May 2016

Service Descriptions

Infrastructure as a Service

Infrastructure as a Service (IaaS) provides Green Cloud Customers and Partners with a public or private multi-tenant architecture including shared or dedicated storage, CPU, memory, and operating system licensing. The primary objective of IaaS is to provide the end-user with a virtual server environment capable of supporting their production services. There are currently three delivery mechanisms for IaaS environments: Virtual Server, Bulk Resources, or Private Cloud.

IaaS Service Options

Virtual Servers and Bulk Resources are provisioned in a shared environment, while Private Cloud resources (compute and/or storage) can be provisioned in a dedicated environment.

Virtual Server

The IaaS Virtual Server provisioning option includes the provisioning of individual servers by Green Cloud based on the OS, vCPU, vRAM, and storage profile requested. Provisioning includes the creation of a VMware Organization, Virtual Datacenter with allocated resources, vApp based on the OS template, and finally, the individual Virtual Server.

Bulk Resources

The IaaS Bulk Resourcing provisioning option includes the provisioning of a Virtual Datacenter by Green Cloud and allocation of the resources selected, based on the vCPU, vRAM, storage quantities, and storage profiles requested. Provisioning includes the creation of a VMware Organization, Virtual Datacenter with allocated resources, and creation of a vCloud Director Organization administrator account.

The Service Options for these products are:

- Choice of server operating system
  - Windows 2008[R2]
  - Windows 2012[R2]
  - Linux [CentOS, Ubuntu]
- Specified number of virtual CPUs (vCPUs) per Virtual Server
  - From 1 to 8 vCPU
  - vCPU speed is 2GHz
- Specified amount of memory (GB of RAM) per Virtual Server
  - up to 64GB
- Choice of storage performance profiles per Virtual Server
  - up to 16TB per disk
  - “Premium” for SSD-like performance,
  - “Standard” for SAS-like performance, or
  - “Archive” for SATA-like performance
- Choice of data recovery options:
  - “Local” for 24 hour RPO and best effort RTO
  - “24hr” for 24 hour RPO and 24 hour RTO
  - “6hr” for 6 hour RPO and 6 hour RTO
- Choice of additional data backup:
  - None
  - “Standard” for single repository
  - “Replicated” for dual repositories
- Choice of Data Center location (Greenville, SC or Nashville, TN)

- Professional Services available for managed import of data, migration of physical servers (P2V conversions), and/or migration of virtual server images. See “Professional Services Description” for more details.

Included with all IaaS Virtual Server and Bulk Resource services are:

- Daily snapshot management, with up to seven (7) days retention
- Microsoft Windows Server OS licensing
- Standard customer service and technical support

Required Green Cloud services for each IaaS Virtual Server and Bulk Resources environment are:

- Choice of Network & Security Bundle for each virtual data center (VDC), or logically separated end-user environment. See “Network and Security Description” for more details
- Licenses for any installed Microsoft applications (e.g. Remote Desktop, MS Office suite, MS SQL)

IaaS Storage Profiles

Premium
The premium storage profile has high input/output (I/O) availability for large volume transactional servers. Low latency, high throughput Flash-like performance provides at least 1,000 I/O operations per second (IOPS) at less than five (5) milliseconds latency, assuming 4k block size. Encryption at rest is provided with this storage profile. Example uses: SQL database servers, MS Exchange servers, or servers containing electronic protected health information (ePHI). Green Cloud currently leverages Tintri VMStore T6xx and T8xx series (https://www.tintri.com/products/tintri-vmstore) for Premium level storage.

Standard
The standard storage profile has an equivalent I/O performance level of a typical small business sized, premise-based server. Average latency, average throughput SAS-like performance provides at least 250 IOPS at less than twenty (20) milliseconds latency. Example uses: web servers, application servers, file servers, terminal servers. Green Cloud currently leverages Tintri VMstore T6xx and T8xx series (https://www.tintri.com/products/tintri-vmstore) for Standard level storage.

Archive
The archive storage profile has low I/O performance specifically for data that is not frequently accessed. There is no guaranteed I/O for archival storage. High latency and low throughput provides SATA-like performance. Example uses: archive file server, document management systems, old/inactive EMR systems. Green Cloud leverages NetApp E-Series with SATA drives (http://www.netapp.com/us/products/storage-systems/e5400/index.aspx) for Archive level storage.

Storage Type	I/O Guarantee	Latency	Throughput
Premium	1,000 IOPS	<5 ms	High
Standard	250 IOPS	<20 ms	Average
Archive	None	High	Low

Snapshots vs Backups vs Replication

Snapshots are not the same as backups and shouldn't be used in the same way for Disaster Recovery planning.

Here's why:

A **snapshot** is a point-in-time 'picture' of the state of a virtual machine's disk(s) at the instant the snapshot is taken. Snapshots are also usually saved on the same media as the VM, to save I/O when a recovery is needed. Snapshots are not overwritten in the "grandfather-father-son" schema; they live 'side-by-side' until deleted. It is also not optional to retrieve individual files from a snapshot (the entire disk must be mounted and made available; see the 3 data recovery options for snapshots below).

