Disaster Recovery as a Service (DRaaS)
DRaaS solutions from Green Cloud Technologies

RECOVERY OF YOUR MOST IMPORTANT ASSET.

Let’s face it - things happen. Servers kick the bucket. Mother Nature wreaks havoc. And, yes, sometimes the data you thought you were backing up isn’t actually backing up at all. Like Murphy’s Law, if it can go wrong, sometimes it will.

Whatever the circumstance, data is the engine that powers most businesses. Perhaps, it is your company’s most important asset. And, losing that data permanently - or even temporarily - can destroy a business through the inability to operate, loss of critical documents or failure to deliver a service or project.

We hang our hat on being disaster recovery experts. Our products are Cisco Powered, built on validated Cisco architectures. And with industry leading technology partners, like Zerto and StorageCraft, your data will be replicated and readily available when - or if - you need it.

According to US Census Bureau research, 93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of a disaster; and 50% filed for bankruptcy immediately.

Yet, 56% of organizations in North America don’t have a tested disaster recovery plan.

DATA CENTER SPECIFICATIONS

<table>
<thead>
<tr>
<th>Features</th>
<th>Specifications</th>
</tr>
</thead>
</table>
| Locations | Greenville, SC (Immedion)  
Nashville, TN (Peak 10) |
| Certifications | SSAE16 SOC 1 Type II  
Uptime Institute Tier 3 |

PRODUCT SPECIFICATIONS

<table>
<thead>
<tr>
<th>Features</th>
<th>ServeRestore Specifications</th>
<th>ExpressRestore Specifications</th>
</tr>
</thead>
</table>
| Storage   | NetApp FAS32xx Series Filers with RAID-DP  
Tintri VMstore™ | NetApp Clustered ONTAP  
NetApp 7 Mode ONTAP  
Tintri VMstore™ |
| Software  | VMware vCloud  
StorageCraft ShadowProtect | VMware vCloud Director  
Zerto |
| OS Supported | Windows Server 2003 (R2), 2008 (R2), 2012 (R2) | Any valid VMware supported OS |
| Hypervisors Supported | NA | VMware*  
Hyper-V** |
| SQL Server Versions Supported | 2005 SP4 and newer. | 2003 or newer (SBS not supported) |
| Exchange Versions | 2003 or newer (SBS not supported) | |
| File Level Restore | File level restore capabilities available locally using provided StorageCraft tools or at $150 per incident via Green Cloud Support. | |
| Bandwidth Requirements | Minimum of 1M upload | |
| Remote Connectivity | RDP, SSL VPN and IPSEC Site to Site VPN | RDP, SSL VPN and IPSEC Site to Site VPN |
| Encryption | Data is encrypted when transferred and stored data can also be encrypted at customer request. | |
| Licensing | Microsoft Windows Server OS licenses for recovery in our cloud  
StorageCraft ShadowProtect Licenses | Microsoft Windows Server OS licenses for recovery in our cloud  
Zerto licenses for all protected VMs.  
NetApp ONTAP and Tintri OS licenses for source devices not included. |

*Vsphere Enterprise Edition with vCenter required for Zerto options.  
**Hyper-V only supported with San-to-San replication without cloud recovery.
While traditional backup may take days to recover, ServeRestore can restore your on-premise data in a virtual data center in just a few hours. Take a look at your recovery time objective (RTO) and choose an option that best fits your needs.

**Restoration Guidelines**
- **Servers 1 - 5:** Up to 4 hours
- **Each Additional 5 Servers:** 1 hour

**REAL-WORLD SERVER RESTORATION SCENARIOS**

<table>
<thead>
<tr>
<th>Example A</th>
<th>Example B</th>
<th>Example C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law Office: 5 Servers</td>
<td>Non-Profit: 10 Servers</td>
<td>Medical Office: 20 Servers</td>
</tr>
<tr>
<td>Total Data: 500G</td>
<td>Total Data: 1TB</td>
<td>Total Data: 2TB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Servers 1 - 5</th>
<th>Additional Servers</th>
<th>Recovery Time Objective (RTO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 hours</td>
<td>-</td>
<td>4 hours</td>
</tr>
<tr>
<td>4 hours</td>
<td>1 hour</td>
<td>3 hours</td>
</tr>
<tr>
<td>4 hours</td>
<td>5 hours</td>
<td>7 hours</td>
</tr>
</tbody>
</table>

**THE 3-2-1 RULE FOR BACKUP AND REPLICATION.**

The 3-2-1 rule is a simple, best practice method for preventing data loss in any scenario. It suggests having:

1. **One backup located offsite.**
2. **Two different forms of storage media** (i.e. tape, NAS, or offsite).
3. **Three copies of your data:** one production copy, two backups.

Find out how Green Cloud’s disaster recovery solutions, as well as our new backup service, can help provide a 3-2-1 scenario for your data.

For more information on our new backup solution, go to www.gogreencloud.com/backup.
**DISASTER RECOVERY FOR ON-PREMISE ENVIRONMENTS.**

ServeRestore, our cloud disaster recovery solution for on-premise physical servers, is often called our “better than backup” solution. Traditional backup approaches lack the flexibility and efficiency of virtualization, requiring manual, time-consuming backup and restoral processes or complex server failover configurations. That could take days.

With ServeRestore, our engineers pre-build a fully configured virtual environment for your data. When disaster strikes, we fully manage the recovery of your servers, configuring them to run within our cloud environment in just a couple of hours*.

You continue to operate from our virtual environment for up to two weeks. Then, you can decide to stay in the cloud or purchase hardware and rebuild your on-premise environment. The choice is yours. However, to date, 100% of businesses who have failed over to a virtual environment have chosen to remain there permanently.

**RECOVERY IN HOURS, NOT DAYS.**

While traditional backup may take days to recover, ServeRestore can restore your on-premise data in a virtual data center in just a few hours. Take a look at your recovery time objective (RTO) and choose an option that best fits your needs.

