two datastore resources of 2TB and two datastores resources of 3TB, the "Pack" considered will be made of the two datastore resources of 2TB.*
  - *the VMware vSphere interface, known as vSphere Web Client, is the management interface as provided by VMware, to administer the resources provided to the Client. This interface will provide logical access to the platform usually made out of 1 vCenter, 1 virtual Datacenter and 1 Cluster, plus at least 2 datastores, plus the ability to configure the vSAN datastore and the software-defined networking resources.*

"Point of Presence": *Physical locations on the OVHcloud network of CDN Servers connected to the Internet, as presented in its commercial offering (CDN infrastructure, Geocache Accelerator, CDN WebStorage).*

"Range": *This is defined as the generation of Hosted Private Cloud added to the Client infrastructure.*

"Service": *Basic unit to calculate Service Level Agreement and service credits that are claimable by Client. The unit is established under the same vCenter and at the virtual Datacenter level and depending upon the Range added. This can be a mix of different Ranges as long as it is within the same virtual Datacenter and therefore the same vCenter.*

"Storage Resource": *Dedicated storage resource (typically a NAS-type resource presented as a datastore) provided and managed in a Client's Hosted Private Cloud Premier. This resource uses disk space in the Hosted Private Cloud Premier to provide additional capacity that can be managed using VMware® User Interface.*

"Virtualisation Interface": *Third-party software provided by OVHcloud that allows the Client to manage its Hosted Private Cloud Premier and associated services, and in particular to establish and manage its Virtual Machines.*

"Virtual Machine": *A non-physical workload that uses Virtual Datacenter resources and is installed on the Hosted Private Cloud Premier network. Each virtual workload is managed independently from others within the Client's Virtual Datacenter.*

"Virtualisation": *Technology that allows multiple operating systems, virtual workloads or applications to operate on the same physical server.*

“vRack”: *One or a set of Virtual Local Area Networks (“VLANs”), set up on OVHcloud's internal private network (“Backbone”), made up of resources (Servers, Storage Resources, etc.) provided to a Client by OVHcloud. Resources physically located in different, geographically remote OVHcloud Datacenters may be connected to vRack. Some OVHcloud resources are not suitable for vRack. Information regarding the suitability of OVHcloud resources for vRack is available online on OVHcloud website*.

ARTICLE 1: PURPOSE

These Specific Conditions set out the specific terms and conditions, including, but not limited to, terms of use and financial conditions, applicable to OVHcloud Hosted Private Cloud Premier services (hereinafter the "Service(s)"). They supplement the OVHcloud General Conditions of Service currently in effect. Where a discrepancy arises, these Specific Conditions shall take precedence over the OVHcloud General Conditions of Service.

ARTICLE 2: DESCRIPTION OF SERVICES

2.1 Overview

Under the Service, OVH (or hereafter “OVHcloud”) provides the Client with a Hosted Private Cloud Premier consisting of one or more Virtual Datacenters within a secure private network.

Physical resources provided under this Service are reserved exclusively for the Client.

The Hosted Private Cloud Premier Service is intended for professional users and allows the Client to use its own secure private network.

The Service may come with restrictions (e.g. number of Virtual Machines that can be used in a Hosted Private Cloud Premier, traffic, bandwidth, etc.). These are set out in the documentation/specification available on the OVHcloud website. The Client agrees to comply with these restrictions.

As part of the Service, the Client is the resource administrator for IP addresses. The Client is responsible for managing these appropriately to ensure that its Service operates properly. The Client should ensure that it has sufficient IP addresses to allocate or, where applicable, for the Hypervisor to allocate, an IP address for each of its Virtual Workloads. The Client is therefore solely responsible for the use of IP address resources allocated or leased as part of the Service.

Each Hosted Private Cloud Premier has its own secure private network.
The outgoing bandwidth from the Hosted Private Cloud Premier is limited to a maximum data speed.

The Client may view its Hosted Private Cloud Premier bandwidth usage history, as well as average speed via the Management Interface.

OVH provides the Client with a range of Pack configurations, descriptions for which are available online OVHcloud website.

The Host Server product line and Pack selection determine the functionalities that can be accessed on the Virtual Datacenter, as well as performance levels.

2.2 Functionalities

VIRTUALISATION INTERFACE

The Service is based on functionalities intrinsic to integrated Third-party Products from OVHcloud partner VMware®'s software package and which enable server ("vSphere® Hypervisors"), network ("NSX®") and storage ("vSAN®") visualisation, in accordance with applicable VMware®'s specific terms and conditions currently in effect. All Third-party Products from the VMware® software package (which constitutes a Visualisation Interface) are hosted on resources managed directly by OVHcloud and external to the Client's Hosted Private Cloud Premier.

Each Visualisation Interface has its own functionalities. The Client should ensure that it makes an informed choice of Visualisation Interface and acknowledges that vSphere® Hypervisor selections cannot be subsequently changed. The Client acknowledges that full compatibility of functionalities and interoperability between Virtualisation Interfaces cannot be guaranteed.

VIRTUAL MACHINE Encryption (VM Encryption)

VM Encryption uses an internal functionality in vSphere 6.5 or later, which can be used to encrypt VM data on the fly using an encryption key provided by a component external to the Hosted Private Cloud Premier (box encryption), with the aim of encrypting data stored in the Hosted Private Cloud Premier datastore.

The Client is responsible for managing its own encryption key; OVHcloud accepts no responsibility in this regard.

FEDERATION

This functionality allows users to connect their own LDAP (Lightweight Directory Access Protocol) server to their Hosted Private Cloud Premier in order to handle authentication and identification on its existing accounts. The Client alone is responsible for ensuring that its LDAP server has proper connectivity.

2FA (DUAL FACTOR AUTHENTICATION)

2FA functionality provides double authentication method when logging into its management interfaces. As well as a username and password, the Client requires a temporary access token to log in. The Client is responsible for generating access tokens.