Snapshots are ideal for recovery to the last known good - and recent - VM configuration in case of VM failure.

A **backup** is a full copy of the virtual machine's data and applications, taken while the VM is in a prepared state and is usually saved to separate media (i.e. to a different SAN or a redundant data center). Backup jobs are typically configured to consolidate the files periodically based on the "grandfather-father-son" schema (or similar). For example, daily backups might be consolidated every 8th day to be replaced by a weekly version. The weekly backups might be consolidated after five weeks, as this is when monthly version created; and the monthly copies are replaced by an annual backup, and so on.

Backups are ideal for retrieval of historical data and files in case of audit or data loss; and while possible, backups are not intended for full VM recovery in case of failure.

Replication is the practice of copying live data from one location to another to maintain a mirrored version of the machine on separate media. Replication is ideal for machines and applications that have very high availability requirements but low retention needs.

IaaS Backup and Recovery Options

"Local"
A snapshot of the virtual server image will be created and saved automatically once every twenty-four (24) hours to the same, local Storage Area Network (SAN). Each individual daily snapshot is archived by default for seven (7) calendar days on the same storage platform on which the virtual server resides. Default option also known as "Local Only."

"Standard"
A crash consistent, or optionally an application consistent, backup job is managed by Green Cloud on a per-vApp basis. The backup repository (sized in 500GB increments) can be located in the same data center in which the virtual server resides, or can be provisioned in a geographically disparate data center. NOTE: if Standard backup is chosen to reside in the disparate data center, some options are no longer available.

- RPO - "Configurable" refers to the fact that the partner and/or end-user chooses the Backup & Replication schedule.
- Retention - "Unlimited" refers to the fact that Green Cloud provides repository space only, in 500GB increments. The partner and/or end-user can purchase as much space as needed to accommodate their unlimited ability to retain backups based on their need. Green Cloud will grow the repository when reports indicate that backup jobs need the space to successfully be saved. (* reference SLA)

"Replicated"
A crash consistent or optionally application consistent backup job is managed by Green Cloud on a per-vApp basis. The backup repository (sized in 500GB increments) can be located in the same data center in which the virtual server resides, and will also be copied (or optionally consolidated and archived) to a geographically disparate data center.

- RPO - "Configurable" refers to the fact that the partner and/or end-user manages the Backup & Replication jobs and schedule
- Retention - "Unlimited" refers to the fact that Green Cloud provides repository space only in 500GB increments. The partner and/or end-user can purchase as much space as needed to accommodate their

unlimited ability to retain backups based on their need. Green Cloud will grow the repository when reports indicate that backup jobs need the space to successfully be saved.

IaaS Backup & Recovery Feature Summary

Type	Service Option	RPO	Retention Period	RTO	Recovery Method	Location	File Level Restore
Snapshot	**Local** (default)	24 Hours	7 Days	None	Prof Svcs	Local SAN	No
	24 Hour	24 Hours	7 Days	24 Hours	Prof Svcs	Local & Offsite SAN	No
	6 Hour	6 Hours	7 Days	6 Hours	Prof Svcs	Local & Offsite SAN	No
Backup	**Standard**	Configurable	Unlimited	Varies	Self Service	Single Data Center	Yes
	Replicated	Configurable	Unlimited	Varies	Self Service	Dual Data Centers	Yes
Replication	***Express*Restore**	< 15 min	7 Days	< 1 Hour	Self Service	Second Data Center	No

IaaS Implementation Plan and Timeline

Green Cloud will manage the initial creation of the virtual data center, configure the virtual appliances and initial networking upon receipt of an executed Proposal of Service. Secure RDP and HTTPS access via vCloud Director and specific customer credentials will also be provided upon provisioning completion.

The Partner/Customer responsibilities include providing full and complete documentation regarding the VPN configuration and following any written procedural documentation provided by Green Cloud.

Duration	Milestone/Requirement	Responsibility
	Sales Order Site Survey	Partner, Customer, and Green Cloud Channel
1-3 days	IaaS Setup and basic network configuration	Green Cloud Operations
1-2 days*	Site-to-Site or SSL VPN configuration (as needed)	Partner, Customer, and Green Cloud Channel

**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.

Sales Order

Responsibility: Partner, Customer, and Green Cloud Channel Manager
Estimated Timeframe: n/a

1. IaaS Proposal created and delivered to Partner/end-customer via DocuSign
    a. Proposal includes Infrastructure as a Service product, specifying "Bulk Resources" or "Virtual Servers," depending on provisioning and server management requirements. The order will specify a preferred data center location, if any, and the number of VMs, vCPUs, gigabytes of RAM, storage profile type and volume of storage, and any application licensing required to support the end-users' applications.