Restoration Guidelines
Servers 1 - 5: Up to 4 hours
Each Additional 5 Servers: 1 hour

**REAL-WORLD SERVER RESTORATION SCENARIOS**

<table>
<thead>
<tr>
<th>Example</th>
<th>Server</th>
<th>Total Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Law Office: 5 Servers</td>
<td>500G</td>
</tr>
<tr>
<td>B</td>
<td>Non-Profit: 10 Servers</td>
<td>1TB</td>
</tr>
<tr>
<td>C</td>
<td>Medical Office: 20 Servers</td>
<td>2TB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Servers 1 - 5</th>
<th>4 hours</th>
<th>4 hours</th>
<th>4 hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Servers</td>
<td>1 hour</td>
<td>1 hour</td>
<td>3 hours</td>
</tr>
<tr>
<td>Recovery Time Objective (RTO)</td>
<td>4 hours</td>
<td>5 hours</td>
<td>7 hours</td>
</tr>
</tbody>
</table>

**DISASTER RECOVERY FOR VIRTUAL ENVIRONMENTS.**

ExpressRestore, our disaster recovery solution for virtualized environments, is powered by Zerto, the industry’s most comprehensive hypervisor-based data replication solution for VMware vSphere. It offers a faster recovery and RTO with production-class replication targets for SSD, SAS or SATA per virtual machine.

We provide a Zerto graphical user interface allowing the customer to initiate recovery directly into our hosted VMware environment. With easy point and click technology, the customer can select any VM to replicate and boot up in Green Cloud's data center.

At any time, the customer can perform failover and fail-back testing using the self-service portal at no additional cost. And our engineering team will help ensure all networking is preset to your specifications. This pre-configured direct connection allows for a simple, fast recovery and management in as little as 15 minutes.

**THE 3-2-1 RULE FOR BACKUP AND REPLICATION.**

The 3-2-1 rule is a simple, best practice method for preventing data loss in any scenario. It suggests having:

1. **One backup located offsite.**
2. **Two different forms of storage media (i.e. tape, NAS, or offsite).**
3. **Three copies of your data: one production copy, two backups.**

Find out how Green Cloud's disaster recovery solutions, as well as our new backup service, can help provide a 3-2-1 scenario for your data.

For more information on our new backup solution, go to www.gogreencloud.com/backup.
Disaster Recovery as a Service (DRaaS)

DRaaS solutions from Green Cloud Technologies

RECOVERY OF YOUR MOST IMPORTANT ASSET.

Let’s face it - things happen. Servers kick the bucket. Mother Nature wreaks havoc. And, yes, sometimes the data you thought you were backing up isn’t actually backing up at all. Like Murphy’s Law, if it can go wrong, sometimes it will.

Whatever the circumstance, data is the engine that powers most businesses. Perhaps, it is your company’s most important asset. And, losing that data permanently - or even temporarily - can destroy a business through the inability to operate, loss of critical documents or failure to deliver a service or project.

We hang our hat on being disaster recovery experts. Our products are Cisco Powered, built on validated Cisco architectures. And with industry leading technology partners, like Zerto and StorageCraft, your data will be replicated and readily available when - or if - you need it.

According to US Census Bureau research, 93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of a disaster; and 50% filed for bankruptcy immediately.

Yet, 56% of organizations in North America don’t have a tested disaster recovery plan.

DATA CENTER SPECIFICATIONS

<table>
<thead>
<tr>
<th>Features</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locations</td>
<td>Greenville, SC (Immedion) Nashville, TN (Peak 10)</td>
</tr>
<tr>
<td>Certifications</td>
<td>SSAE16 SOC 1 Type II Uptime Institute Tier 3</td>
</tr>
</tbody>
</table>

PRODUCT SPECIFICATIONS

<table>
<thead>
<tr>
<th>Features</th>
<th>ServeRestore Specifications</th>
<th>ExpressRestore Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>NetApp FAS32xx Series Filers with RAID-DP Tintri VMstore™</td>
<td>NetApp Clustered ONTAP NetApp 7 Mode ONTAP Tintri VMstore™</td>
</tr>
<tr>
<td>Software</td>
<td>VMware vCloud StorageCraft ShadowProtect</td>
<td>VMware vCloud Director Zerto</td>
</tr>
<tr>
<td>OS Supported</td>
<td>Windows Server 2003 (R2), 2008 (R2), 2012 (R2)</td>
<td>Any valid VMware supported OS</td>
</tr>
<tr>
<td>Hypervisors Supported</td>
<td>NA</td>
<td>VMware* Hyper-V**</td>
</tr>
<tr>
<td>SQL Server Versions Supported</td>
<td>2005 SP4 and newer.</td>
<td>2003 or newer (SBS not supported)</td>
</tr>
<tr>
<td>Exchange Versions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Level Restore</td>
<td>File level restore capabilities available locally using provided StorageCraft tools or at $150 per incident via Green Cloud Support.</td>
<td></td>
</tr>
<tr>
<td>Bandwidth Requirements</td>
<td>Minimum of 1M upload.</td>
<td></td>
</tr>
<tr>
<td>Remote Connectivity</td>
<td>RDP, SSL VPN and IPSEC Site to Site VPN</td>
<td>RDP, SSL VPN and IPSEC Site to Site VPN</td>
</tr>
<tr>
<td>Encryption</td>
<td>Data is encrypted when transferred and stored data can also be encrypted at customer request.</td>
<td></td>
</tr>
<tr>
<td>Licensing</td>
<td>Microsoft Windows Server OS licenses for recovery in our cloud StorageCraft ShadowProtect Licenses</td>
<td>Microsoft Windows Server OS licenses for recovery in our cloud Zerto licenses for all protected VMs. NetApp ONTAP and Tintri OS licenses for source devices not included.</td>
</tr>
</tbody>
</table>

*Vsphere Enterprise Edition with vCenter required for Zerto options.**Hyper-V only supported with San-to-San replication without cloud recovery.
ExpressRestore DRaaS via Zerto

Service Description

Introduction ........................................................................................................................................... 2
Service Options (Scope) ..................................................................................................................... 2
Prerequisites ......................................................................................................................................... 2
Service Operations ..............................................................................................................................

Implementation Plan and Timeline ................................................................................................. 3

Service Support .................................................................................................................................. 4
  Customer Operations ....................................................................................................................... 4
  Network Operations ......................................................................................................................... 4
  Availability ........................................................................................................................................ 4
  Business Hours ................................................................................................................................. 4
  On-Call Hours .................................................................................................................................. 4
  Incident Categorization & Management .......................................................................................... 5
  Problem Management ..................................................................................................................... 6
  Event Management .......................................................................................................................... 7
  Major Incidents / Outage Response Process ................................................................................... 7

Disaster Recovery ............................................................................................................................. 8

Change Requests ............................................................................................................................... 8
  Simple ............................................................................................................................................... 8
  Normal .............................................................................................................................................. 9
  Complex .......................................................................................................................................... 9

Critical Success Factors .................................................................................................................... 9

Billing and Costs ................................................................................................................................. 9

Authorization ........................................................................................................................................ 10
Introduction
ExpressRestore Disaster Recovery as a Service (DRaaS) via Zerto provides Green Cloud Customers and Partners with an interface to recover a protected server group to the Green Cloud hosted VMware environment. This allows for self-service recovery with approximately one hour Restore Time Objective, depending on the size of the protected environment.