VRACK

vRack allows the Client to connect some or all resources (Host Servers and Storage Resources) provided by OVHcloud, including resources located in multiple environments and/or geographically remote OVHcloud Datacenters. It is used to allow Virtual Workloads to run on dedicated vLANs and allow those vLANs to be propagated to other Virtual Machines on other Hosted Private Cloud Premier located in other OVHcloud Datacenters, or with other OVHcloud services.

The Client's vRack is isolated from other OVHcloud Backbone components in a logical manner.

The Client alone is responsible for the administration of its vRack and Resources deployed thereon. The Client should determine the vRack's composition (connected Resources) and logical configuration (logical network and sub-network architecture). The Client shall administer its vRack directly via the Management Interface. The Client may securely connect its own infrastructure and external resources to vRack through OVHcloud Connect Service for example.

2.3 Additional Services

As part of the Hosted Private Cloud Premier Service, the Client may subscribe to the following additional Services, which are subject to their own respective Specific Conditions.

- Veeam Managed Back-up
- Disaster Recovery Plan
- OVHcloud Connect

ARTICLE 3: SERVICE TERMS AND CONDITIONS OF USE

3.1 Eligibility

Subscriptions to the Hosted Private Cloud Premier Service are available to professionals only, who shall not be covered by applicable Consumer law. By way of derogation from the provisions in the General Conditions of Service, the arrangements for cancellation do not apply to the Service.

3.2 Subscription

In addition to the chosen Pack, the Client may also add extra resources and Services to the Pack, which may consist of an additional Host Server, Storage Resource, or options detailed in the annex hereto or on the OVHcloud website.

For each Virtual Datacenter, the Client may subscribe to additional resources (increases in Host Server or Storage resources) to meet occasional or long-term requirements. The Client may opt to be charged for the current month or solely for the hours in which these resources are used.

3.3. Applicable conditions

Hosted Private Cloud Premier Services are subject to the Conditions of Service in effect, including these Specific Conditions, OVHcloud's General Conditions of Services, and any applicable Third-party Product Conditions currently in effect. Hosted Private Cloud Premier Services must be used in accordance with the latest version of the aforementioned Conditions of Service.

3.4. Responsibility of the Client

The Client is solely responsible for the use of Services, including the administration of keys used to manage credentials and access to the Service, the use of APIs, software and tools provided by OVHcloud, the administration of subscriptions and of Data that it uses in connection with the Services.

The Client must possess the necessary technical knowledge and competence and become familiar with the characteristics of Services before use.

OVHcloud's role is limited to Infrastructure maintenance operations and responsibility for energy supply and network connection to the Client's Hosted Private Cloud Premier.

The Client confirms that it has the range of technical knowledge required to properly administer a Virtualisation service such as the OVHcloud Hosted Private Cloud Premier.

The Client shall be the sole administrator of Virtual Datacentres, Host Servers and Storage Spaces in its possession.

The Client undertakes to make responsible use of the Service, in particular allocated network resources and is responsible for ensuring that it has sufficient resources to ensure that its Virtual Machines function correctly.

3.5 Maintenance

To deliver the Services, OVHcloud carries out maintenance operations. The Client will be notified of any planned maintenance operations on at least one of the methods detailed below, by email at the address given by the Client by its NIC admin/tech, publishing on the OVHcloud travaux website, contacting the Client directly by phone or by any means. These communications will clearly state the type of maintenance to be performed.

3.5.1 Types of Maintenance

There are three (3) types of maintenance operations that can be performed by OVHcloud.

a) Emergency changes for critical occurrences. This type of maintenance is defined by high severity and critical updates, patches and/or modifications to the infrastructure, hardware, firmware, software or any other component. The consequence of not applying this could be (including but not limited to):

a. loss of compliance for security certifications
b. put security and stability of the system at risk
c. expose critical vulnerabilities
d. loss of service to a wider customer base.

Once OVHcloud has been made aware of the issue with a clear understanding of the impact, information is shared with the Client that we are working on a fix, within 24h we will inform the Client what is the process that will be followed, when and how this will be applied to the environment, actions to be taken, and the level of impact for the Client, ranging from a minor impact on a given component all the way up to a major impact bringing down any or all of the components.

Given the impossibility to predict how many critical vulnerabilities will be unveiled at any given point in time during any calendar month, there is not limit on the number of emergency change tasks to be performed. Due to the criticality of the tasks to be performed, these can be undertaken at any point in time during the calendar month. For such cases that we rely on the vendor to provide a patch or fix, then OVHcloud will need to extend this period of time to provide the complete fix to include the lead time needed by the manufacturer.

b) Standard. These maintenance tasks are not critical and urgent in nature. These are of medium criticality and can apply to the Client only or the wider of the company, but it does not pose a security compromise nor loss of compliance. These will be communicated to the Client at least seventy-two (72) hours in advance. These tasks may or may not trigger any downtime but Client is advised to plan ahead to avoid any possible downtime. These planned tasks will take place outside of the regular working hours (normally 9am-5pm). Change Management Board must sign off on these. These are limited to two (2) maintenance tasks per calendar month.

c) Normal. These tasks are of low or no material impact that will result in a loss of service for the Client. These may have a level of criticality that can be from low to high. Client is to be notified at least seventy-two (72) hours in advance. These tasks will have undergone the proper change advisory board process to get approved. There is not limit on the number of tasks to be performed.

As part of the Lifecycle Management, OVHcloud updates the Infrastructure with planned maintenances. During that process, the Hosts Servers will be updated. If the Private Cloud environment is sized (with enough spare compute and Storage Resources) to allow the automation to reboot safely the Hosts Server, OVHcloud reboots the Hosts Servers to be up to date without any downtime. If the environment is not sized to allow the automation to reboot safely, the responsibility is on the Client to reboot the Hosts Servers within one (1) month after the installation of the new build. If the reboot has not been performed, the automation will proceed to reboot automatically at the end of the 30 days. That reboot will not be able to enter the Hosts Servers in maintenance mode and the reboot will create downtime.