        NOTE: Selection of a Networking and Security Bundle is required for new customers/locations (when provisioned as a new VDC within the Customer/Partner vCloud Organization, requiring logically separate networking)

        NOTE: Any and all server and data migrations require that additional product(s) are added to the IaaS Proposal. Process and Procedure documentation available in Professional Services description.

    b. If it is known at the time of the Proposal that Professional Services are needed to support the IaaS environment post-installation or post-migration; or if the scope of the engagement is to exceed the process outlined below, then a Statement of Work (SOW) is to be generated and executed along with the Customer Proposal
2. The executed Customer Proposal (agreement) is received via DocuSign. NOTE: Provisioning cannot begin until the fully executed agreement is in-hand at Green Cloud.
3. IaaS Proposal marked Sold and Work Order is generated. The Work Order is assigned by the Operations manager to an Operations technician (estimated timeframe: 1 business day).

IaaS Environment Setup and Customer Preparation

Responsibility: Green Cloud Operations
Estimated timeframe: 1-2 business days

1. Provision new VMware Organization, Virtual Datacenter (VDC), and Organization Network in the destination vCloud Director site.
2. Ensure that the VDC resources are sufficient to run all of the replicated VMs during a failover.
    a. If resources are not sufficient, Partner/Customer and Green Cloud Channel Manager are engaged to adjust the Work Order and be notified of pricing change.
3. Provision the virtual networking appliance, based on selected Network & Security Bundle
    a. "Standard Routing w/ Advanced Firewall" is delivered via Cisco ASAv appliance
    b. "Standard Firewall w/ Advanced Routing" is delivered via Cisco CSR-SEC appliance
    c. "Premium" is delivered via Cisco CSR-IPB and ASAv appliances.

Basic Networking & Security Setup

Responsibility: Green Cloud Operations
Estimated Timeframe: Concurrent with IaaS Setup (1-2 business days)

1. Deliver to the Customer/Partner a VPN Connection Settings document to capture far-end (peer) information for any IPsec VPN tunnels ordered
    a. Upon receipt of the site survey, information is transferred into the Work Order.
    b. Configure the site-to-site VPN tunnel Cisco ASAv/CSR, depending on selected Networking & Security option. Create necessary firewall rules to allow traffic to pass to/from the VPN subnets.
2. Provision virtual appliance with default, initial routing and firewall configuration
    a. Setup and test outbound Internet connectivity
    b. Setup and test inbound access via RDP or SSH
        i. RDP and SSH traffic will be configured using Network Address Translation (NAT) and a randomly selected "high" port number in an effort to prevent unauthorized access
    c. Setup and test VPN connectivity (provided far-end peer is configured and responding)
3. Additional networking and security support is available for more complex routing and firewall configuration needs; refer to Professional Services product description for more details on Managed Router/Firewall support.

Order Finalization

1. Green Cloud will send notification of "Order Completion" via secure email, including the Partner/Customer's specific access credentials
    a. Custom vCloud Director portal access (one "admin" user)
    b. Custom SSL VPN web site URL for VPN desktop client download (if ordered)
    c. VDC resources provisioned (total resources allocated may exceed those available to virtual servers, based on number and type of virtual appliances ordered through Networking and Security options)

Service Operations

After delivery of the product, it is the end-user's responsibility to notify Green Cloud in the event of any major changes that could impact the performance of the IaaS environment. The following client-side changes will impact the ability for the environment to be accessible:

- Change of ISP or local area networking (which could impact site-to-site connectivity or firewall rules)
- Modification to firewall rules disallowing public or private access

Events, Incidents, and Problems will be addressed by Green Cloud per the Incident Resolution process as outlined in the Services Agreement.

IaaS 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 or support@gogreencloud.com.

If the customer is subscribed to IaaS Backup (Standard or Replicated), server and file restoration can be completed via the self-service web portal.

Otherwise, the Restore Point Objective (RPO) and Restore Time Objective (RTO) for server recovery are based on the Storage Profile selected and provisioned for the given virtual machine. (Refer to “Storage Profiles” above for more details).

Additionally, and by default, Green Cloud will retain up to seven (7) days of daily "snapshots" from which a server can be restored. There are three virtual server restore options that we can provide, each of which carries a $100 per VM per instance professional service fee (when requested by a customer/partner and not the result of a Green Cloud business continuity interruption):

- Option 1: replace the existing VM with a recent working version
- Option 2: mount a restored VM as a virtual hard drive within the existing VM
- Option 3: "spin up" a restored VM in the same virtual data center as the existing VM (aka "side-by-side")

Each of the above options occur in the same physical data center as where the existing VM resides.

IaaS Professional Service Fees

IaaS Professional Services		
Service Change Fee - Simple		$ 25.00
Service Change Fee - Normal		$ 150.00
Consultation Time	*(per hour)*	$ 125.00
Migration/Implementation - Simple	*(per Virtual Server)*	$ 150.00
Migration/Implementation - Advanced	*(per Virtual Server)*	$ 300.00
Server Restore	*(per Virtual Server)*	$ 100.00
Server Export	*(per Virtual Server)*	$ 175.00
Data Import	*up to 1TB*	$ 175.00
	Add'l 5TB increments	$ 100.00

Private Cloud

Private Cloud is intended to provide Green Cloud Customers and Partners with a single-tenant architecture with dedicated or shared storage, dedicated computer (CPU and memory) and private network bandwidth and connectivity options. In this environment, the end-user maintains full control so that resources can be reallocated on demand while maintaining speed, performance, and availability in the Green Cloud infrastructure.