Green Cloud is solely channel focused and will only sell products and services through an authorized partner.

Service Options (Scope)
Unless otherwise stated, only the work and products outlined in the Scope section below are covered under this Service Description. Ancillary products and services can and will be charged separately through additional Proposals, Work Orders, or addendums. The initial Proposal products and/or pricing may need to be adjusted following the discovery or implementation phases, in order to meet Service Level Objectives for the product.

All of Green Cloud’s provisioning and support is to be performed remotely and as such, no on-site access will be necessary.

The primary objective of ExpressRestore DRaaS via Zerto is to provide the end-user with an interface to manage and initiate their own server environment recovery to the Cloud.

The Service Options for the product are:

- Initial test failover with Green Cloud assistance included
- 10 Mb/s replication bandwidth over public Internet or IPsec VPN included (Higher bandwidth speeds and MPLS interconnections are available, through additional products/services)
- Choice of SSD, SAS, or SATA (Premium, Standard, and Archival) replication targets on a per VM basis.
- Support for any Guest OS that is supported by VMware
- Support for VMware hypervisor only (Hyper-V not supported)
- Zerto licensing for all protected virtual servers
- Microsoft Windows Server OS licenses for recovery in the Green Cloud infrastructure
- Remote connectivity via RDP, SSL VPN, and IPsec VPN
- Standard customer service and frontline technical support included (Professional Services available)

Prerequisites

- Customer VMware environment must have vCenter deployed with VMware Essentials
- Bandwidth between customer premise and the Green Cloud datacenter must be sufficient to manage replication and also production traffic in the event of a failover
- If the customer will be moving production users to a secondary site in the event of a failover, bandwidth from the secondary site to the Green Cloud datacenter must be sufficient to manage production traffic
- Should the customer choose the “failback” option, moving production servers from the Green Cloud datacenter back to the premise or a recovery site, the VMware vCenter environment at that location must be Enterprise edition
After delivery of the product, it is the end-user’s responsibility to notify Green Cloud in the event of any major vCenter changes that could impact the performance of ExpressRestore failover. The following client-side changes will impact the ability for the environment to be recovered at Green Cloud:

- Adding or removing hosts and other cluster hardware
- Changing cluster-wide settings like DRS
- Licensing changes
- Networking changes that might affect VPN connectivity
- VMware platform upgrades
- Significant increases in hardware resource requirements for protected VMs
- Changing the storage platform on which a VRA is hosted

**Service Operations**

**Implementation Plan and Timeline**

Through the Implementation Plan, Green Cloud will identify the necessary resources to support the environment in the Green Cloud infrastructure, manage the initial “seeding” of the recovery environment, configure the Zerto software and applications, and provide credentials to the self-service portal to the responsible end-user party.

The Partner/Customer responsibilities include providing full and complete documentation regarding the protected server environment, configuring local VPN end-point(s) for connectivity, managing the temporary installation of network attached storage (NAS) device, as needed, and following written procedural documentation provided by Green Cloud.

<table>
<thead>
<tr>
<th>Duration</th>
<th>Milestone/Requirement</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sales Order Site Survey</td>
<td>Partner, Customer, and Green Cloud Channel</td>
</tr>
<tr>
<td>1-3 days</td>
<td>IaaS Environment Setup and Customer Preparation</td>
<td>Green Cloud Operations</td>
</tr>
<tr>
<td>1-2 days</td>
<td>Zerto Cloud Manager (ZCM) Setup</td>
<td>Green Cloud Operations</td>
</tr>
<tr>
<td>1 day</td>
<td>Configure Zerto Cloud Connector (ZCC)</td>
<td>Green Cloud Operations</td>
</tr>
<tr>
<td>2-5 days</td>
<td>Initial Customer Site Configuration</td>
<td>Green Cloud Operations and Customer/Partner</td>
</tr>
<tr>
<td>3-30 days*</td>
<td>Seeding via NAS (if applicable)</td>
<td>Green Cloud Operations and Customer/Partner</td>
</tr>
<tr>
<td>1-2 days</td>
<td>Customer Site Finalization</td>
<td>Green Cloud Operations</td>
</tr>
<tr>
<td>1-3 days</td>
<td>Virtual Protection Group (VPG) Setup</td>
<td>Green Cloud Operations</td>
</tr>
<tr>
<td></td>
<td>Delta Sync</td>
<td></td>
</tr>
<tr>
<td>2 days*</td>
<td>Finalization, ZSSP Access, Failover Test</td>
<td>Green Cloud Operations and Customer/Partner</td>
</tr>
</tbody>
</table>
*some timeline estimates dependent on Partner/Customer scheduling with Operations, on-site access, and communication methods*

NOTE: The timeline outlined above assumes there is no delay in communication between high-level milestones. There are several end-user requirements outlined in the Onboarding Procedure which require sign-off, validation, or on-premise action and may delay Green Cloud from satisfying the requirement within the expected duration.

**Service Support**

Green Cloud Operations will address and manage all customer service needs: new customer provisioning, existing customer change requests, customer incidents and customer problems. The Service Operations function is also responsible for management and resolution of system and network related alerts and events.

**Customer Operations**
The Customer Operations role satisfies all customer technical support incidents, customer change requests, and normal and standard new order provisioning.

**Network Operations**
The Network Operations role addresses and resolves customer problems escalated from Customer Operations and also manages the customer network infrastructure. They partner with the Engineering team to insure that all network service level objectives are met.

**Availability**
Service Operations management is located at 411 University Ridge, Suite 201 in Greenville, South Carolina. The Service Operations function is accessible to Partners and Customers via two methods: e-mail, and telephone.

- The Service Operations e-mail address is support@gogreencloud.com
- The telephone number for Partners/Customers is 877-465-1217.

**Business Hours**
The Customer Operations group will staff a centralized support desk to handle all requests and order provisioning during defined business hours. These hours are currently defined as Monday through Friday, 8:00am until 6:00pm Eastern time. New customer provisioning and change requests are handled during this time.