OVHcloud shall provide updates to vCenter, NSX options and vROPS. Updates carried out are those released by VMware, in accordance with the Third-Party’s conditions currently in effect. Updates to vCenter may result in automatic updates to the ESXi Hypervisor.

With regards to ESXi installations on dedicated Client resources (Host Server), OVHcloud will notify the Client as stated above. The Client shall be fully responsible for, and directly administer, minor updates (patches) to ESXi. As such, OVHcloud encourages the Client to regularly check for available updates with the VMware publisher. For this purpose, the Client may use VMware's VUM (Virtual Update Manager). OVHcloud accepts no responsibility for any Service malfunctions resulting from updates to the Hypervisor installed by the Client. Likewise, the Client assumes full responsibility for non-application of updates or upgrades to the Hypervisor.

Where the Client refuses an upgrade provided by OVHcloud, it shall not receive Virtualisation Interface improvements or new functionalities. OVHcloud reserves the right not to maintain or make improvements to older versions of the Hypervisor. The Client may be required to move to a later version of the Virtualisation Interface to ensure effective Service operation. Older versions of Hypervisor are understood as two major versions behind the most current as provided by OVHcloud.
Furthermore, where failure on the part of the Client to apply an update poses a security risk (to the Client, OVHcloud and/or third parties), OVHcloud reserves the right to restrict or suspend service to the Client. In such cases, OVHcloud shall notify the Client immediately.
The Client alone is responsible for maintenance of and updates to systems and applications that it installs on Virtual Machines, which are outside OVHcloud's scope of operations.

The Client acknowledges that Hosted Private Cloud Premier Services are developed solely at the discretion of OVHcloud, its partners and third-party publishers who provide solutions used as part of the Service on their own schedule. The Client may be required to move to a later version of Hosted Private Cloud Premier Services to ensure effective Service operation.

3.6 Limits and restrictions

The Client acknowledges that, for security reasons, some functionalities and protocols (such as IRC or peer-to-peer file sharing) may be subject to restrictions under the Service. The use of proxies, and anonymisation services are strongly discouraged under the Service. Applicable restrictions are set out in the documentation available on the OVHcloud website.
The Client is responsible for using the Service in accordance with the user licences of integrated solutions. OVHcloud reserves the right to perform checks to ensure compliance with these conditions of use by the Client, and to suspend the Service under the conditions set out in the Contract, where the Client does not comply with the terms and conditions of use of Services, applicable law and regulations, and/or third-party rights.
A minimum number of Host Servers may be required to activate some functionalities, as per Pack definition.

3.7 Business continuity

Clients are reminded that, unless stipulated otherwise, the Hosted Private Cloud Premier service does not include a Business Continuity Plan (“BCP”) or Disaster Recovery Plan (“DRP”). As such, the Client is responsible for implementing its own BCP and/or DRP; it may order Hosted Private Cloud Premier Services in different datacenters, which will provide resources in different risk environments. The Client must then take the necessary technical and organisational measures to ensure continuity in its business activity in the event of a major malfunction that might impact the availability, integrity or privacy of its Service. The Client may use the DRP option, the Specific Conditions for which are attached to this document.

3.8 Back-ups

OVHcloud makes no commitment to back up Client data hosted on the Hosted Private Cloud Premier. It is therefore the Client's responsibility to take all necessary measures to back up its data in the event of loss, damage to shared data, for any reason, including data not expressly mentioned in these Conditions. The Client may use the Back-up option, the Specific Conditions for which are attached to this document.

ARTICLE 4: MITIGATION (PROTECTIONS AGAINST DoS (Denial of Service) AND DDoS (Dynamic Denial of Service) ATTACKS)

OVHcloud has implemented protective measures against DoS and DDoS cyberattacks (Denial-of-service attacks) where these are massive in scale. This functionality is used to help ensure continuity of service to the Client for the full duration of the attack.

This functionality involves verifying incoming traffic intended for the Client's Service from outside the OVHcloud network. Traffic considered illegitimate is then rejected before it can reach the Client's infrastructure, thereby allowing legitimate users access to applications provided by the Client despite the cyberattack.

These protection measures are not effective against cyberattacks such as SQL injections, Bruteforce or exploiting security vulnerabilities.
Due to the high complexity of the protection Service, OVHcloud is only subject to best-efforts obligation. It is possible that an attack is not detected by the systems in place, and that those systems cannot ensure continuity of Service operation.

Due to the nature and complexity of the attack, OVHcloud shall provide multiple levels of traffic protection in order to protect its infrastructure and the Service of the Client.

Mitigation is only activated once an attack has been detected by OVHcloud tools. Therefore, until mitigation is activated, the Service will sustain the attack directly, which may result in unavailability of service.

Once the attack is identified and mitigation is activated automatically, mitigation may not be deactivated until the attack has ended.

While mitigation is activated, OVHcloud cannot guarantee accessibility of Client applications, but will make every effort to minimise the impact of the attack on the Service and OVHcloud Infrastructure.

If, despite activating mitigation measures, the cyberattack affects the integrity of OVHcloud and OVHcloud Client infrastructures, OVHcloud shall apply more robust protective measures which may result in a reduction in quality or unavailability of the Service.

Lastly, it is possible that a portion of traffic generated by the cyberattack may not be detected by OVHcloud systems and thus adversely affect the Service to the Client. The effectiveness of mitigation measures also depends on the Service configuration. As such, the Client is responsible for ensuring that it has the necessary competence to provide effective administration.

It is important to note that mitigation does not exempt the Client from ensuring the security of its Service, installing security tools (e.g. firewalls), carrying out regular updates of its systems, backing up its data, or monitoring the security of its computer programmes (e.g. scripts, codes).

