Service Description Virtual Data Center (VDC)

Version / Datum
1.0
16.04.2020

Authors
Product Management

Inhaltsverzeichnis

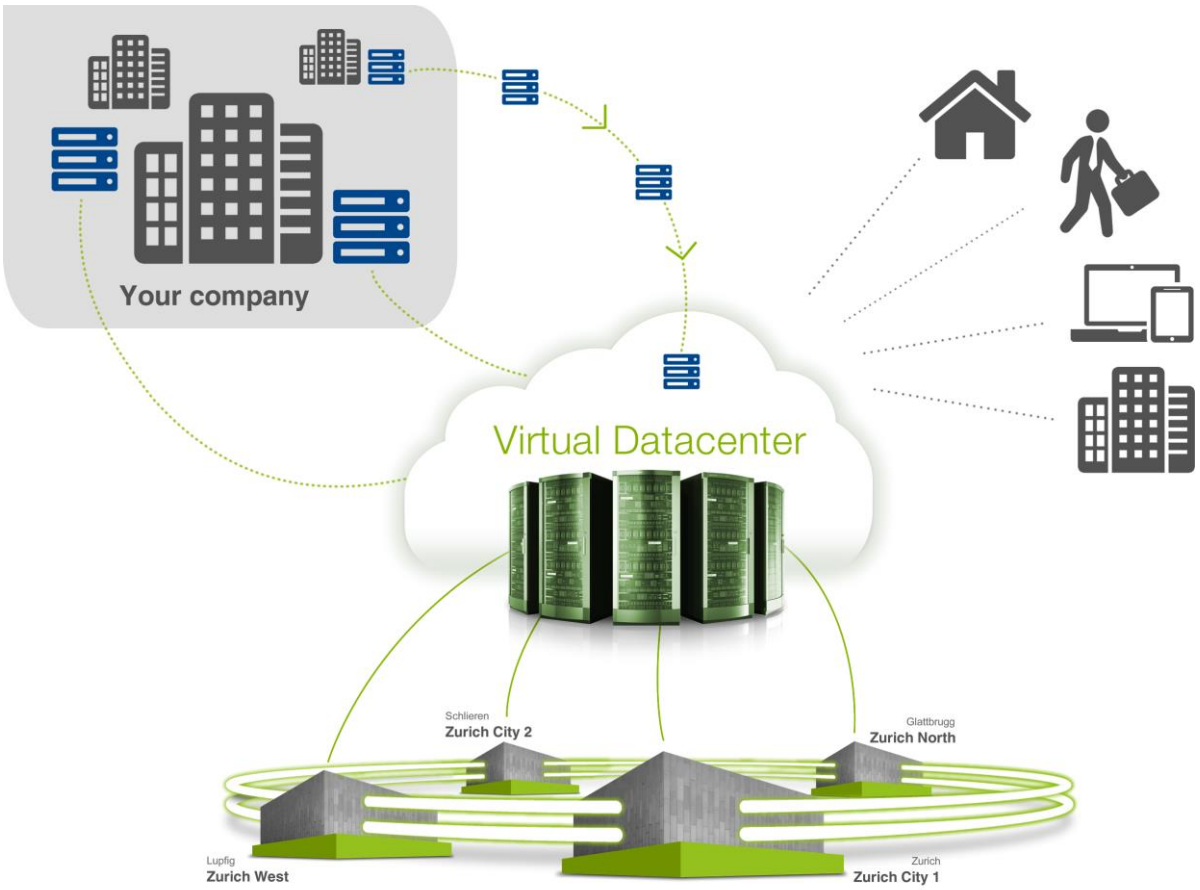
1. Service description

green.ch and Green Datacenter (hereafter Green) provide cloud products on many different architectures, divided among several redundant data centers, storage clusters and server systems. The physical infrastructure is operated in state-of-the-art data centers in Switzerland, chiefly in the Zürich-West area.

With the virtual data center, or "VDC" for short, Green offers its customers the facility to virtualise their company's IT infrastructure and replicate the corporate structure, complete with departments. Your administrator can dynamically allocate resources like servers, disk space and authorisations by a simple mouse clicks from everywhere.

Green's cloud products offer customers many options in the area of IaaS (Infrastructure as a Service).

Virtualisation means that every virtual server acts like your own server. The virtual servers are intelligently distributed over the high-performance, underlying hardware. Resources can be shared or reserved explicitly for individual virtual servers, giving you flexibility and mobility.