**On-Call Hours**
Outside of Business Hours, the Green Cloud Operations group will staff at least one (1) technician to answer incoming telephone calls and respond to email requests for urgent service impacting incidents. NOTE: new customer provisioning and change requests are deferred until start of next business day.
The use of automated on-call paging is leveraged after business hours and weekends to insure 24/7 availability for service impacting Incidents.

Unscheduled normal or standard service changes or unscheduled service provisioning requests are not typically completed outside of business hours, at Operations management’s discretion, unless otherwise arranged through Professional Services or Statement(s) of Work.

**Incident Categorization & Management**

The Operations Manager is responsible for real-time assessment of new, unassigned customer requests and incidents in the incident management system. This team member will prioritize, categorize, assign, and update new incoming requests to be best handled by Customer Operations.

**Ticket Creation**

Customers are to email or phone the Operations group to have a new incident or change request created. System Events generating alerts from monitoring applications are automatically tracked in the ticket management system.

**Ticket Categorization (Type, Status, & Priority)**

**Request Type**
- Event – system generated alert indicating possible impact to customer service
- Incident – record of impact to customer service as reported by customer or monitoring systems
- Problem – an impact to customer service with no currently known resolution
- Question – a general inquiry resulting in no service or account information change
- Customer MACD – request to modify or deliver new products
- Billing – request related to invoicing or payments

**Status**
- Open – issue or request is currently being addressed or awaiting work from an agent.
- Pending – issue requires work from an agent, but later time (or the issue is not service impacting)
- Waiting on Customer – the agent can perform no further work until the Customer responds
- Waiting on Third Party – the agent can perform no further work until the Third Party responds
- Resolved – the incident has been remedied and tested by Green Cloud, but not yet confirmed
- Closed - the incident has been confirmed as resolved and no further action is needed

**Priority**
- Low –
  - Incidents -- No service impact
  - Requests – No required completion date/time
- Medium –
  - Incidents/Problems - Less than 50% service impact
  - Requests - Completion date/time more than 24 hours
- High –
  - Incidents/Problems - More than 50% service impact, but some services working
- Requests - Completion within next 24 hours
- Urgent –
  - Incidents/Problems - All services down
  - Requests - Immediate requested completion

**Service Level Objectives**

A designated member of the Operations team will be responsible for real-time assessment of new, unassigned customer requests in the incident management system. This team member will prioritize, categorize, assign, and update new incoming requests to be best handled by Customer Operations.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Response SLO</th>
<th>Resolution SLO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgent</td>
<td>15 minutes</td>
<td>1 hour</td>
</tr>
<tr>
<td>High</td>
<td>30 minutes</td>
<td>4 hours</td>
</tr>
<tr>
<td>Medium</td>
<td>1 hour</td>
<td>1 day</td>
</tr>
<tr>
<td>Low</td>
<td>2 hours</td>
<td>2 days</td>
</tr>
</tbody>
</table>

When an SLO target is violated, a notification is immediately delivered to management to prompt action. All service change requests have priority “Medium” by default.

**Problem Management**

Incidents received by the Customer Operations group which have no known resolution are created as Problem tickets and handed off to the Network Operations group for acknowledgement, categorization, and root cause analysis.

Network Operations will engage external vendors not only for problem reporting, but also to identify and rectify provisioning or networking errors.

- Problems which are customer impacting and require analysis from external vendors will be submitted to the vendor within one (1) hour of receipt
- Problems which require root cause analysis and are not customer impacting will be submitted to the vendor within four (4) hours of receipt
- Problems which require provisioning or networking changes will be submitted to the vendor within twenty-four (24) hours of receipt

The Green Cloud Network Operations engineer must request and obtain a vendor tracking number for the issue and record that tracking number in the related problem management system. Regular requests for update and receipt of information must also be recorded, if received separately from the problem management system.
**Event Management**
Alerts reported by Green Cloud systems and equipment are documented, detected, filtered, logged, and tracked in a centralized database. Each new incoming event is automatically assigned a severity code based on the threshold reached. Those severities are: Debug, Informational, Warning, Error, and Critical.

Each member of the Network Operations team has access to the database and all events with severity of “Warning” or higher will send email notifications to engineers and management.

Events are categorized by class and by various components of the device that is monitored. When a new event comes in to the Event Console, a NOC engineer acknowledges, triages and assesses the event and its current and potential future impact.

Alerts with immediate and known customer impact may subsequently generate Incidents in the Incident Management System or invoke the Outage Response Process. Alerts with limited or no immediate customer service impact and low severity are classified and appropriate correction action taken and tracked in Network Operations Change Log.

- Monitoring system is highly available due to the underlying infrastructure (HA features).
- Environmental data is monitored and recorded for each device where available.
- Monitoring system is currently configured to poll infrastructure devices at 5 minute intervals.
- All event and monitoring data is stored perpetually.

**Major Incidents / Outage Response Process**
Major Incidents, or outages, are defined as system events that have an impact to Green Cloud service for more than one customer. Outages are categorized based on the breadth of the impact as well as the type of services impacted. Customer Operations personnel are to follow the Outage Declaration and Management process and adhere to communication policies set forth therein.

*Identification*
When an outage scenario is discovered, Operations personnel are to immediately notify the impacted customer base via updates to Operational Status web site: [http://status.grncld.net](http://status.grncld.net)

Partners and Customers can subscribe to receive alerts and notifications for Network Events and Network Maintenance.

*Categorization*
A member of Operations Management will be responsible for determining the severity of the issue and initiate the Outage Response Communication Process.

- White - Impacts only a small percentage of total customers and issue is isolated to a single network or equipment failure
- Yellow - Impacts less than 50% of total customer base *OR* issue is isolated to only one service. Unknown amount of downtime, but Network Operations and/or Engineering agree that cause is known.
• Orange - Impacts 50% or more of total customer base *OR* issue is not isolated to one service. Unknown amount of downtime and cause/resolution is not known.
• Red - Impacts 75% or more of total customer base *OR* issue causes customer inability to contact Green Cloud (e.g. email, web and telephone services are down)

Communication Process

Both internal and external updates will be provided at pre-designated time intervals (refer to matrix below), depending on the severity, via approved communication methods only.