ARTICLE 5: MEASURES TO PREVENT SPAMMING USING THE OVHcloud NETWORK

OVHcloud has implemented a system of technical measures aimed at preventing fraudulent emails as well as spamming from its infrastructures.

For this purpose, OVHcloud shall verify outbound traffic from the Service used by the Client for port 25 (SMTP server). This operation shall involve monitoring traffic using automated systems.

Mail is not filtered or intercepted, but instead monitored with a time lag of a few seconds. These operations are carried out in parallel, but are not frontal, between the server and the web-based network.

Moreover, no operations are performed on outgoing emails: OVHcloud does not tag emails, nor does it modify emails sent by the Client in any way. OVHcloud does not store any information regarding these operations, aside from statistical data.

This operation is routine and entirely automated. There is no human input to monitoring traffic to port 25 (SMTP port).

Where multiple emails identified as spam or fraudulent are sent from the Client's server, OVHcloud shall notify the Client by email and block the SMTP port for the IP in question.

OVHcloud does not retain copies of emails sent from the Service's SMTP port where these are identified as spam.

The Client may request to unblock the SMTP port using its Management Interface.

All additional emails identified as spam shall result in a further blockage of the SMTP port for a longer period.

After the third blockage, OVHcloud reserves the right to refuse any further requests to unblock the SMTP port.

ARTICLE 6: SERVICE-LEVEL AGREEMENT

In order to benefit from the Service Level Agreement defined below, the Client must have:

i. a minimum of two identical Host Servers of same technical specification (i.e. identical components must be CPU & RAM), the minimum is three identical Host Servers for vSAN product range;

ii. enable the High Availability ("HA") option (and its components) on its Virtualization Interface.

Maintenance operations (defined in article 3.5.1) with explicit impacts are excluded from Service Level Agreement ("SLA").

SLA applies at a Service level based on the virtual Datacenter and Range added. For this if Client has one (1) virtual Datacenter with all the Hosts Servers from the same Range, then an individual SLA applies to that virtual Datacenter. If Client has different Ranges within the same vCenter and virtual Datacenter but with different Ranges, then the SLA is calculated based on the Range impacted. In case there is a shared component that will be used for one or more Ranges then this is to be treated as individual incidents, such will enable the Client to claim multiple service credits if and when a shared component (i.e. SSL Gateway, vCenter, or any other shared component) is impacted and suffers from unavailability.

When Client decides to migrate from a certain range to a different one, whether it is a new one, higher or lower) then the target Range determines which specific Terms and conditions and SLA level is applied from them on.

The SLA monthly availability rate is determined at 99.9% for the entire Service. If it falls below 99.9% then Client is entitled to 10% of the monthly Service. If it falls under 99% then Client is entitled to 30% of the monthly Service.

The commitment on delivery of a replacement host is 43 minutes.

Service credit is to be claimed by opening a request ticket. Client is to claim these service credits no longer than 30 days after the incident occurrence.

"Monthly availability rate" refers here to the total number of minutes in the month in question, minus the number of minutes of unavailability in the month in question, divided by the total number of minutes in the month in question. To calculate service credit, periods of unavailability are calculated from the beginning of the incident, until the fault is resolved and confirmation of resolution is communicated by OVHcloud.

"Unavailability" refers here to:

- For Host Servers (including vSAN): Access not possible to (one or more) Host Servers provided to the Client due to a fault with or downtime of Host Servers. Downtime and faults that do not prevent access to host servers shall not be considered unavailability, even in cases where a reduction in Infrastructure performance levels is observed. If a Host Server is rebooted by Client or due to scheduled and communicated maintenance, the availability of the Host Server will resume monitoring thirty (30) minutes after the reboot.
- For Storage Resources (excluding vSAN): Access not possible to Storage Resources (including additional NFS datastores), due to a fault with or downtime of the Storage Resources. Downtime and faults that do not prevent access to host servers shall not be considered unavailability.
- For network and connectivity: Access not possible to Host Servers and/or Storage Resources due to a fault with or downtime of network or connectivity equipment. Downtime of and/or faults with network or connectivity equipment that does not prevent access to Host Servers or Storage Resources shall not be considered unavailability, even where there is a noticeable reduction in performance levels.
- For Virtualisation Interfaces: Use not possible for some or all Virtualisation Interface functionalities due to a problem related to the application (excluding faults or bugs in VMware products and configuration issues or faults linked to poor maintenance or updates to the application, which remain the responsibility of the Client).

Service credits due to breaches of the SLAs are a fixed lump sum for all harm or loss resulting from the breach. As such, the Client waives all other claims and/or action.

Service credits shall not accrue where a single event results in a breach of multiple SLAs for the same Service. In such cases, the service credit most favourable to the Client shall apply.

The total cumulative monthly amount (all incidents and SLAs combined) of service credit payable by OVHcloud is capped at 30% of the monthly cost of the Service impacted.

Service credits are issued if and when customer has payed all its overdue invoices, and are deducted from the invoice for the month following receipt by OVHcloud of the Client's claim provided that all previous and overdue invoices have been paid by the Client.

Where the Client's action is required to establish a diagnostic or resolve an incident, and where the Client is unavailable or does not cooperate with OVHcloud, the corresponding length of time shall not be counted as a period of unavailability, action or restoration.

Service credit shall not be due where breaches of the SLA are the result of (i) events or factors beyond the control of OVHcloud, including, but not limited to, instances of force majeure, third-party actions, pandemia, faults or improper use of equipment or software under the Client's supervision, (ii) failure on the part of the Client to meet its obligations under this Contract (e.g. failure to cooperate in resolving an incident or validating a Token when requested by OVHcloud), (iii) improper or inappropriate use of the Service by the Client (e.g. poor network configuration, overloading Storage Resources, inappropriate use of systems, software or other elements used by the Client in connection with Services), (iv) planned maintenance, (v) suspension of service under the conditions in Article 3 of the OVHcloud General Conditions of Service, or (vi) hacking or software piracy. In such cases, and without prejudice to (iv), OVHcloud reserves the right to charge the Client, where applicable, for actions to restore availability. Such actions shall be included on an invoice, presented for approval by the Client.