Private Cloud Service Options

The primary objective of Private Cloud is to provide the end-user with dedicated virtual server resources and the ability to manage a customized cloud infrastructure.

The Service Options for the product are:

- Choice of host resources, in the following configurations:
    - 2 Sockets, 16 Cores, 192GB Memory
    - 2 Sockets, 16 Cores, 384GB Memory
    - 4 Sockets, 32 Cores, 1000GB Memory
    - 4 Sockets, 48 Cores, 192GB Memory
- Choice of dedicated or shared storage
- Option for dedicated networking
- Licensing for hosts (one required):
    - VMware Enterprise (vCenter), and/or
    - Microsoft OS (Windows Server Data Center)
- Professional Services available for environment management

Included with all Private Cloud services are:

- Infrastructure management (to Hypervisor; additional management available via Professional Services)
- Firmware and patch management of Green Cloud provided hardware and software
- Default networking & security delivered via Cisco ASAv (unless customer provided)
- Standard customer service and frontline technical support

Required Networking & Security services for each Private Cloud environment are (pre-configured bundles do not apply):

- For Colocated equipment:
    - Rack Unit(s) & Power
    - Cross Connect(s)
    - Public & Private Interconnect Port(s)
    - IP addresses (as needed)
- For virtual networking appliances:
    - Public Internet Port
    - Customer or Green Cloud provided licensing
    - IP addresses (as needed)
- For multi-site and/or replication [*Express*Restore] installations:
    - Inter-city bandwidth
    - Additional cross connects, ports at additional site(s)
    - IP addresses (as needed)
- For customer provided bandwidth:
    - Cross Connect(s)
    - Private Interconnect Port(s)

- Rack Unit(s) & Power to accommodate CPE (as needed)
- IP addresses (as needed)

Service Operations

Events, Incidents, and Problems will be addressed by Green Cloud per the Incident Resolution process as outlined in the Services Agreement.

Private Cloud Implementation Plan and Timeline

Green Cloud will install dedicated equipment and provision hosts as ordered. Additionally, Green Cloud will install and activate Windows or VMware software/applications as requested by the Customer and/or Partner. Green Cloud may also install dedicated networking and security equipment (per the Networking and Security product options selected in the Work Order).

NOTE: Delivery timelines for Private Cloud are heavily dependent on vendor delivery timeframes for hardware.

The Partner/Customer responsibilities for Private Cloud include management of the software applications and networking infrastructure once provisioned, and following written procedural documentation provided by Green Cloud.

Duration	Milestone/Requirement	Responsibility
	Sales Order Private Cloud Design Review – Draft	Partner, Customer, GC Channel Manager and GC Cloud Services
2-5 days	Statement of Work – Draft	GC Cloud Services
2-5 days	Engineering review/approval of Design and Statement of Work	GC Engineering
*	SOW Approval	Partner / Customer
1-3 days	Equipment Ordered	GC Engineering
*	Equipment Delivery	Equipment Vendor
5-10 days	Equipment Installation Network, Application, and Hardware Configuration	Green Cloud Operations
1-2 days*	Finalization, Verification of Remote Access	Partner / Customer and Green Cloud Operations

**some timeline estimates dependent on Partner/Customer scheduling, underlying contracts with equipment vendors, and availability of dedicated hardware resources*

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.

Private Cloud Professional Service Fees

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:

Professional Services Rate Schedule		
Consultation Time	(per hour)	$125.00
Data Import	up to 1TB	$175.00
	5TB increments	$100.00
Managed Router/Firewall	(per router)	$100.00
Service Change Fee - Normal		$150.00
Service Change Fee - Simple		$25.00
Smart Hands	(per incident)	$50.00

ServeRestore Disaster Recovery as a Service (DRaaS)

ServeRestore DRaaS provides Green Cloud Customers and Partners with managed disaster recovery for Windows servers from the premise to the cloud.

The ServeRestore service is installed and managed by Green Cloud and leverages the use of an on premise network attached storage device (typically a Synology NAS) with backup and synchronization software (StorageCraft).

By synchronizing the servers' latest backup images to Green Cloud's infrastructure, ServeRestore offers a server recovery time of as little as four hours, depending on the size of the protected environment.

ServeRestore Service Options

The primary objective of ServeRestore DRaaS is to provide the customer with the ability to fully recover a server in the event of a disaster without having to manage a complicated backup process.

The Service Options for the product are:

- For each protected server, the
  - Amount of CPUs,
  - Amount of memory (GB of RAM), and
  - Amount of used disk space (GB).
- Choice of recovery to Greenville, SC or Nashville, TN data center.