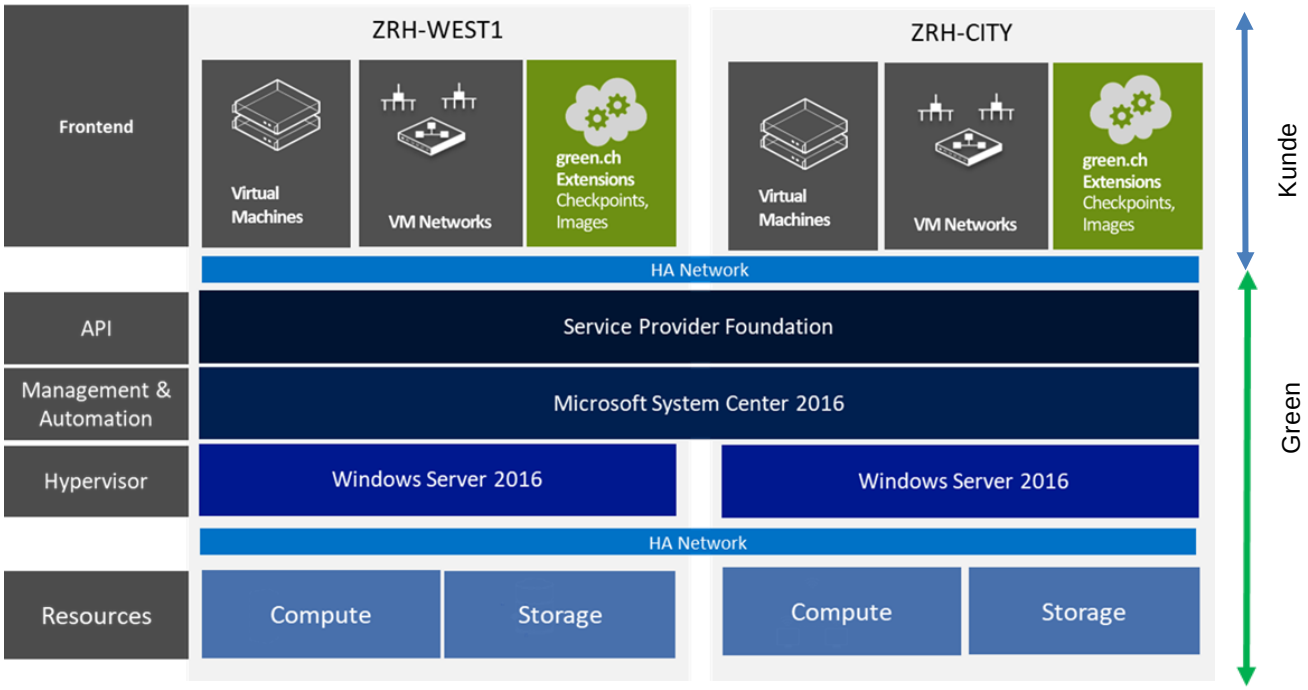
Green's virtual data center is highly scalable and based on Microsoft Hyper-V© virtualisation technology. This means the resources in your own data center can be flexibly combined with the VDC or your entire IT infrastructure can run in the virtual data center.

1.1 Components

The virtualisation is based on Hyper-V© by Microsoft Windows Server. The following components of the
Microsoft System Center are used for management and automation:

- Virtual Machine Manager
- Orchestrator
- Service Manager

The customer front end for administration and management of your company's servers and networks is based on the Windows Azure Pack.



With the basic subscription, you gain access to the VDC portal, where you manage your departments, the servers, the disk space and the networks.
You can re-size your virtual servers via this portal at any time, increase the disk space or register new users. Flexibility is paramount. At the click of a button, you determine your company's growth to keep pace with your need for hardware flexibility.

To connect your departments (subscriptions) with each other, Green provides a virtual WatchGuard firewall, which can be integrated and configured via the portal as either a managed or an unmanaged service. In addition, you can use this product as a VPN endpoint to ensure that your users or their location are securely connected.

1.2 Customer benefit

You decide when to migrate which application and move it into the virtual data center. Your infrastructure is operated in two secure data centers in Switzerland and is fully functional from day one. Worries about air-conditioning, power, capacities and resources will be a thing of the past and you will enjoy maximum flexibility.

Flexible.
Lots of different server and OS configurations are possible.

Simple.
24/7 online self-management from any location.

Cost-effective.
You only pay for what you actually use. Divided into server, disk and options.

Secure.
Your data are protected by a firewall and redundancy.

Monitored.
Complete control over the costs and consumption of your resources at all times.

Carefree.
Hosting in highly secure data centers with 24/7 monitoring.

Highly available.
You always have secure access to your business. Anywhere, anytime.

Personal.
99.9% availability thanks to redundant network and server infrastructure.

Fast.
Cutting-edge technologies (hyperconverged servers, SSD-tiered disks).

Complete.
Fully functional basic platform including connection to the Internet.

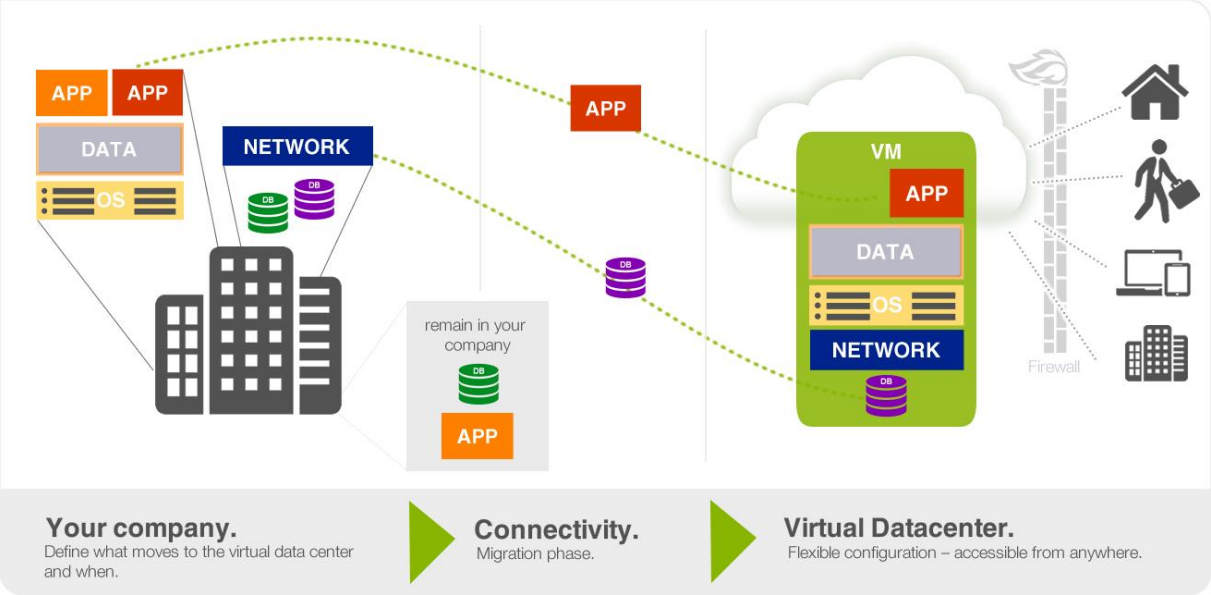
1.3 What we offer

The main "VDC" product is split into three key components:

1. Various possible server and operating system configurations and related options
2. Freedom to choose your disk space size for each server. Usage is simply added up at the end of the month.
3. The flexibility of your virtual company, with a maximum of 8 departments, and subscriptions protected by a virtual firewall

Green also allows hybrid versions with connections to your colocation rack.