Reasons for unavailability, in particular in cases of exclusion described above, may be established by any means, based on evidence taken from OVHcloud's information system (such as connection data) which, by express agreement, shall be admissible.

ARTICLE 7: DURATION, PAYMENT, RENEWAL AND END OF SERVICE

7.1 Duration

The Client agrees to use the Service for the full term of subscription selected when placing the order.

- During the commitment period, for resource under commitment the Client is:
  - Entitled to upgrade its Hosted Private Cloud Premier with a higher end Hosted Private Cloud Premier reference (Higher means a higher RAM and CPU resources per Host Server, in such case the Client will renew its subscription period for the same duration as the one initially selected. The Client will be responsible to manage the anniversary dates of all its Hosted Private Cloud Premier products. The upgrade flexibility is limited to one change per commitment period.
  - Not authorised to downgrade its Hosted Private Cloud Premier. Should the Client downgrade the Service committed to, the prices for the Service will revert to the public prices as shown on OVHcloud website.
- At the end of this initial period, the user subscription shall renew automatically for consecutive periods of equal length at the discounted price based on the commitment level chosen and with the same conditions than the initial contract. Unless the Client chooses to opt out automatic renewals using the Management Interface, in that case the price will be adjusted to the public price without any commitment

The applicable prices and payment methods are available on OVHcloud website.

During Ordering, the Client selects the initial duration of their Service subscription (“Initial Period”). The Initial Period begins on the day that the Service is activated. At the end of the Initial Period, the Service automatically renews in successive periods of the same duration (“Renewal Period(s)”), unless the Service is renewed with a modified duration or terminated in accordance with the conditions set out above or in the General Terms and Conditions of Service currently in force.

Commitment is not applicable to the following services: (i) Back-up Service (ii) Disaster Recovery Plan Service.

Furthermore, the Contract may be terminated in accordance with the OVHcloud General Conditions of Service.

The Client may carry out a change of configuration on the Service being billed. In this case, the Switch to a higher configuration is billed to the Client at the time of request according to the price applicable to the new configuration, which can be checked on OVHcloud website.

The delivery time is established by OVHcloud based on the available data in its information system, which is authentic and is fully binding on the Client.

7.2 Payment

During Ordering, as well as when the Service is renewed, a bill is issued and paid automatically using the payment method registered by the Client. The Client agrees to register, at any time, a valid payment method from the methods available.

The Client agrees to always have sufficient funds in their bank account and the payment method that they are using, so that their bills can be paid within the specified deadlines.

If OVHcloud is unable to collect money via the associated payment method, an email will be sent to the Client inviting them to pay the amount of their outstanding bill as soon as possible. Failure to pay the amount will result in OVHcloud suspending the Service by right.

7.3 Renewal

The Client may modify the duration of future Renewal Periods for their Services using their Management Interface, at least 24 hours before the end of the Initial Period or the current Renewal Period.

When the Initial Period does not begin on the first day of the calendar month (start-up during the month), the Service’s renewal cycle is realigned to a calendar cycle during the first renewal so that the following Renewal Periods begin on the 1st of the calendar month. (For example: for a Service initially subscribed to for one (1) year on 24 May 2017, the automatic renewal at the end of its Initial Period results in the Service being extended from 24 May 2018 up to 31 May 2019.)

If the Client does not wish for a Service to be renewed at the end of its Initial Period or current Renewal Period (“Renewal Date”), they must deactivate the automatic payment function in their Management Interface.

In order to be effective and result in the termination of the Service at the end of the Initial Period or current Renewal Period, the automatic payment function must be deactivated under the following conditions:

a. For Services with a monthly renewal cycle, before the 19th day of the calendar month at 11:00 PM (Paris time) at the latest,
b. For Services with a non-monthly renewal cycle (quarterly, six-monthly, annually, etc.) before the 19th day of the calendar month preceding its Renewal Date at 11:00 PM Paris time at the latest (For example: to terminate a Service subscribed to for one (1) year in June 2018, at the end of its Initial Period, the automatic payment must be deactivated before 19 May 2019, at 11:00 PM Paris time).

If the automatic payment is deactivated under the conditions set out above, the related Service is automatically terminated and deleted at the end of the Initial Period or current Renewal Period ("Expiry Date") including all of the content and data stored by the Client as part of the Service. It is the Client's responsibility to take all the necessary measures to ensure that their content and data is preserved before the Service is terminated.

However, the Client retains the ability to renew the Service up to 24 hours before its Expiry Date, either by reactivating the automatic payment function, or by paying for the next Renewal Period in advance.

The duration of certain options or functions that may be associated with the Service, along with their renewal and termination conditions, may differ to those applicable to the Service. It is the Client's responsibility to be aware of these.

7.4 End of Service

In the event of non-renewal or termination of the Hosted Private Cloud Premier Service, for any reason, all Virtual Workloads, data and information contained shall be automatically and irreversibly deleted (including back-ups and duplications).

Before its Hosted Private Cloud Premier Service expires, or before terminating or removing a Hosted Private Cloud Premier Service, the Client is responsible for making the back-ups and data transfers necessary for continued storage.

OVHcloud deletes and destroys disks at the end of the Service in accordance with established, documented procedures:

- Deletion of data on hard drive disk or array is carried out by overwriting data (overwrite sanitize, one pass).
- Deletion of data on SSD disk or array is carried out using the logical erase procedure (block erase one pass) or by removing the encryption key (PSID revert).
- Where the storage device is removed from its bay, data are in all cases deleted before removal from the bay. The device is destroyed in the event that an error occurs during the deletion process.
- Storage devices are destroyed using dedicated machines in a secure space in each datacenter.