Included with all ServeRestore services are:

- Synchronization management between premise and cloud
- RDP, SSL VPN, and/or IPsec site-to-site VPN connectivity to the cloud environment
- Daily or Weekly synchronization and disk space status notifications via email
- Standard customer service and technical support included

ServeRestore Service Limitations

- Servers to be recovered in the Cloud must be Windows Server versions 2003, 2008, or 2012 (Windows Small Business Server not supported)
- Servers to be recovered in the Cloud should be volume licensed (if OEM, conversion/upgrade may be required before recovery)
- Customer has at least 1.5Mbps (typical T1) Internet bandwidth to support synchronization 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)
- Conflicting backup software applications must be uninstalled

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, or the 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
- Uninstallation or disabling of the synchronization software

Events, Incidents, and Problems will be addressed by Green Cloud per the Incident Resolution process as outlined in the Services Agreement.

ServeRestore 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 continually 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.

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

**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 process which require sign-off, validation, or on premise action and may delay Green Cloud from satisfying the requirement within the expected duration.

Sales Order

Responsibility: Partner, Customer, and Green Cloud Channel Manager
Estimated Timeframe: n/a

4. DRaaS Proposal created and delivered to Partner/end-customer via DocuSign
    a. Proposal includes ServeRestore product, specifying the number of protected virtual servers and their specifications: vCPUs, gigabytes of RAM, and storage profile type and quantity.
    b. Backup Only option available (required for Microsoft Small Business Server operating system and servers licensed under the OEM channel)
    c. If it is known at the time of the Proposal that Professional Services are needed, or the scope of the engagement is to exceed the below process, then a Statement of Work (SOW) is to be generated and executed along with the Customer Proposal
5. The executed Customer Proposal (agreement) is received via DocuSign. NOTE: Provisioning cannot begin until the fully executed agreement is in-hand at Green Cloud.
6. DRaaS Proposal marked Sold and Work Order is generated. The Work Order is assigned by the Customer Operations manager to a Customer Operations technician (1 business day)

Site Survey

Responsibility: Partner and/or Customer
Estimated Timeframe: 1 week (requested)

Green Cloud to deliver to the partner/end-user the ServeRestore Site Survey document to obtain necessary configuration information. **The process cannot continue until this document is completed in full and returned to the Operations group.**

NAS Configuration

Responsibility: Green Cloud Operations
Estimated Timeframe: 1-3 business days

1. Upon receipt of the completed Site Survey, the Green Cloud technician will compare the protected servers' specifications to the Work Order. If there are any discrepancies, the order may be stopped until clarification is received. In some cases, resources may be changed on the Work Order which in turn will modify billable charges, but by no more than +/-25%.
2. The partner and dealer manager will be notified that the work order cannot be completed when protected servers are:
    a. Currently licensed under the OEM channel with Windows Server 2003 or earlier, or
    b. Running Windows Small Business Server of any version, or
    c. Virtual servers running within a physical host and not listed individually on the Work Order, or are
    d. Not Windows servers (i.e. UNIX/Linux machines not supported).
3. Based on the consumed disk space amounts, the NAS will be configured with appropriately sized hard disk drives. The NAS' operating system will be installed, configured and optimized to receive incremental backups from the local servers once on premise.

4. Green Cloud technician will configure the cloud environment to receive the incremental files relayed by the NAS
5. Green Cloud will ship the NAS and an encrypted USB drive to the address specified in the Site Survey. If no specific address is entered, the shipment will default to the service address on the Work Order.

NAS Installation

Responsibility: Partner or Customer
Timeframe: 1 week (requested)

1. Upon receipt of the NAS, the customer and/or partner are asked to follow the installation instructions provided in PDF format via email:
    1) Plug the included AC adapter into a power outlet and the back of the Synology.
    2) Plug the provided Ethernet cable into the RJ45 port on the back of the Synology and into the selected RJ45 Ethernet port on the local LAN switch.
    3) Connect the encrypted USB drive to the Synology using both prongs of the provided Y-cable and unlock the drive by entering the provided code and pressing the unlock button in the bottom left.
    4) Press the blue power button on the face of the Synology.
2. Once the NAS is installed and powered on, the customer and/or partner are asked to contact Green Cloud.
3. Green Cloud will verify remote access to the NAS and at least one server on which to install ImageManager software for replication job management.

Seed Data

Responsibility: Green Cloud Operations
Timeframe: 1-3 business days

1. Green Cloud will remotely install ImageManager software for replication job management. To complete the installation, a reboot of the server must be completed.
2. Green Cloud will request that the server be rebooted at the earliest convenience to the customer and/or partner.
3. When the installation is complete, and initial backups are running, the customer and/or partner will be notified.
4. Typically on the next business day, Green Cloud will verify that the incremental backups are being received in the cloud and start the full backup of the server(s) to the encrypted USB drive which is connected to the NAS.
5. When backups are complete, the partner and/or customer are requested to disconnect the USB drive, enclose it in the provided packaging, and return to Green Cloud using the provided pre-paid shipping label.