<table>
<thead>
<tr>
<th>Customer/Partner Communications</th>
<th>White</th>
<th>Yellow</th>
<th>Orange</th>
<th>Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update status.grncld.net</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Frequency of Updates</td>
<td>n/a</td>
<td>120min</td>
<td>60min</td>
<td>30min</td>
</tr>
<tr>
<td>Proactively send RFO</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Management follow-up</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Disaster Recovery

In the event that the end-user determines it is necessary to initiate a failover, there is no immediate need to contact Green Cloud. The partner/customer will access their specific Zerto Self Service Portal (ZSSP) via credentials provided in the finalization step.

From within the ZSSP, the end-user can specify the options for the type and timing of the failover.

Once the failover begins, the VMs on the customer side will start to shut down and power off, but the data will remain at the customer site. Simultaneously, the VMs will be powering up in the customer VDC at Green Cloud.

It is recommended that the Partner/Customer then access each VM individually via console to verify/modify networking to match the IP networking chosen during VPG setup.

Issues following the failover can be referred to Operations via the Incident Management process (e.g. support@gogreencloud.com and/or 877-465-1217)

Change Requests

Simple
A simple change request is defined as an Add, Change or Disconnect which has no complexity or significant modification to monthly recurring charges. A normal change request can usually be completed within 1 hour of receipt and does not require customer re-design or end-user scheduling.

Simple change requests have an associated one-time $25 non-recurring charge.
Normal
A normal change request is defined as an Add, Change or Disconnect which requires some level of complexity and has either significant modification to monthly recurring charges (+/- 25% MRC) or requires customer re-design or end-user scheduling.

Simple change requests have an associated one-time $150 non-recurring charge.

Complex
A complex change request is defined as an Add, Change or Disconnect which requires pre-approval due to service re-design and will invoke professional services for project management and scheduling. Custom Statements of Work are required for Complex change requests.

Complex change requests have applicable charges outlined and approved via Statement(s) of Work.

Critical Success Factors

1) Reservation of sufficient resources in the Green Cloud infrastructure to support a failover of the entire protected server environment in the event of a disaster
2) Completion of one full test failover, with accessibility and functionality approval from the end-user
3) Customer/Partner ability to access the Zerto Self Service Portal (ZSSP) to initiate a failover independent of Green Cloud Operations

Billing and Costs
Standard product and service costs are outlined in Schedule A of the Partner’s agreement with Green Cloud. Adjustments to pricing must be coordinated through Partner Support and/or the assigned Dealer Manager.

Work deemed out-of-scope may require an associated Professional Service engagement or one-time non-recurring charge for additional labor. Those standard rates are listed below for reference:

<table>
<thead>
<tr>
<th>DRaaS Professional Services</th>
<th>Description</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Change Fee - Simple</td>
<td>(per incident)</td>
<td>$ 25.00</td>
</tr>
<tr>
<td>Service Change Fee - Normal</td>
<td>(per incident)</td>
<td>$ 150.00</td>
</tr>
<tr>
<td>Consultation Time</td>
<td>(per hour)</td>
<td>$ 125.00</td>
</tr>
<tr>
<td>Restore</td>
<td>(per server)</td>
<td>$ 150.00</td>
</tr>
</tbody>
</table>

Monthly recurring charges for services provided are effective upon successful delivery of the Green Cloud infrastructure needed to support a failover of the entire protected server environment (a.k.a. Zerto Cloud Manager) and access to the Zerto Self Service Portal.
Authorization

<<PARTNER/CUSTOMER>>                                Green Cloud Technologies

Signed:                                                Signed:

Title:                                                 

Date Signed:                                           Date Signed:
ServeRestore DRaaS

Service Description

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Service Options (Scope)</td>
<td>2</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>2</td>
</tr>
<tr>
<td>Service Operations</td>
<td>3</td>
</tr>
<tr>
<td>Implementation Plan and Timeline</td>
<td>3</td>
</tr>
<tr>
<td>Service Support</td>
<td>4</td>
</tr>
<tr>
<td>Customer Operations</td>
<td>4</td>
</tr>
<tr>
<td>Network Operations</td>
<td>4</td>
</tr>
<tr>
<td>Availability</td>
<td>4</td>
</tr>
<tr>
<td>Business Hours</td>
<td>4</td>
</tr>
<tr>
<td>On-Call Hours</td>
<td>4</td>
</tr>
<tr>
<td>Incident Categorization &amp; Management</td>
<td>5</td>
</tr>
<tr>
<td>Problem Management</td>
<td>6</td>
</tr>
<tr>
<td>Event Management</td>
<td>6</td>
</tr>
<tr>
<td>Major Incidents / Outage Response Process</td>
<td>7</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>8</td>
</tr>
<tr>
<td>Change Requests</td>
<td>8</td>
</tr>
<tr>
<td>Simple</td>
<td>8</td>
</tr>
<tr>
<td>Normal</td>
<td>8</td>
</tr>
<tr>
<td>Complex</td>
<td>9</td>
</tr>
<tr>
<td>Critical Success Factors</td>
<td>9</td>
</tr>
<tr>
<td>Billing and Costs</td>
<td>9</td>
</tr>
<tr>
<td>Authorization</td>
<td>9</td>
</tr>
</tbody>
</table>
Introduction
ServeRestore DRaaS provides Green Cloud Customers and Partners with both local and off-site server backup with recovery in the cloud. The ServeRestore service is managed remotely by Green Cloud and leverages the use of on-premise network attached storage, a Synology NAS, and synchronization software (StorageCraft). ServeRestore offers a recovery time of approximately four hours or less, per server, depending on the size of the protected environment.

Green Cloud is solely channel focused and will only sell products and services through an authorized partner.

Service Options (Scope)
Unless otherwise stated, only the work and products outlined in the Scope section below are covered under this Service Description. Ancillary products and services can and will be charged separately through additional Proposals, Work Orders, or addendums. The initial Proposal products and/or pricing may need to be adjusted following the discovery or implementation phases, in order to meet Service Level Objectives for the product.

All of Green Cloud’s provisioning and support is to be performed remotely and as such, no on-site access will be necessary. The Partner will need on-site access to physically install the NAS and the Customer or Customers vendor may need to modify local area network settings, including possible firewall changes, to allow for remote access to the NAS and servers.

The primary objective of ServeRestore DRaaS is to provide the end-user with the ability to quickly and fully recover business operations when a disaster occurs impacting the use of their on-premise server(s).