ARTICLE 8: FINANCIAL CONDITIONS

8.1 Billing

OVHcloud may propose different types of pricing for the same product as disclose on the OVHcloud website. It is the Client responsibility to manage and ensure that the pricing offer chosen match with its needs. For the sake of clarity, the hourly offer might be more expensive than the monthly subscription offer, Clients will be invoiced according to the offer subscribed and usage.

Before the end of the current month, OVHcloud may ask the Client to pay the amount of its Infrastructure, consumption and/or options subscribed during the current month, as soon as their total amount exceeds the outstanding amount authorized by OVHcloud for the Client. OVHcloud also reserves the right to ask the Client to pay a security deposit covering the consumptions of the Client.

For the sake of clarity, if a Client subscribes to Private Cloud Premier on the day 15 of any given month, then the Client is invoiced and charged for a prepayment of 30 days. At the beginning of the next calendar month, after subscription of services, and if the Client still maintains the same product and exactly the same options, then OVHcloud issues an invoice for the remaining of the current month. This invoice is then sent to the Client to be paid in full. After this regularization takes places then all the invoices for the same product, with the same options, is invoiced at the beginning of the subsequent calendar months and for as long as the Client subscribes the Service. If at any given point in time the Client adds any additional resource (Host Server, Storage Resource) during a calendar month, the same process will apply to synchronize and maintain all invoicing at the beginning of calendar months.

8.2 Additional resources

The Client can, upon request, temporarily increase the Storage Resource and/or add Host Servers to its Virtual Datacentre. These additional Infrastructures are invoiced to the Client according to the prices applicable available on the OVHcloud website at the time of subscription and paid immediately by direct debit.

8.3 Pay as you go

Additional Infrastructure (Host Server, Storage Resource, etc.) or additional options may also be invoiced by the hour. In that case OVHcloud will invoice, at the end of the current month, the totality of the services subscribed by the Client for the current month and subject to an hourly invoicing. Any hour started is due. Invoice will be issued at the end of the month and paid immediately by direct debit.

8.4 Payment term and payment default

All services are invoiced on a monthly basis, month in advance and paid immediately by direct debit. Any payment default on due time, including partial payment, will generate a service interruption. If payment reminder served by email remains unresolved four (4) days after notification. Consequences of unsettled payment default are:

1) the Client will not be able to add services
2) seven (7) days after service interruption OVHcloud is entitle to (i) definitely interrupt the service and (ii) delete all the data stored on the Infrastructure

ARTICLE 9: LIFECYCLE POLICY

OVHcloud will announce within six (6) months after the launch of a new generation of any Hosted Private Cloud the specific dates, for the new and previous generations of the Service, for the following terms:

- End of Sales. This refers to when sales for the previous generation will be discontinued. After End of Sales for a specific Hosted Private Cloud generation, the Clients will still be able to grow and add additional individual Hosts Servers. Packs will not be available from that previous generation or any other generation before it. Packs will be sold for the new Hosted Private Cloud generation launched on the market.
- End of Support. This refers to when the previous generation of Hosted Private Cloud will cease to have support from OVHcloud, including but not limited to, no automatic spares only on a commercially reasonable effort basis due to limited stock, delivery of such Hosts will not be guaranteed within a specific timeframe and SLA will also be limited to 99%.
- End of Life. This refers to when the generation being sunset will be discontinued, no additional sales for individual hosts will be allowed, no more SLA or Support Services will be provided for the Hosted Private Cloud generation that has reached this stage. Clients can still remain on this hardware generation temporarily until the definitive cessation of the range, with a maximum grace period of 3 months after this date. OVHcloud reserves the right to not grant a grace period. It is strongly recommended to move to the newest generation available.

Other terms that pertain to the lifecycle of Hosted Private Cloud are as follows:

- Beta. This refers to a stage where product may or may not go into to allow Clients to test before it is generally available. There is no SLA nor official support during this stage. Use of the product during beta stage should never be for production use.
- General Availability. This is the date when the product becomes available for the whole of the market. This is the date where the product is launched. At this point the previous generation of the product goes into End of Sales automatically for packs.

- End of Marketing. This is used at OVHcloud's sole discretion. Marketing efforts are being put in place during the life of a product. OVHcloud may decide to enter this stage at any given point in time without further notice to Clients.
- Support for middleware. Third-Party software support will be offered by OVHcloud for those within the last two (2) major versions. OVHcloud encourages its Clients to upgrade to the newest version available at OVHcloud. Support for Third-Party software will be offered as long as the vendor of such software still provides the product in general availability, maintains public support for it and within the same conditions. OVHcloud reserves the right to discontinue offering any Third-party at any given point in time. OVHcloud will inform Clients of such change at least 3 months in advance.

ANNEX 1
DIVISION OF TASKS AND RESPONSIBILITIES BETWEEN THE CLIENT AND OVHcloud

	OVHcloud	CLIENT
Maintenance		
Private Cloud Infrastructure Hardware	X	
Virtualisation Interface	X	X
Software installed by the Client		X
Software provided by OVHcloud	X	
Back-up		
Virtual Machine and Client Content		X
Configurations provided by OVHcloud	X	
Maintenance VEEAM Back-up	X	
VEEAM Back-up use (including ensuring proper back-up performance and integrity)		X
Service Operation		
Administration		X
Infrastructure Availability	X	
Reversibility		
Data retrieval		X
Deletion of data on termination	X	
Security		
Hosted Private Cloud Infrastructure	X	
Virtual architecture hosted in the Hosted Private Cloud		X
Safeguarding VM content		X
PCI DSS-SPECIFIC		
To be included in PCI DSS		

ANNEX 2
VEEAM MANAGED BACKUP

This document describes and sets out the specific terms and conditions applicable to the Veeam Managed Backup Service offered by OVHcloud as part of its Hosted Private Cloud Service (hereinafter referred to as the "Backup Option" or " Veeam Managed Backup "). It complements and forms an integral part of the Hosted Private Cloud Premier Specific Conditions. In the event of any inconsistencies, this appendix shall prevail.