This is how your company might look if you migrate to the VDC:



1.3.1 The base subscription

The VDC basic subscription can be cancelled on a month-by-month basis. Additional components are billed dynamically on a daily basis and totalled at the end of the month. Our Business SLA with 24/7 support is already included in the basic package. After ordering the VDC, you get your access details for the portal (login and password).

You have access to a public IP network with an address range of /28 IPv4 addresses. The first 3 addresses in the network are required for gateway and VRRP addresses and must be left blank. This leaves you with 11 usable addresses.
A configured admin zone is already set up as a vNetwork, so you can get on with choosing servers and disk space.

Personal advice is important for us. We will be happy to assist you with all aspects of migrating to our virtual data center (VDC). We also offer you more extensive support services. Four hours of consultancy is included in the basic package.

On the firewall, business units, departments or projects can easily be connected via the firewall using the available templates. It is up to you which model you would like to use. The options are self-configuration with your own virtual product or our managed or unmanaged firewall.

Needless to say, we are happy to provide you with a quote for Green to handle the entire project for you. Just ask!

1.4 Specifications

1.4.1 Server types Disk space

The virtual servers are divided into twenty-four different options. What distinguishes them are the performance parameters of the individual product features (vCPU, RAM and disk type). The values specified for each option are fixed and – aside from disk space - cannot be altered. Each main product is supplemented with optional extras.
The disk space can be configured as you wish for each server.
There are two statuses for individual servers:
Online: the server is functional.
Power off: the server is on standby, you pay only for disk space.

1.4.2 Virtual server configurations

	specifications		
Virtual Server	**RAM in GB**	**vCPU**	**SSD-tired Diskspace**
A001-C1	1	1	standard
A002-C1	2	1	standard
A004-C2	4	2	standard
A004-C4	4	4	standard
A008-C2	8	2	standard
A008-C4	8	4	standard
A016-C4	16	4	standard
D001-C1	1	1	SSD-tiered
D002-C1	2	1	SSD-tiered
D004-C2	4	2	SSD-tiered
D004-C4	4	4	SSD-tiered
D008-C2	8	2	SSD-tiered
D008-C8	8	8	SSD-tiered
D016-C4	16	4	SSD-tiered
D016-C12	16	12	SSD-tiered
D032-C8	32	8	SSD-tiered
D032-C16	32	16	SSD-tiered
D048-C8	48	8	SSD-tiered
D048-C12	48	12	SSD-tiered
D064-C12	64	12	SSD-tiered
D064-C24	64	24	SSD-tiered
D096-C12	96	16	SSD-tiered
D096-C16	96	16	SSD-tiered
D128-C16	128	16	SSD-tiered
including	– vNetwerk LAN, one internal vLAN – vNetwerk Public, 1x Public IP-Addressrange /28 – Free choice of operating system (Windows,CentOS, Debian, Ubuntu) – Business SLA 24/7 h		
Exklusive	– Firewall selection of self- managed, Green-managed or the virtual firewall of your choice – Business vNetwork Connect (Connection to your rack in the colocation or to one of the 40 Carriers we can provide)		

1.4.3 Operating system

You have a choice of various operating systems for the virtual server.

Operating systems (The latest version is available on the website www.green.ch)	– Microsoft Windows (license included)	– Various Linux derivatives – Own virtual OS

1.5 Terms of offer and use

1.5.1 CPU/processor

The number of vCPUs defined in the product are allocated to the appropriate virtual server as vCPUs. The higher the number of vCPUs allocated to it, the better the performance of a virtual server. If the server is in Power-off mode, only the disk space is charged on a daily basis.

1.5.2 Disk drive

The disk space in GB can be chosen for each server. The size can be changed by the administrator in the portal at any time. There are two disk types:

- SSD–tiered disk, geo-redundant (asynchronous)
- Standard disk, local redundant

1.5.3 RAM/Random Access Memory

RAM resources are fully available to the customer.

1.5.4 Backup/Disaster Recovery

Green regularly creates a replica of the VDC for a disaster scenario affecting the cloud infrastructure (network, storage, hypervisor). This replica is not accessible to the customer. The customer is responsible for data backup and for backing up the virtual server. Our option for this is called green Cyber Protect: https://www.green.ch/en/products/detail/cyber-protect-cloud

1.5.5 Snapshots

Snapshot technology enables the customer to independently create a snapshot via the service management portal at any given time. When a snapshot is retrieved, the virtual server is restored to the previously backed up status.

Snapshots are not a backup, but a short-term way of preventing the irreparable destruction of a system or enabling critical procedures to be carried out (software installation, patch installation etc.). The snapshots are created and deleted by the customer. The storage allowance for the subscription concerned is used for the snapshots.

1.5.6 Data storage location

The data are stored at Green's highly secure data centers, which are located and operated entirely in Switzerland.

1.5.7 Network/bandwidth

The virtual network technologies used in the VDC are based on the standards dictated by the cloud solution. Virtual networks are made available for the servers on the basis of these standards.
As a general rule, a bandwidth of 1,000 Mbit/s is available to a virtual internal network. For the first internal network, the use of this bandwidth is included in the monthly costs for the VDC. Additional internal networks and their use can be ordered as optional extras and are also billed monthly.

If you require external access to the virtual network, you can allocate a /28 public network to the internal network using the NAT function (activate direct Internet access by NAT). Access to the internal network is always port-based via NAT.

Green is authorised to remove customers from the network at any time and without warning if networks are abused or they are having a negative impact on the entire infrastructure (exceeding the fair use policy as detailed in Section 4.2 etc.).