The Service Options for the product are:

- Option of cloud recovery to Greenville, SC or Nashville, TN data center
- Specification of servers to recover (virtual or physical instances) and amount of CPU, RAM, and storage needed to recover fully to the cloud
- RDP, SSL VPN, and/or IPsec site-to-site VPN connectivity to the cloud environment
- Local file restore available (per incident charge)
- Backup Only option available (required for Microsoft Small Business Server operating system and servers licensed under the OEM channel)
- Daily or Weekly status notifications via email to technical points of contact
- Standard customer service and frontline technical support included (Professional Services available)

Prerequisites
- Servers to be recovered in the Cloud are Windows Server versions 2003, 2008, or 2012 (Windows Small Business Server not supported; backup-only options available)
- Servers to be recovered in the Cloud are Volume licensed (if OEM, conversion/upgrade may be required before recovery)
- Customer has at least 1.5Mbps (typical T1) Internet bandwidth to support incremental transfers to the datacenter
- Available gigabit switch port with DHCP on the local area network
- Ability to send email/status messages from local area network to Green Cloud (outbound port 25 open or relay through mail server)
- No conflicting backup software applications installed on server(s) to be recovered
After delivery of the product, it is the end-user’s responsibility to notify Green Cloud in the event of any major server changes that could impact the performance of ServeRestore recovery. The following client-side changes will impact the ability for the protected environment to be recovered at Green Cloud:

- Adding or removing hard disk drives to/from a protected server
- Disconnecting, moving, or powering off a protected server
- Re-configuring CPU, RAM, number or size of hard disks
- Upgrading Operating System
- Networking or Firewall changes that might affect remote access
- ISP changes (public IP addressing) impacting remote access

Service Operations

Implementation Plan and Timeline

Through the Implementation Plan, Green Cloud will manage the initial seeding of the physical servers, provide a fully configured Synology NAS, remotely configure the StorageCraft software on a customer server, and manage the off-site synchronization of incremental server changes to the cloud.

The Partner/Customer responsibilities include providing full and complete documentation regarding the physical server environment prior to NAS configuration and delivery, on-site installation of the NAS, ensuring necessary network and firewall changes provide remote access to Green Cloud, and following written procedural documentation provided by Green Cloud for the purpose of providing the service.

<table>
<thead>
<tr>
<th>Duration</th>
<th>Milestone/Requirement</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sales Order</td>
<td>Partner, Customer, and GC Channel Manager</td>
</tr>
<tr>
<td></td>
<td>Site Survey</td>
<td></td>
</tr>
<tr>
<td>1 day</td>
<td>Request to complete site survey sent to Technical POC and/or Partner</td>
<td>Green Cloud Operations</td>
</tr>
<tr>
<td>1-3 days</td>
<td>NAS Configuration</td>
<td>Green Cloud Operations</td>
</tr>
<tr>
<td>*</td>
<td>NAS and encrypted USB drive Shipped</td>
<td>Green Cloud Operations</td>
</tr>
<tr>
<td>*</td>
<td>On-site NAS installation, remote access provided</td>
<td>Partner and/or Customer</td>
</tr>
<tr>
<td>1-3 days</td>
<td>Seed data obtained and transferred to encrypted USB drive</td>
<td>Green Cloud Operations</td>
</tr>
<tr>
<td>*</td>
<td>Upon completion of seed data transfer, USB drive shipped to Green Cloud</td>
<td>Partner and/or Customer</td>
</tr>
<tr>
<td>1-2 days</td>
<td>Seed data received, transferred. Setup finalization</td>
<td>Green Cloud Operations</td>
</tr>
<tr>
<td>7-14 days</td>
<td>Data sync obtained, Status Notifications configured</td>
<td>Green Cloud Operations</td>
</tr>
<tr>
<td>1-3 days</td>
<td>Mock Restore performed, results provided.</td>
<td>Green Cloud Operations</td>
</tr>
</tbody>
</table>
*some timeline estimates dependent on Partner/Customer scheduling with Operations, on-site access, and communication methods*

NOTE: The timeline outlined above assumes there is no delay in communication between high-level milestones. There are several end-user requirements outlined in the Onboarding Procedure which require sign-off, validation, or on-premise action and may delay Green Cloud from satisfying the requirement within the expected duration.

### Service Support

Green Cloud Operations will address and manage all customer service needs: new customer provisioning, existing customer change requests, customer incidents and customer problems. The Service Operations function is also responsible for management and resolution of system and network related alerts and events.

#### Customer Operations

The Customer Operations role satisfies all customer technical support incidents, customer change requests, and normal and standard new order provisioning.

#### Network Operations

The Network Operations role addresses and resolves customer problems escalated from Customer Operations and also manages the customer network infrastructure. They partner with the Engineering team to insure that all network service level objectives are met.

### Availability

Service Operations management is located at 411 University Ridge, Suite 201 in Greenville, South Carolina. The Service Operations function is accessible to Partners and Customers via two methods: e-mail, and telephone.

- The Service Operations e-mail address is support@gogreencloud.com
- The telephone number for Partners/Customers is 877-465-1217.

#### Business Hours

The Customer Operations group will staff a centralized support desk to handle all requests and order provisioning during defined business hours. These hours are currently defined as Monday through Friday, 8:00am until 6:00pm Eastern time. New customer provisioning and change requests are handled during this time.

#### On-Call Hours

Outside of Business Hours, the Green Cloud Operations group will staff at least one (1) technician to answer incoming telephone calls and respond to email requests for urgent service impacting incidents. NOTE: new customer provisioning and change requests are deferred until start of next business day.

The use of automated on-call paging is leveraged after business hours and weekends to insure 24/7 availability for service impacting Incidents.
Unscheduled normal or standard service changes or unscheduled service provisioning requests are not typically completed outside of business hours, at Operations management’s discretion, unless otherwise arranged through Professional Services or Statement(s) of Work.

**Incident Categorization & Management**

The Operations Manager is responsible for real-time assessment of new, unassigned customer requests and incidents in the incident management system. This team member will prioritize, categorize, assign, and update new incoming requests to be best handled by Customer Operations.

**Ticket Creation**

Customers are to email or phone the Operations group to have a new incident or change request created. System Events generating alerts from monitoring applications are automatically tracked in the ticket management system.