Description: The Backup Option allows the Client to back up the Virtual Machines on their Hosted Private Cloud Premier, as well as the data stored on them (hereinafter referred to as "Backup"). This backup feature is integrated into the Management and Virtualization Interfaces. The Backup Option is an optional Service that is not included by default in the cost of the Hosted Private Cloud Premier Service. This Option must be the subject of a specific order or activation, and results in additional invoicing.

Software: The software that allows the Client to use the Backup Option is developed by third-party suppliers ("Third-Party Products"). OVHcloud does not participate in the creation and development of these Third-Party Products made available to the Client as part of the Option. Consequently, OVHcloud is not responsible for Third-Party Products made available as part of the Service, which may include technical errors, security vulnerabilities, incompatibilities or instability, and does not give any guarantee on Third-Party Products made available as part of the Service. The Client is only allowed to use the Third-Party Products made available by OVHcloud within the scope of the Service in accordance with any applicable Third Party's terms and conditions currently in effect. This excludes in particular any possibility of decompiling, accessing sources, reinstalling on other infrastructures and sub-licensing the Third-Party Product programs or systems made available to them. OVHcloud and the third-party supplier reserve the right to modify the Third-Party Products at any time.

Backup Option Mechanisms: Backups are performed using the "Veeam Managed Backup" Third-Party Product. From the OVHcloud Manager. Client will activate the Veeam Managed Backup option in their management interface and will chose between 3 level of offers: "Standard, Advanced or Premium". Once one of these offers is selected and activated on the Client's Hosted Private Cloud, this is the only offer that will be available for the backup of all its virtual machines. Number of incremental backup, full backups and additional features available depend on the level of service selected in the Management interface. Backups are not replicated by default, and only available on the higher offers. On each update, a consistency check between the backed up Virtual Machine and its Backup is performed automatically via a control application. This check concerns only the consistency of the Backup file against the source file and does not check the integrity of the Backup or the data contained on it. In the event of an inconsistency or error detected, a new Backup is automatically performed by the system. In the event of a new inconsistency or error detected, this is mentioned in the daily Backup report communicated to the Client. This consistency check is an obligation of means (commercially reasonable efforts), and OVHcloud shall not assume any responsibility or liability in the event of the failure of this check, or corruption of the backed-up or duplicated data. The Backup Options are conceived for Virtual Machines to be backed up that do not exceed two (2) terabytes.

Storage space: The storage resources allocated to the Backup Option are shared. The Storage Resources allocated to the Client are logically isolated from those allocated to other OVHcloud Clients, and are physically separated from the Infrastructure in which the Client has set up their Hosted Private Cloud Premier. The Storage space used for the Backup Option is located in the same datacenter as the

Hosted Private Cloud Premier Service that is being backed up. It is the Client’s responsibility to ensure that the location of the datacenter meets their needs and requirements.

Terms of use: The Client is solely responsible for the use of the Backup Option, and in particular (a) for selecting the Virtual Machines on their Hosted Private Cloud to be backed up, (b) for checking that the Backups are properly performed, (c) for checking the integrity of the backups using the tools that the Client considers appropriate, and, (d) in the event of failure, for implementing a new Backup operation if necessary by contacting OVHcloud Support. OVHcloud does not manage Backup or Restore operations performed as part of the Services. OVHcloud cannot be held responsible in the event of failure, malfunction or error in the Backup operations. The Client agrees to flag as soon as possible the discovery of a malfunction, error or vulnerability in the Backup operation. The Client is solely responsible for the content of the Backups. The Client ensures that they hold the necessary rights and are in compliance with the regulations in force. OVHcloud has no knowledge of the content and activities for which the Client uses the Backup and Restore solution. The Backup option may be suspended and interrupted in accordance with the terms of the General and Specific Conditions applicable to the Hosted Private Cloud Premier Service. OVHcloud is subject to an obligation of means.

Billing: The Client is invoiced according to (i) the number of Virtual Machines backed up, (ii) the size of the Virtual Machines backed up and (iii) the Backup service chosen.

End of Services: In the event of deletion, reinstallation or configuration change of a Virtual Machine or Backup, as well as in the event of termination or non-renewal of a Hosted Private Cloud Premier Service or the Backup option, all Backups (including the data and information they contain) are automatically and irreversibly deleted. Before starting these tasks, as well as before the expiry date of their Backup Option or Hosted Private Cloud Premier Services, it is the Client’s responsibility to back up or transfer their Virtual Machines (including all the data and information they contain) to other devices, in order to protect against any loss or alteration.

Service Level Agreement. SLA is defined as the availability of the Veeam Managed Backup Service provided by OVHcloud to allow Clients to perform daily backup tasks and make those tasks available to Clients. To do this we will collect a combination of metrics, but not limited to, such as these:

- Veeam service uptime
- Uptime of infrastructure where Veeam Services are installed
- Network uptime
- Storage uptime

In addition, we will watch for errors on API calls, in case there are any, for longer than 120ms. SLA does not apply on the backup content nor the time it takes for the backup job to run.

SLA	Uptime	GTI*	GTR**
Standard	99.9%	12h	72h
Advanced	99.9%	8h	48h
Premium	99.9%	4h	24h

* : Backup jobs are excluded
** : Start from the Backup Report for backup Backup jobs

GTI, Goal Time for Intervention. Maximum time OVHcloud will take to intervene on an incident. Starts when a task is launched by Client, results in an error, and it ends when OVHcloud contacts Client with a Support Ticket ID, or when OVHcloud Support personnel replies for the first time on an incident ticket opened by Client.