1.6 Options

1.6.1 MIPS/Fixed IP addresses

The allocated IP addresses are available only to the customer to whom they are assigned. MIPS-packages of different sizes are available. 4 IP addresses (MIPS-4) are essential for applications such as email services, to ensure that the reverse DNS functions properly. The costs of any blocking (e.g. spam/phishing) are borne by the customer. Please note that, if a network is deleted and subsequently recreated, the same IP address range cannot be allocated a second time.

1.6.2 Green managed firewall

There is an optional Managed Firewall Service subscription, based on WatchGuard. Green handles all the administration and monitoring. A maximum of 8 zones can be connected. The Firebox V product is built in your admin zone, is completely virtualised and includes the standard security support. The firewall is als capable of terminating VPN-connections. Enhanced functions for the Basic Security Suite or the Total Security Suite can be supported.

1.6.3 Customer managed firewall

Green provides a template with a Firebox V. Configuration and maintenance are undertaken or arranged by the customer. Green provides the licence keys and the access details.

1.6.4 Image container

Green provides the customer with an image container, by means of which the customer can import his own disk images to the VDC. This enables whole servers to be directly migrated to the cloud or the customer's own operating systems to be used with the cloud.

VHDX and ISO formats are supported. The images can be uploaded to the image container via FTP, where they remain for 7 days. As soon as the uploaded image is attached to a server in the cloud, the image is moved from the image container to the VDC storage quota, where it remains until the customer removes the image from the server.

1.6.5 High Availability

The HA option enables you the freely choose the location of your VM's. Provisioning is done in DC Zürich-West or Zürich-City based on your selection. Your networks are shown in transparent mode (Layer 2) in both datacenters. Even geo-redundant high availability configuration are possible with this option.

1.6.6 Backup

Cyber Protect Cloud is our implementation of Acronis-Cloud-Backup. Please refer to our web-site: https://www.green.ch/en/products/detail/cyber-protect-cloud

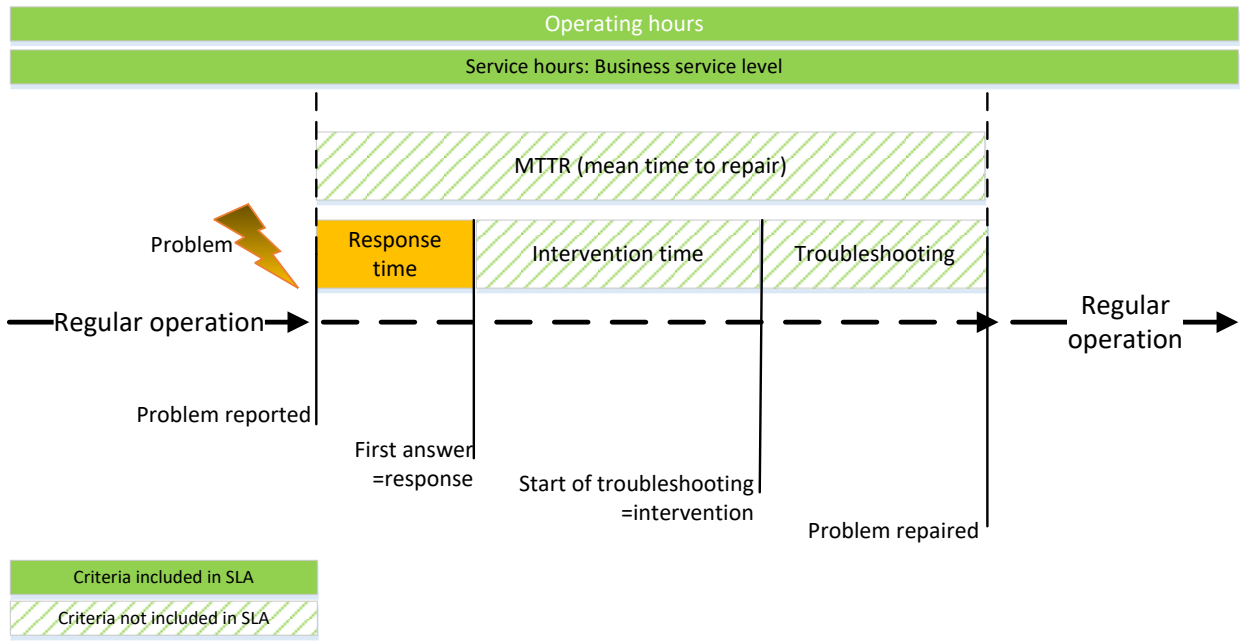
2. Service Level Agreement

The successful outsourcing of IT services calls for a transparent definition of the customer/supplier relationship. Green and the customer will stipulate the expected service level and the customer's obligations in the following Service Level Agreement ("SLA").

2.1 Definition of terms

Service Level, SL	Specified and measurable criteria for the achievement of a particular service quality by Green
Key Performance Indicators, KPI	Desired but not binding performance indicators
Service time	The service time is the time within which the contractually agreed services are rendered.
Normal hours	Normal hours are the hours between which the system is generally available. Planned and announced maintenance windows are not part of normal hours. Normal hours are a minimum of 8,604 hours and are calculated as follows: 1 year 24/7 = 8,760 h – 156 h maintenance window. In the case of a redundant architecture, the two redundant devices/equipment undergo maintenance at different times.
Availability	Availability [%] = 100 * ((normal hours - unplanned outages during normal hours/agreed normal hours). The agreed normal hours do not include the time frames for planned maintenance windows). Availability is guaranteed by Green on the data center infrastructure. This includes the following levels: Building with supply infrastructure, network, storage and hypervisor. To achieve high availability on the connection, the solutions at the end customer must also be designed with the requisite high availability.