**Ticket Categorization (Type, Status, & Priority)**

**Request Type**
- Event – system generated alert indicating possible impact to customer service
- Incident – record of impact to customer service as reported by customer or monitoring systems
- Problem – an impact to customer service with no currently known resolution
- Question – a general inquiry resulting in no service or account information change
- Customer MACD – request to modify or deliver new products
- Billing – request related to invoicing or payments

**Status**
- Open – issue or request is currently being addressed or awaiting work from an agent.
- Pending – issue requires work from an agent, but later time (or the issue is not service impacting)
- Waiting on Customer – the agent can perform no further work until the Customer responds
- Waiting on Third Party – the agent can perform no further work until the Third Party responds
- Resolved – the incident has been remedied and tested by Green Cloud, but not yet confirmed
- Closed - the incident has been confirmed as resolved and no further action is needed

**Priority**
- Low –
  - Incidents -- No service impact
  - Requests – No required completion date/time
- Medium –
  - Incidents/Problems - Less than 50% service impact
  - Requests - Completion date/time more than 24 hours
- High –
  - Incidents/Problems - More than 50% service impact, but some services working
  - Requests - Completion within next 24 hours
- Urgent –
  - Incidents/Problems - All services down
  - Requests - Immediate requested completion
Service Level Objectives

A designated member of the Operations team will be responsible for real-time assessment of new, unassigned customer requests in the incident management system. This team member will prioritize, categorize, assign, and update new incoming requests to be handled by Customer Operations.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Response SLO</th>
<th>Resolution SLO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgent</td>
<td>15 minutes</td>
<td>1 hour</td>
</tr>
<tr>
<td>High</td>
<td>30 minutes</td>
<td>4 hours</td>
</tr>
<tr>
<td>Medium</td>
<td>1 hour</td>
<td>1 day</td>
</tr>
<tr>
<td>Low</td>
<td>2 hours</td>
<td>2 days</td>
</tr>
</tbody>
</table>

When an SLO target is violated, a notification is immediately delivered to management to prompt action. All service change requests have priority “Medium” by default.

Problem Management

Incidents received by the Customer Operations group which have no known resolution are created as Problem tickets and handed off to the Network Operations group for acknowledgement, categorization, and root cause analysis.

Network Operations will engage external vendors not only for problem reporting, but also to identify and rectify provisioning or networking errors.

- Problems which are customer impacting and require analysis from external vendors will be submitted to the vendor within one (1) hour of receipt
- Problems which require root cause analysis and are not customer impacting will be submitted to the vendor within four (4) hours of receipt
- Problems which require provisioning or networking changes will be submitted to the vendor within twenty-four (24) hours of receipt

The Green Cloud Network Operations engineer must request and obtain a vendor tracking number for the issue and record that tracking number in the related problem management system. Regular requests for update and receipt of information must also be recorded, if received separately from the problem management system.

Event Management

Alerts reported by Green Cloud systems and equipment are documented, detected, filtered, logged, and tracked in a centralized database. Each new incoming event is automatically assigned a severity code based on the threshold reached. Those severities are: Debug, Informational, Warning, Error, and Critical.
Each member of the Network Operations team has access to the database and all events with severity of “Warning” or higher will send email notifications to engineers and management.

Events are categorized by class and by various components of the device that is monitored. When a new event comes in to the Event Console, a NOC engineer acknowledges, triages and assesses the event and its current and potential future impact.

Alerts with immediate and known customer impact may subsequently generate Incidents in the Incident Management System or invoke the Outage Response Process. Alerts with limited or no immediate customer service impact and low severity are classified and appropriate correction action taken and tracked in Network Operations Change Log.

- Monitoring system is highly available due to the underlying infrastructure (HA features).
- Environmental data is monitored and recorded for each device where available.
- Monitoring system is currently configured to poll infrastructure devices at 5 minute intervals.
- All event and monitoring data is stored perpetually.

**Major Incidents / Outage Response Process**

Major Incidents, or outages, are defined as system events that have an impact to Green Cloud service for more than one customer. Outages are categorized based on the breadth of the impact as well as the type of services impacted. Customer Operations personnel are to follow the Outage Declaration and Management process and adhere to communication policies set forth therein.

**Identification**

When an outage scenario is discovered, Operations personnel are to immediately notify the impacted customer base via updates to Operational Status web site: [http://status.grncld.net](http://status.grncld.net)

Partners and Customers can subscribe to receive alerts and notifications for Network Events and Network Maintenance.

**Categorization**

A member of Operations Management will be responsible for determining the severity of the issue and initiate the Outage Response Communication Process.

- White - Impacts only a small percentage of total customers and issue is isolated to a single network or equipment failure
- Yellow - Impacts less than 50% of total customer base *OR* issue is isolated to only one service. Unknown amount of downtime, but Network Operations and/or Engineering agree that cause is known.
- Orange - Impacts 50% or more of total customer base *OR* issue is not isolated to one service. Unknown amount of downtime and cause/resolution is not known.
- Red - Impacts 75% or more of total customer base *OR* issue causes customer inability to contact Green Cloud (e.g. email, web and telephone services are down)

**Communication Process**
Both internal and external updates will be provided at pre-designated time intervals (refer to matrix below), depending on the severity, via approved communication methods only.

<table>
<thead>
<tr>
<th>Customer/Partner Communications</th>
<th>White</th>
<th>Yellow</th>
<th>Orange</th>
<th>Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update status.grnclld.net</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Frequency of Updates</td>
<td>n/a</td>
<td>120min</td>
<td>60min</td>
<td>30min</td>
</tr>
<tr>
<td>Proactively send RFO</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Management follow-up</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

**Disaster Recovery**

In the event that the end-user determines it is necessary to initiate a server recovery, there is an immediate need to contact Green Cloud. The partner/customer will reach Operations Support at 877-465-1217.

Green Cloud Operations will begin the server recovery, based on the priority identified in the Mock Restore summary.

The customer and/or partner will be required to assist in configuring an IPsec site-to-site VPN tunnel, as needed, for remote access to the recovered environment. The customer and/or partner will be required to provide any necessary information that may impact the production of the end-users in the recovered environment (e.g. administrative passwords, operating system license keys, usernames, and local area network changes).

Once the server(s) are recovered to the cloud, remote access will be verified with the customer and/or partner by Green Cloud. At that point, the customer and/or partner have 10 business days to determine if there is a need to “failback” the production environment.

If the production environment remains in the Green Cloud infrastructure, the Green Cloud Channel Manager will present a Proposal of Service to migrate the products from ServeRestore DRaaS to Virtual Server Infrastructure as a Service (IaaS).

Issues following the failover can be referred to Operations via the Incident Management process (e.g. support@gogreencloud.com and/or 877-465-1217)

**Change Requests**

**Simple**

A simple change request is defined as an Add, Change or Disconnect which has no complexity or significant modification to monthly recurring charges. A normal change request can usually be completed within 1 hour of receipt and does not require customer re-design or end-user scheduling.