Setup Finalization

Responsibility: Green Cloud Operations
Estimated Timeframe: 1-2 business days

1. Upon receipt of the seed data via the encrypted USB drive, Green Cloud will upload into a secure, segregated customer environment.
2. Green Cloud will configure the retention, verification, and consolidation settings to maintain the synchronized data from the on premise customer NAS.
3. The technical contact(s) will be added to weekly status notifications as to the overall health of the synchronization process. Upon request, status notifications can also be sent daily.
4. The work order is considered complete, and an email correspondence will be sent to partner and/or customer indicating that work is complete.

Mock Restore Summary

Responsibility: Green Cloud Operations
Timeframe: 7-30 business days

1. Within 30 days of reaching stable synchronization, a Green Cloud Operations technician will be assigned to perform a mock restore of the protected servers.
2. By default, the servers will be spun up using the image(s) retained in the cloud into an isolated environment. (Isolation is required to prevent network and application conflicts, as the servers restored during testing will be duplicates of production servers. It is possible to perform a full test restore to a production network and virtual datacenter environment with a Professional Services engagement).
3. Green Cloud will provide to the partner and/or customer a written summary of the results of the mock restore test. These results will include recommendations for how to handle restoration of servers with particular operating systems, applications, databases, or timing requirements.
4. The Partner can also request a Business Continuity Plan template be provided, with Mock Restore Summary details included, to further the disaster recovery conversation with the customer beyond the server environment.

Service Operations

Events, Incidents, and Problems will be addressed by Green Cloud per the Incident Resolution process as outlined in the Services Agreement.

ServeRestore Disaster Recovery Process

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 (MRS). The Restore Time Objective (RTO) is 4 hours per average sized server, and any customer specific RTO will be identified and recorded per server in the Mock Restore Summary.

The Restore Point Objective (RPO) for each server will be based on the scheduling of replication jobs and the quality of the customers' offsite replication of the local backup jobs to the Green Cloud environment, but is by commitment 24 hours. This should be discussed at the time of provisioning to insure that there is not a misconception regarding RPO.

If the NAS is not lost in the disaster and the sync is not current, the partner/customer has the option to physically deliver to Green Cloud the NAS and/or incremental files to obtain a more recent restore point.

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 return to the production environment.

For those customers that do not wish to recover to the cloud, or their server environment (e.g. licensing constraints) prevents recovery to a virtual infrastructure, they may choose "Backup Only."

The Backup Only option carries with it no Restore Time Objective and should be discussed at the time of provisioning to insure there is not a misconception on the service level.

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

If the production environment is to be returned to a physical infrastructure, the server image(s) can be provided on encrypted, removable media or made available for download. The Partner and/or Customer is then responsible for restoration from those images.

ServeRestore Professional Service Fees

DRaaS Professional Services		
Service Change Fee - Simple	*(per incident)*	$ 25.00
Service Change Fee - Normal	*(per incident)*	$ 150.00
Consultation Time	*(per hour)*	$ 125.00
Server Restore (Mock Restore excluded)	*(per server)*	$ 150.00

_Express_Restore DRaaS

_Express_Restore 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.

_Express_Restore Service Options

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:

- Specified number of protected VMs
- Specified number of virtual CPUs (vCPUs) per protected group
- Specified amount of memory (GB of RAM) per protected group
- Choice of storage performance profiles:
  - "Premium" for SSD-like performance,
  - "Standard" for SAS-like performance, or
  - "Archive" for SATA-like performance
- Choice of Data Center location (Greenville, SC or Nashville, TN)

Included with all _Express_Restore services are:

- Initial test failover with Green Cloud assistance
- 10 Mb/s replication bandwidth over public Internet or IPsec VPN included (Higher bandwidth speeds and MPLS interconnections are available, through additional products/services)
- 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)

Required for all _Express_Restore services are:

_Express_Restore Service Limitations

- 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

*Express*Restore 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.

Duration	Milestone/Requirement	Responsibility
	Sales Order Site Survey	Partner, Customer, and Green Cloud Channel
1-3 days	IaaS Environment Setup and Customer Preparation	Green Cloud Operations
1-2 days	Zerto Cloud Manager (ZCM) Setup	Green Cloud Operations
1 day	Configure Zerto Cloud Connector (ZCC)	Green Cloud Operations
2-5 days	Initial Customer Site Configuration	Green Cloud Operations and Customer/Partner
3-30 days*	Seeding via NAS (if applicable)	Green Cloud Operations and Customer/Partner
1-2 days	Customer Site Finalization	Green Cloud Operations
1-3 days	Virtual Protection Group (VPG) Setup	Green Cloud Operations
	Delta Sync	
2 days*	Finalization, ZSSP Access, Failover Test	Green Cloud Operations and Customer/Partner

**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.

Sales Order
Responsibility: Partner, Customer, and Green Cloud Channel Manager
Estimated Timeframe: n/a