Response time	The response time is the maximum time that passes between the occurrence or reporting of a fault and the start of fault analysis. Green endeavours to adhere to the indicated response times and to swiftly remedy outages and faults. However, observance of the response time cannot always be guaranteed. Failure to meet the response time will not incur a penalty or give rise to claims for damages
Mean Time To Repair, MTTR	Average time taken to carry out a repair or restore operation.
Maintenance windows	For the purposes of this SLA, "planned maintenance" is necessary in order to provide the services or update the infrastructure. Planned maintenance windows are set in advance and announced on status.green. Moreover, customers will be given at least 48 hours' notice ahead of the planned service interruption due to maintenance work. Green sends an email to the technical contact point named in writing by the customer, informing him of the planned service interruption and the nature of the interruption. If maintenance is necessary, Green will endeavour to carry it out during one of the regular maintenance windows, which are every Saturday from 5.30 a.m. to 8.30 a.m. Should unforeseen incidents or faults occur, Green has the right to carry out emergency maintenance at any time and without prior notice. In such cases the maintenance work is made public on our status page https://status.green.ch
Single Point Of Contact, SPOC	The single point of contact (SPOC) is the central point of contract for customers. This role is fulfilled by the Customer Care Center (Support Hotline +41 44 330 3535.



2.2 Customer Support

Green's highly qualified, multilingual support staff is available to the customer by telephone or via the online ticket system at www.green.ch to handle support requests and administrative enquiries. Customer Support can be contacted by phone from Monday to Friday between 8.00 a.m. and 5.00 p.m. (Swiss local time, excluding general public holidays). The Business Support Team is the first point of contact for all non-technical questions. Problems that cannot be resolved in consultation with the Support Team are passed on to the appropriate technical or commercial employees of Green.

Enhanced Customer Support
For emergency support (VDC not available) outside of the normal working hours, customer may use the same SPOC phone number.

Support is provided for all our services via standard channels:

Online support:	via ticket system
Phone SPOC	+41 44 330 3535
Live chat:	https://www.green.ch/support
The Green website:	http://www.green.ch/en/

2.2.1 Obligations of Support

- Checking the authorisation of the person making the request and the service level

- Commencing the fault management process and the troubleshooting process. The steps are as follows:
  1. Receipt of the request, opening of a trouble ticket and confirmation
  2. Prioritisation, coordination and monitoring of the troubleshooting process, using internal and external resources
  3. Inform the customer about the measures taken, workarounds and solution
  4. Inform the customer about the restoration of service availability
  5. Analyse root cause and recommendations going forward (change management) if required

2.2.2 Obligations of the customer

To guarantee a high standard of service, Green requires observance of the following guidelines:

- The customer provides all necessary contact information, including contacts for the escalation of all services rendered, and ensures that they are promptly updated to reflect any changes.
- The customer makes sure that the information about changes to the configuration, interfaces, channels, applications and systems relevant to the provision of joint services is passed on to Green and is always kept up to date.
- The customer is responsible for the maintenance of all customer applications. Green is not responsible for maintenance of customer applications or customer data.
- All equipment installed must be in perfect condition and must not present a risk to persons and objects.
- The customer may not have write access to managed devices of Green.

2.3 General measures to safeguard operations

At its data centers, Green exclusively provides services of the highest quality and security. The security of customer data and availability of services are ensured by measures including the following:

2.3.1 Structural, operational and technical measures to ensure physical security:

- Access control systems
- Video surveillance outside and inside the building
- Smoke, dust and water detectors
- Firefighting system
- Air conditioning via two separate cooling circuits
- Redundant power supply from energy provider
- Circular connection to the public high-voltage current system
- Power supply filtered through UPS
- High-performance diesel emergency power generators
- Duplication of supply cables in the building

2.3.2 Security and availability of internal network infrastructure:

- Segmentation of networks and strict separation of the different data flows
- Daily backup of own systems

- Use of firewalls at relevant points in the network
- Network monitoring by our own NOC (Network Operation Center)
- Exclusive use of branded components

2.3.3 Availability of external network connection:

- Carrier-neutral and redundant IP connection of the data center

2.4 Subject of the agreement, scope of application

This SLA applies only to the offer sent with the SLA and the resulting service contract. Other contracts between Green and the customer remain unaffected. The SLA can only be transferred to the VDC services and related options, but not to other product areas. In the event of inconsistency, the agreements in the relevant service contract take precedence over the provisions of the SLA. The applicable General Terms and Conditions of Green also apply.

3. Service level

A "Business" service level is available. The service level applies to all the systems and components included therein. The agreed service level is deemed to have been met if Green has achieved the thresholds agreed in these service agreements during the measurement period.

Performance	**Value or comment**
Guaranteed service level	
Availability	99.9% of the normal hours of the IaaS platform
Key Performance Indicator, KPI	
Response time	below 2 hours
Framework conditions	
Normal hours	24/7 (less planned and announced maintenance windows)
Service time	24/7
Office hours	Mon–Fri 8.00 a.m. to 5.00 p.m.
Technicians on standby outside office hours	✓
Priority handling	✓
Callback	✓
Fault reporting	By telephone +41 330 3535 contact form, out of office hours by same telephone as above
Business continuity	Must be ensured by the customer by means of a solution architecture

3.1 Availability

Availability is defined by the service level. Availability is guaranteed by Green on the data center infrastructure. This comprises the following layers: network, storage and hypervisor. To achieve 99.9% availability on the virtual server, the solutions at the end customer must be designed with the requisite high availability.

To measure the service level, availability is monitored by our own monitoring systems. Green uses various technical procedures to check the availability of the virtual machine. Alternatively, a fault can be reported by the customer, by opening a service ticket. Only Green's evaluations are relevant when reviewing claims.

3.1.1 Calculating availability

Availability=(normal hours-downtime)/normal hours*100
Green offers credits as soon as the service availability drops below the guaranteed thresholds. The tables in this document show the credits as percentages of the basic, monthly recurring charges (MRC). These credits and compensation payments are final. Any further or different compensation is excluded. No credit or payment shall be made for reasons or in an amount other than indicated here, including – but not limited to – loss of business suffered by the customer due to downtime.