Simple change requests have an associated one-time $25 non-recurring charge.

**Normal**

A normal change request is defined as an Add, Change or Disconnect which requires some level of complexity and has either significant modification to monthly recurring charges (+/- 25% MRC) or requires customer re-design or end-user scheduling.

Simple change requests have an associated one-time $150 non-recurring charge.
Complex
A complex change request is defined as an Add, Change or Disconnect which requires pre-approval due to service re-design and will invoke professional services for project management and scheduling. Custom Statements of Work are required for Complex change requests.

Complex change requests have applicable charges outlined and approved via Statement(s) of Work.

Critical Success Factors

1) Consistent remote access to the physical NAS device and protected servers on the customer premise
2) Management of synchronization and quick resolution to delays or interruptions in that synchronization
3) Completed mock restore and documented results for quick recovery to cloud

Billing and Costs
Standard product and service costs are outlined in Schedule A of the Partner’s agreement with Green Cloud. Adjustments to pricing must be coordinated through Partner Support and/or the assigned Dealer Manager.

Work deemed out-of-scope may require an associated Professional Service engagement or one-time non-recurring charge for additional labor. Those standard rates are listed below for reference:

<table>
<thead>
<tr>
<th>DRaaS Professional Services</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Change Fee - Simple</td>
<td>(per incident)</td>
<td>$ 25.00</td>
</tr>
<tr>
<td>Service Change Fee - Normal</td>
<td>(per incident)</td>
<td>$ 150.00</td>
</tr>
<tr>
<td>Consultation Time</td>
<td>(per hour)</td>
<td>$ 125.00</td>
</tr>
<tr>
<td>Server Restore (Mock Restore excluded)</td>
<td>(per server)</td>
<td>$ 150.00</td>
</tr>
</tbody>
</table>

Monthly recurring charges for services provided are effective upon successful delivery of the seed data into the Green Cloud virtual environment, as this is prerequisite for a successful recovery from disaster.

Authorization

<<PARTNER/CUSTOMER>>                    Green Cloud Technologies

Signed:                                  Signed:

Title:

Date Signed:                Date Signed:
Green Cloud Technologies Service Level Agreement (SLA) – Virtual Server & Disaster Recovery

Green Cloud guarantees that our network and infrastructure will be available at all times, excluding maintenance periods. The Green Cloud “network” is defined as the data network from the virtual server to the outer most port of the Green Cloud owned routing infrastructure. Green Cloud “infrastructure” is defined as the compute, storage switching and routing equipment owned and maintained by Green Cloud. “Maintenance periods” are defined as periods between 12:00 a.m. (ET) and 6:00 a.m. (ET) wherein pre-planned maintenance may take place.

Green Cloud guarantees that our Virtual Server components, including compute, storage, and software, will function at all times. In the unlikely event that a virtual server should fail, Green Cloud guarantees restoration and/or repair within the time period specified for each SLA subscribed to. SLA time periods begin from the time of problem notification via email or telephone to Green Cloud by customer. If specific SLA guarantees are not subscribed to by the customer and, instead, the customer utilizes Local-only or Backup-only, Green Cloud shall use best efforts to restore non-SLA servers once SLA-guaranteed customers are restored.

“Virtual Server components” are defined as those components that make up the physical machine that houses your virtual server. “Virtual Server” is defined as your unique virtual machine instance.

Our Promise
If Green Cloud fails to uphold the 100% uptime guarantee, Customer will be eligible for a credit, which will be a percentage of the monthly recurring Fees for the services adversely affected by the failure. These credits will be calculated in the following manner:

- 2.5% percent of the monthly recurring fees for the every hour of downtime, after breach of the specific SLA subscribed period per server. SLA credits cover services adversely impacted by the identified issue on a per server basis.

- If the customer is not covered by a specific recovery timeframe, or for the time a customer is down until their SLA recovery time specifies, customer will receive credit equal to the monthly recurring charges divided by 720 hours. So, for example, a server that was inaccessible for 1 hour would get a credit equal to 1 hour on the next bill.

- Credits due will be applied at the end of the billing cycle during which the notification of failure was received.

“Fees” are defined as the monthly fees for your Virtual Server for the monthly billing cycle in which the failure occurs.

Disaster Recovery Restoration Commitment: Any customer of Green Cloud’s Disaster Recovery
solution will operate under the following SLA when Green Cloud is notified to restore the servers: From the time the customer notifies Green Cloud support to request that a server or multiple servers be activated for restart, Green Cloud guarantees that the servers will be restored in accordance with each server’s contracted SLA.

If Green Cloud fails to meet the above guidelines, the customer will be eligible for a credit that will be calculated in the following manner:

- 2.5% percent of the monthly recurring fees for the every hour of downtime, after breach of the specific SLA subscribed period per server. SLA credits cover services adversely impacted by the identified issue on a per server basis.
- Credits due will be applied at the end of the billing cycle during which the notification of failure was received.
- There are no credits unless a server is subscribed to a specific SLA.

“Fees” are defined as the monthly recurring fees for your Disaster Recovery solution for the monthly billing cycle in which the failure occurs.

Limitations
You are not entitled to any credits if your account is delinquent or in breach in any way. If failure occurred as a result of your breach, misuse, or other action on your part, you are not entitled to any credits as SLA’s have not been breached.

The parties’ performance under this agreement, in whole or in part, is subject to acts of God, war, government regulation, terrorism, disaster, strikes, civil disorder, curtailment of transportation facilities, or similar emergency beyond the parties’ control, making it impossible, illegal, or commercially inadvisable, or which materially affects a party’s ability to perform its obligations under this agreement in whole or in part.

To be eligible to receive a credit, you must contact Green Cloud within thirty (30) days of the specified failure and show that your use of the Green Cloud Virtual Server was negatively impacted as a result of the downtime.

This Service Level Guarantee is your sole and exclusive remedy for any Green Cloud failure as defined above. Notwithstanding anything in this Service Level Agreement to the contrary, the maximum total credit for the monthly billing period, including all guaranties, shall not exceed 100% of your monthly fee for that billing period. Credits that would be available but for this limitation will not be carried forward to future billing periods.

This Service Level Agreement is part of your agreement with Green Cloud Technologies, along with our Terms and Conditions and AUP, located at http://gogreencloud.com/policies, and is subject to the terms and conditions stated in those documents.