1. DRaaS Proposal created and delivered to Partner/end-customer via DocuSign
    a. Proposal includes ExpressRestore product, specifying type "Zerto" with required amount of VMs, vCPUs, gigabytes of RAM, and storage profile type and quantity.
    b. **If it is known at the time of the Proposal that the site-to-site bandwidth is not sufficient to seed the VMs "over-the-wire," then a one-time charge for seeding via network attached storage (NAS) device is added. NOTE: This charge may be added as a delivery requirement following site discovery.
    c. If it is known at the time of the Proposal that Professional Services are needed, or the scope of the engagement is to exceed the below process, then a Statement of Work (SOW) is to be generated and executed along with the Customer Proposal
2. The executed Customer Proposal (agreement) is received via DocuSign. NOTE: Provisioning cannot begin until the fully executed agreement is in-hand at Green Cloud.
3. DRaaS Proposal marked Sold and Work Order is generated. The Work Order is assigned by the Network Operations manager to a Network Operations engineer **(1 business day)**

IaaS Environment Setup and Customer Preparation
Responsibility: Green Cloud Operations
Estimated Timeframe: 1-3 business days

1. Deliver to the partner/end-user the ExpressRestore Site Survey and VPN Configuration sheet to obtain necessary configuration information. The process cannot continue until both documents are returned. The Green Cloud vCenter administrator account in the customer's environment will be created by the customer during this step as well.
2. Provision new Organization, Virtual Datacenter (VDC), Edge Gateway, and Organization Network in the destination vCloud Director site.
3. Ensure that the VDC resources are sufficient to run all of the replicated VMs during a failover.
    a. If resources are not sufficient, Partner/Customer and Green Cloud Channel Manager are engaged to adjust the Work Order and be notified of pricing change.
4. Configure the site-to-site VPN tunnel on the Edge Gateway or Cisco ASAv/CSR, depending on selected Networking & Security option. Create necessary firewall rules to allow traffic to pass to/from the VPN subnets.

Zerto Cloud Manager (ZCM) Setup
Responsibility: Green Cloud Operations
Estimated Timeframe: 1-2 business days

1. Upon receipt of the site survey, information is transferred into the Work Order. Provisioning may begin.
2. From Zerto Cloud Manager (ZCM), add a new ZORG.
    a. The name will be "siteid-Company/SiteName" (e.g. "10000000001-GreenCloud/Corporate").

   b. The CRM ID will be the partner or customer Enterprise/Account ID, which correlates to the invoice.
   c. Under the login credentials, the username will be the Site/Location ID. Save a passphrase in the appropriate encrypted database.
3. Add the site's/customer's VDC to the "vCD Cloud Resources" tab and configure resources to match Work Order (VMs, storage quantity and profile).
4. Create the "Preseed folder" in the destination VMware datastore using the name specified in the "Manage ZORG" tab of the Zerto Cloud Manager interface. Then create subfolders for each VM to be migrated.

Configure Zerto Cloud Connector (ZCC)
Resopnsibiilty: Green Cloud Operations
Estimated Timeframe: 1 business day

In the ZCM interface, under the "Customer Sites" tab for the ZORG, deploy a Zerto Cloud Connector (ZCC) for the destination vCloud Org Network.

   a. There must be one ZCC created for each customer vCenter/ZVM that is being protected.

Initial Customer Site Configuration
Responsibility: Green Cloud Operations and Customer/Partner
Estimated Timeframe: 2-5 business days

1. Import a new server template into the customer's VDC for the management VM that will be used by Green Cloud. (Specs are 2Ghz, 4GB RAM, and 44GB storage and must be added to ordered quantity of VDC resources; no pricing adjustment)
2. Ensure that the Customer can connect their local network to the destination vCloud Org Network over a VPN connection to the Edge Gateway. Pinging an IP on their network from the management VM is a good test, as is having the customer ping the ZCC's IP (on the Org VDC network) from their network.
3. If the site survey indicates that any of the VMs to be protected are thick provisioned and data will be seeded using the NAS (as opposed to seeding over the wire using the customer's Internet connection), then it is important to emphasize the importance of specific procedure for the clone operation.
4. Determine if seeding will be done over the wire or via NAS. If over the wire is chosen, skip to next section.
5. Validate bandwidth**
   a. If the site survey indicates that they have <10 Mbps for a "moderate" number of VMs, login to the management VM and run script to gather the write change rate info on the VMs to be protected. The script will output data to be interpreted through the Zerto WAN sizing calculator
   b. If their VDC bandwidth ordered is not sufficient, Partner/Customer and Green Cloud Channel Manager are engaged to adjust the Work Order and be notified of pricing change.

Seeding via NAS
(3-30 business days*)

1. Send the customer an ExpressRestore seed NAS with return labels and such along with the "Schedule Installation" email, which includes the physical installation instructions and the seeding steps that should be taken by the customer.
2. The customer will then mount up the NFS datastore in their environment using the provided instructions.