3.1.2 Service guarantees

	VDC
Availability	99.9% of the normal hours of the IaaS platform
Service management 24x7 by Green's Server and Network Operation Center	✓

3.2 Portal activation

A portal will be made available to the customer to activate and administer his VDC basic subscription. The customer is aware that incorrect use of this portal (MyGreen/ VDC service management portal) may cause the entire customer infrastructure to go offline or be irretrievably deleted. Green accepts no liability in the event of incorrect use by the customer or by partners who have access to the end customer portal. In particular, all claims under the SLA will lapse.

3.3 Financial refund

If Green is unable to fulfil its contractual obligations, Green shall grant the customer for each registered hour of downtime (outside the service guarantee) a credit of 5% of the monthly subscription for the contract component involved, up to a maximum of 100% of the monthly subscription. All further claims for compensation are explicitly excluded. The customer must assert its claims to Green by submitting a request using the contact form

No SLA credit will be granted if a service is unavailable for a certain period of time due entirely or in part to one of the following causes:

1. The failure of equipment in the customer's premises (if not owned by Green), the customer's location (e.g. due to power failure) or of equipment of a provider of the customer
2. Natural disasters, terrorist attacks or other catastrophic events
3. An outage due to magnetic/electromagnetic interference or electrical fields
4. Any negligent conduct or omission by the customer (or by employees, representatives or sub-contractors or the customer), including:
   a. delays in the delivery of necessary equipment by the customer
   b. failure to grant Green adequate access to the facilities for test purposes
   c. failure to grant access to the customer's premises that is reasonably requested by Green (or its representatives) in order to enable Green to fulfil its obligations with regard to the services
   d. failure to take appropriate countermeasures with respect to the faulty services that are recommended by Green, or preventing Green from taking such measures itself
   e. failure to use redundancies, as required by the service level
5. negligence on the part of the customer or deliberate misconduct, including failure by the customer to follow agreed procedures
6. all planned maintenance periods, if the customer was informed of them, and emergency maintenance aimed at preventing future outages
7. switching off or suspension of the service by Green after the customer has not paid an invoice within 90 days of the invoice date, or on other reasonable grounds.

Lastly, the customer's equipment may not use more electricity than the power supply lines are able to supply at each point, in accordance with the service description. As devices require more electricity during the boot phase, the provider recommends an automatic start-up delay, to prevent overloads when rebooting after a power failure. Such an overload would be regarded as a design error by the customer and, as such, would not be covered by this SLA.

3.3.1 Demarcation points

This SLA applies to Green's virtual data center services. All the assurances given herein with regard to performance or operational readiness apply only to the equipment managed by Green between the equipment managed by the customer and Green's own providers. These providers include the electricity supplier, the lessors and other telecommunications companies.
If the customer manages his own equipment, Green's area of responsibility ends at the patch panels emanating from the patch room or at the end point of the carrier service (transfer point in the building).

3.3.2 Measurement and definition of downtime

Downtime (or unavailability of the service) is only taken into account if Green is responsible for it. Downtime is defined as follows: It starts at the time the customer opens the support request or Green itself identifies an error and ends when an employee of the provider reports the resolution of the problem. No other measurement of downtime applies and all times used for this calculation are those

recorded by Green. Operating time calculations are performed independently for each service, the lowest value (the longest downtime) being used to calculate the credit for the customer.

4. Obligations of the customer

In particular, the customer shall ensure that:

- the servers are adequately protected against threats of any kind from the Internet,
- the servers are not misused, i.e. the absence of passwords or very simple passwords,
- no ports are opened that could compromise the VDC system stability,
- no illegal content is hosted on the servers,
- no illegal applications are installed (e.g. spammers),
- all installed applications and operating systems are properly licensed,
- no applications are installed that are unsuitable for VDC solutions and could negatively affect the VDC platform (e.g. streaming, game servers, computers with constant, guaranteed maximum performance etc.),
- the servers are regularly backed up using suitable third-party software (e.g. online backup by Green),
- both the postal and electronic contact address is always up to date.

4.1 Licensing

Green requires its customers to have 100% correct licences for all operating systems and applications used. When using Microsoft products, the customer is obliged to correctly license them in accordance with Microsoft's applicable licensing terms.
Specifically, products may only be operated in SPLA mode (Service Provider License Agreement) or License Mobility mode (Volume License with Software Assurance). Microsoft explicitly prohibits the use of certain applications on the VDC platform (such as Office 365).

Green has no access to end customer systems. Aside from the licensing of Windows SQL servers (if DBaaS is used), managed/unmanaged firewall and cloud security included in the VDC service, the customer is responsible for the correct licensing of the products used.

By using the Green cloud products, the customer undertakes to provide Green during audits with a summary of the licences for its platform. The customer compiles and sends the summary in cooperation with Green. Green does not have access to the end customer's platform at any time, including during an audit.

If the operating system and applications on a virtual server are not correctly licensed, Green is authorised to retroactively charge all the licence costs and any penalties imposed by the software supplier from the time of first operation of the server.

4.2 Fair Use Policy

All services that we offer without limitation in our VDC products are subject to the Fair Use Policy or the fair use principle.

This principle ensures that we do not have to impose restrictions on traffic volumes and other limitations. It is assumed that the customer will make fair use of the available resources. The customer is aware of the Fair Use Policy and acknowledges that he must not abuse this for personal, economic or financial gain.