GTR, Goal Time for Recovery. Maximum time OVHcloud will take to recover from the incident reported automatically by the system or by the Client, by creating an incident ticket. It starts when a task launched by Client results in error and it ends when the incident is resolved with a state of “done” or “cancel” (with Client agreement).

Conditions

These are the conditions for SLA to be applied:

- Client has the Veeam Backup Server VM hosted and in working order in the Hosted Private Cloud infrastructure at OVHcloud
- Having this VM protected with High Availability at all times
- The VM follows Veeam Backup Best Practices.
- VMs over 2TBs in size are not subject to this SLA agreement.
- Should Client try to back up a VM over the allowed size or if the backup job is cancelled by Client, SLA will not apply.
- OVHcloud reserves the right to request Client to relaunch a backup job that previously failed, if Client is not able to comply and/or if Client is not available to perform this request, SLA should not apply.

ANNEX 3
"Disaster Recovery Plan Option"

This appendix describes and sets out the specific conditions applicable to the "Disaster Recovery Plan" option offered as part of OVHcloud's Private Cloud Services (hereinafter referred to as "DRP"). This option represents one of the possible components of a "Disaster Recovery Plan," which is a global business project built, tested and operated by the Client. This appendix supplements and forms an integral part of the Hosted Private Cloud Premier Specific Conditions. In the event of any inconsistencies, this appendix shall prevail.

Description: The "Disaster Recovery Plan" Option allows the Client to switch their Virtual Machines, whether they are hosted on-premises or in a Hosted Private Cloud Premier, as well as the data stored on them, to a different Hosted Private Cloud Premier infrastructure. This switch feature is available on a dedicated interface. This option is an optional Service that is not included by default in the cost of the Hosted Private Cloud Premier Service. This option must be the subject of a specific order or activation, and results in additional invoicing.

Software: The software that allows the Client to use this option is developed by third-party suppliers ("Third-Party Products"). OVHcloud does not participate in the creation and development of these Third-Party Products made available to the Client as part of the Option. Consequently, OVHcloud is not responsible for Third-Party Products made available as part of the Service, which may include technical errors, security vulnerabilities, incompatibilities or instability, and does not give any warranty on Third-Party Products made available as part of the Service. The Client is only allowed to use the Third-Party Products made available by OVHcloud within the scope of the Service in accordance with any applicable Third Party’s terms and conditions currently in effect. This excludes in particular any possibility of decompiling, accessing sources, reinstalling on other infrastructures and sub-licensing the Third-Party Product programs or systems made available to them. OVHcloud and the third-party supplier reserve the right to modify the Third-Party Products at any time. As part of this option, OVHcloud provides the Client with the licenses to use the "Zerto" Third-Party Product required for usage of the service.

Option mechanisms: The syncing and/or copying of the VMs is carried out by means of the "Zerto" Third-Party Product. Using the Third-Party product’s dedicated interface, the Client selects the Virtual Machines on their Hosted Private Cloud Premier Service to sync on their Hosted Private Cloud Premier backup infrastructure. The backup Hosted Private Cloud Premier must be located in a different datacenter to the main Hosted Private Cloud Premier. For each Virtual Machine selected, a continuous high-bandwidth sync is carried out. Data replication is asynchronous, in addition to being continuous, with an RPO (Recovery Point Objective) present and available to view in the Third-Party Product’s dedicated interface. Client data is synced via the OVHcloud fibre-optic network between OVHcloud datacenters where the Hosted Private Cloud Premier solution is present. Data is transferred via a VPN between remote sites, so that all data transfer is secure. In the event of an emergency, the Client can immediately switch to the Hosted Private Cloud Premier backup site (the DRP site) by clicking on "FailOver" in the Third-Party Product interface to boot their backup infrastructure.
Management of the "FailOver" and the switch to the backup site is the responsibility of the Client.
The "VMware DRS" option available on the VMware vSphere management interface must be enabled in order for this option to be used.

Terms of use: The Client is solely responsible for the use of the "Disaster Recovery Plan as-a-Service" Option, and in particular (a) for selecting the Virtual Machines in their Hosted Private Cloud Premier to be synced, (b) for configuring their VPGs (“Virtual Protection Groups”, a design in the Third-Party

Product) and verifying that they work properly, (c) for checking that the Syncing is carried out properly, (d) for verifying the integrity of the syncing using the tools that the Client considers appropriate, and, in the event of failure, implementing a new Syncing operation if necessary by contacting OVHcloud Support. OVHcloud does not manage Syncing or failover operations between the Client's 2 infrastructures as part of the Services. OVHcloud cannot be held responsible in the event of failure, malfunction or error in the performance of Syncing or failover operations. The Client agrees to flag as soon as possible the discovery of a malfunction, error or vulnerability in the performance of the syncing operation. The Client ensures that they hold the necessary rights, and are in compliance with the regulations in force. OVHcloud has no knowledge of the content and activities for which the Client uses the Disaster Recovery Plan solution. This option may be suspended and interrupted in accordance with the terms of the General and Specific Conditions applicable to the Hosted Private Cloud Premier Service. OVHcloud is subject to an obligation of means.

Billing: The Client is billed according to the number of Virtual Machines protected by the "Disaster Recovery Plan " Option.

End of Services: In the event of deletion, reinstallation or configuration change of a Virtual Machine, as well as in the event of termination or non-renewal of a Hosted Private Cloud Premier Service or this Option, all syncing (including the data and information it contains) is automatically and irreversibly deleted. Before performing such operations, as well as before the expiry date of the “Disaster Recovery Plan” Option or the Hosted Private Cloud Premier Services, it is the Client's responsibility to back up or transfer their Virtual Machines (including all data and information contained therein) to other devices, in order to avoid any data loss or alteration.