Examples of what does and does not constitute fair use:

OK	Not OK
Running a VDC for business or private purposes	Running the virtual server predominantly or exclusively as a download server
Websites that **temporarily** require more traffic, e.g. due to an event	Websites that are likely to have heavy traffic on a permanent basis, such as larger communities, large corporate sites etc. Heavy traffic is defined as follows: Green defines as the average the entire traffic of the VDC platform divided by the number of virtual servers. If a customer regularly or constantly exceeds more than 4 times this volume, Green may draw this to the customer's attention.
Commercial and non-commercial content	Unlawful or other criminal content
Business applications on the virtual servers	Installing applications that are unsuitable for virtual server solutions and could negatively affect the VDC platform (e.g. streaming, game servers, computers with constant, guaranteed maximum performance etc.)
Correct licensing of all SW packages installed on the server	Use of software products that are in breach of the respective manufacturer's licence agreement
Reselling with officially registered resellers and with partner contracts	Reselling without officially registered reseller status and without partner contracts

4.3 Transfer point

When Green activates the VDC portal, responsibility for the VDC passes to the customer. Green defines the WAN segment/28 as the transfer point for responsibility. From this point on, the customer is responsible for ensuring that his servers are adequately protected and regularly backed up.

4.4 Firewall

Running servers "openly" on the VDC is not permitted. The servers must be adequately protected by the firewall built into the operating system or the service management portal or by a third-party product.

If certain ports are opened by the customer, the customer must additionally ensure that further security measures are built into the application.

Green regularly tests the security of the end customer systems and reserves the right to immediately and without prior warning remove from the network unprotected systems that are connected to the Internet.

Example:
Opening of Port 25 (SMTP) Incoming: The customer must ensure that the server is not misused as an open relay.

4.5 Breach of the SLA by the customer

If the customer is in breach of this SLA, Green is authorised to remove the server from the network at any time, without advance notice. If the customer's virtual server causes damage, Green is authorised by law to force its shutdown.

4.6 Warning messages

It is the customer's responsibility to open support requests for all unresolved problems. The generation of an automatic warning message by Green does not constitute confirmation of a problem. Only a properly opened ticket can be used to calculate downtime and credits.

4.7 Customer involvement following a power failure

Following a power failure, it is up to the customer to take all necessary steps to get his equipment back online.

5. Service management

5.1 Incident management

5.1.1 Outage notification

Green informs the customer's technical contact person either by telephone or email (in the case of written notification, to the contact details provided to Green).

5.1.2 Fault procedure

Green's philosophy is to provide the customer with the best possible availability and service quality, from a technical and an operational perspective. In the event of faults, our primary aim is to deal with the issue quickly and restore service availability. This benefits the customer by minimising the impact on his business activities.
Faults and outages affecting services that are "reactively" managed must be reported by the customer. Once the outage has been reported, a trouble ticket is opened. The analysis of the problem then commences. The service is restored in accordance with the agreed service level.
Faults and outages affecting services that are "proactively" managed are reported by the monitoring system. The customer is informed in accordance with the agreed service level. If the outage impacts

on the customer's business activities, the customer must open a trouble ticket via the appropriate channels.

Obligations of Support

a. Ascertaining and checking the authorisation of the person submitting the request and comparing with the service level agreement between the customer and provider.
b. Starting the fault management process, which involves:
    1. Receipt of the request, opening of a trouble ticket and confirmation.
    2. Prioritising, coordinating and monitoring the troubleshooting process, using internal and external resources.
    3. Informing the customer about the measures taken, workarounds and solution.
    4. Informing the customer about the restoration of service availability.

In the case of unforeseen delays to troubleshooting that cause a breach of the SLA, internal escalation is automatically initiated. Depending on the nature of the problem, either internal senior employees or the distributor's/subcontractor's support are the first level of escalation. At this point, the manager on duty is involved to ensure that the SLA is observed during the escalation process and the problem is resolved promptly.

5.2 Amendment procedure

Amendments to the customer agreement are agreed in writing, unless otherwise agreed. Amendments that are not in writing are invalid. In the absence of any specific agreement, the costs incurred in connection with contract management are borne by each contracting party.
The contracting parties check the proposed amendments and inform the requesting party of their consent or, if appropriate, requested changes, in writing, usually within two weeks of submission of the proposed amendments. As a rule, the party whose consent is sought agrees to or rejects the proposed amendment within two weeks of submission of the revised proposal or alternative proposal.
If a party rejects an amendment proposal, stating reasons, or if the other party does not accept the amendment proposal, or does not do so within the binding deadline, the agreed service scope and conditions will continue to apply unchanged.

5.3 Use of subcontractors

In general, Green provides the contractual services with its own employees and resources. However, it is authorised to use third parties and/or employees of external companies (hereafter "subcontractors") for the rendering of the contractual services.
Only companies accredited by Green and their qualified specialists will be used. The subcontractors satisfy the same reliability requirements as the provider itself.

In addition, the following applies to the use of subcontractors:

- Green remains the sole point of contact for the customer with regard to all services rendered by the subcontractor.
- Green has a duty to ensure that the subcontractor abides by the contractual obligations with respect to the customer.
- Green remains responsible for the selection, monitoring and instruction of the subcontractor and the use of the subcontractor does not discharge Green from its own performance obligations. Claims on account of slight negligence are, however, excluded.

- Green must conclude a written contract with each subcontractor, documenting the subcontractor's obligations.

The services rendered by the subcontractor are rendered on behalf of Green, as if they were its services.

The use of subcontractors in the collection, processing and utilisation of company-related and personal data is also subject to the provisions on data protection pursuant to Green's General Terms and Conditions (T&C). Irrespective of the above conditions for the use of subcontractors, the sharing of company-related and personal data is only permitted if the subcontractor has accepted the data privacy agreement pursuant to the T&C. As a general rule, personal data relating to the customer may only be transferred by the provider and its subcontractors to countries outside Switzerland if the customer has given written permission and this is allowed under the data privacy requirements.

5.4 Escalation initiated by the customer

If the customer fears that either the speed or quality of support/the troubleshooting process could seriously jeopardise his business, the customer has the possibility to independently initiate an escalation.

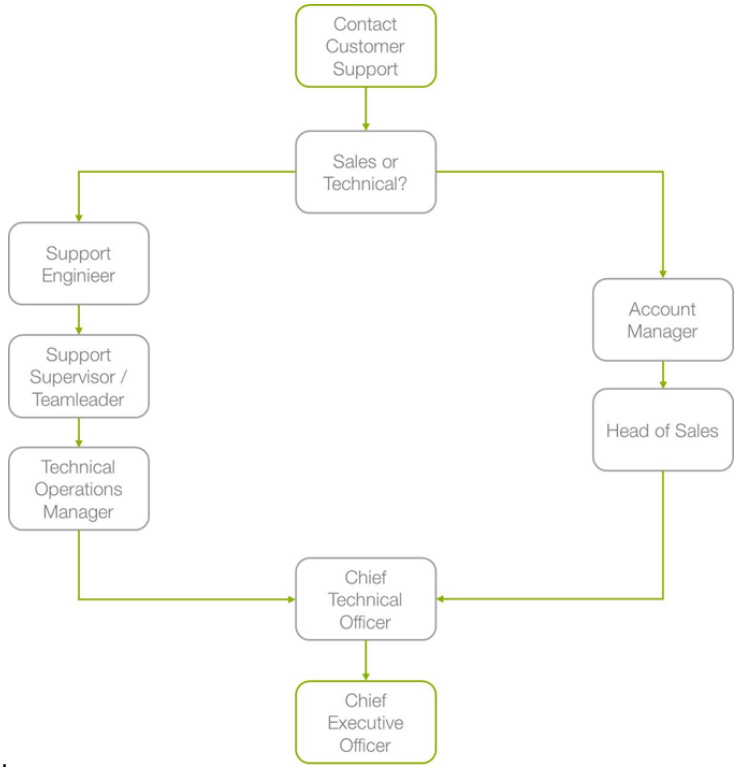


Diagram 1 - Escalation process

Obligations of the customer

a. The customer provides all necessary contact information, including contacts for the escalation of all services rendered, and ensures that they are constantly updated to reflect any changes.

b. The customer supplies and updates for Green a list of all persons who are entitled to access support.
c. The customer implements and updates suitable resources for the identification of those authorised persons.
d. The customer makes sure that the information about changes to the configuration, to interfaces, channels, applications and systems relevant to the provision of joint services is passed on to the provider and is always up to date.
e. The customer is responsible for the continual maintenance of all customer applications. The maintenance of customer applications or customer data is the customer's sole responsibility.
f. All equipment installed must be in perfect condition and must not present a risk to persons and objects.
g. The customer must make sure that Green has access to the equipment managed by Green at all times and for all reasons. Failure to ensure this shall constitute a breach of the agreement and may result in the termination of the contract.
h. The customer has no write permission on the devices managed by Green.
i. When working with Green employees, all activities must be coordinated in advance. This applies to the use of service options such as additional accounts or network changes.
j. Any unauthorised attempt by a customer, either physically or electronically, to gain access to Green's equipment is strictly forbidden. This also applies to CPE (Customer Premise Equipment).

5.5 Insurance

Green systems are insured against the relevant risks. However, neither customer data nor the availability of the services supplied by the customer to his own customer base is in any way insured. It is the customer's express responsibility to get insurance cover. No compensation is paid for the loss of business information or other impact of system outages in excess of the credit percentages expressly described in this document.

6. Legal provisions

6.1 Establishment of a legal relationship

The placing of an order on the website creates a legal relationship between Green and the customer. Measurement of the SLA parameters commences only after the first successful login on the portal. This document forms an integral contractual annex to the web order submitted to Green.

6.2 Compliance with local laws

The customer ensures that no illegal data traffic is sent via Green connections. Green accepts no liability for this.

6.3 Limitations

All remuneration for Green Services is limited to the amounts indicated in this document. No credit or payment shall be made for reasons or in an amount other than indicated here, including – but not limited to – loss of business suffered by the customer due to downtime.

6.4 Use of personal data

Customers expressly accept the Guidelines on the use of personal data adopted by Green.
See: https://www.green.ch/en/legal-aspects/data-privacy

6.5 Amendments

Green reserves the right to amend this document from time to time, provided the customer is duly informed before the changes take effect. If the changes have a significant impact on the services, the service charge or other obligations arising from this contract, the customer may terminate this contract, in writing, at any time, observing the notice period of one month.

7. Glossary

Abbreviation		Definition of terms
DNS	Domain Name System	Directory service in IP-based networks; its primary purpose is to respond to requests for name resolution.
IAAS	Infrastructure as a Service	Provision of virtualised IT infrastructure via public or private networks, usually via the Internet. In IaaS, the customer uses server, storage, network and the other data center infrastructure as an abstract, virtualised service over the Internet.
IP address	Internet Protocol address	Address in computer networks, which – like the Internet – is based on the Internet protocol. It is assigned to devices that are connected to the network, enabling an address to be typed in to access the devices.
Gbit	Gigabit	Data transmission rate. Denotes the digital data volume that is transmitted within a time unit via a transmission channel.
MIPS	Managed IP Service	Service whereby Green connects you to the Internet with fixed IP addresses.
NAT	Network Address Translation	Collective term used in data centers for processes that automatically replace address information in data packets with different information inorder to connect various networks. Typically, therefore, they are used on routers.
LAN	Local Area Network	Computer network comprising at least two computers and covering a limited area.
RAM	Random Access Memory	A store of information, used particularly in computers as a working memory, usually in the form of memory modules
SLA	Service Level Agreement	Agreement or interface between client and service provider for recurring services.
SSD	Solid State Drive	The solid state drive (hard disk) is a very fast electronic storage medium.
STD-DISK	Standard disk	Disk based on conventional technology with less data throughput than SSD
UPS	Uninterruptible power supply	Used in case of faults affecting the power grid to safeguard the supply of critical electrical loads.
VPN	Virtual Private Network	A closed computer network built on a public network infrastructure.
VDC	Virtual data center	The virtualisation of your company at Green's data centers.
WAN	Wide Area Network	Computer network covering a very large geographical area.