3. Once all the clones are complete and the NAS is un-mounted as a datastore, the customer should then contact Green Cloud Operations. At this point, the NAS is to be gracefully shutdown.
4. The customer disconnects, repackages, and returns the NAS device.
5. Once Green Cloud is in possession of the NAS, we will transfer the seed data to the appropriate storage platform as per the Work Order.

Customer Site Finalization
Responsibility: Green Cloud Operations and Customer/Partner
Estimated Timeframe: 1 business day

1. Schedule conference call to install the "ExpressRestore management software" (ZVM) using a screen sharing tool.
2. Install Zerto Virtual Manager (ZVM) on the Windows server allocated for it at the customer's site:
    a. It's highly recommended, although not required, that the Windows machine on which ZVM is installed have no other services or applications. This machine can be virtual or physical. If virtual, it cannot be one of the machines protected.
    b. The ZVM server may not run Windows Server 2012 essentials.
3. Customer must now allow the ZVM server to be accessed via Remote Desktop Protocol (TCP port 3389) and to allow access via TCP port 9669 via the VPN tunnel. (Alternatively, the customer may provide us with a static method to remotely access the ZVM machine).
4. Green Cloud is responsible for the installation of the ZVM software and for configuring initially all VPGs.
    a. There must be only one ZVM per vCenter.
    b. Recommended to always run Zerto services as an account other than LocalSystem.
5. Once the installation is complete, access to the ZVM web interface is verified with the user credentials provided in the site survey.
6. Green Cloud will pair the customer's ZVM(s) with the corresponding ZCC(s).
7. Green Cloud will deploy a Virtual Replication Appliance (VRA) for each ESXi host in the customer's cluster. The customer will asked to input the ESXi root password for each host and provide the vSphere network, IP address for the VRA, and storage location.

Virtual Protection Group (VPG) Setup
Responsibility: Green Cloud Operations and Customer/Partner
Estimated Timeframe: 1-3 business days

A Virtual Protection Group is a logical grouping of VMs which will fail over in unison. By default, Green Cloud will create one VPG per customer VM. The Customer/Partner may not create or edit VPGs

The default service profile provides an RPO of up to 24 hours unless the changes/deltas reach 100% of a given VMDKs size. There are alternative service profiles that can leveraged if there are bandwidth constraints.

Delta/Initial Sync
Responsibility: Green Cloud Operations and Customer/Partner
Estimated Timeframe: Dependent on volume of data

After the initial sync (if seeding over the wire) or deltas (if syncing against seed data) are synchronized and required RPO is being maintained, the order can be finalized.

Finalization, ZSSP Access, Failover Test
Responsibility: Green Cloud Operations and Customer/Partner
Estimated Timeframe: 2 business days, non-sequential

1. Green Cloud will send notification of "Order Completion" via email, including the Partner/Customer's specific access credentials to their Zerto Self-Service Portal (ZSSP)
2. Green Cloud will schedule a call with customer POC to plan a controlled, scheduled "failover test".
    a. The purpose of the failover test is to confirm proper operation of the virtual machine in the cloud, as well as to give the customer the opportunity to discover any changes they'd need to make in the event of a disaster (DNS, DHCP, AD services, etc).
    b. By default, the virtual machines

VPG Operations Options

1. Test Failover
    a. Creates VMs using the test network specified in the VPG (which may or may not be (but usually not) the same subnet as their main LAN, so be careful).
    b. All writes made to virtual disks are done to "scratch" volumes so the longer the test period, the more storage consumed until the VPG-configured maximum disk sizes are reached at which point new writes will fail inside the VM.
    c. NOTE: During the Test Failover, any changes to the customer's live VMs are being transferred and new checkpoints are generated. The VMs will power on automatically without networking. Once testing is complete, the VMs are powered off and removed from the customer's VDC (changes do not persist)
2. Live Failover
    a. The customer VMs and their disks are NOT removed.
    b. All writes made to virtual disks are done to Green Cloud's copy of the VMs and are persistent.
    c. NOTE: If customer requires comprehensive Disaster Recovery testing in which data changes persist while in DR mode (live operations) and then production is failed back, then Live Failover is used

Failover Process

1. Upon customer determination that ExpressRestore-protected VMs need to be spun up in the Green Cloud environment, customer will log into their specific ZSSP interface, select the VPGs to be recovered, and then choose the Live Failover option.
2. A configuration page will follow, giving Auto-Commit, Shutdown Protected VMs, Reverse Protection and Checkpoint options.
    a. Auto-commit: the time delay between the failover and when the failover is committed. Recommended to set at 0 minutes for a Live Failover.
    b. Shutdown Protected VMs: if possible, Zerto will try and gracefully shut down the VMs using VMware tools. Recommended.
    c. Reverse Protection: Zerto will make the "protected VM" the one in Green Cloud's environment and recover to the customer side. Important, if customer plans to fail back to the original environment. NOTE: failing back requires that the customer's vCenter is

licensed with Enterprise licensing (or higher). DRS must also be enabled and set to Partially Automated.

d. Finally, the customer can choose the checkpoint. Useful if not failing over to the most recent checkpoint.

3. 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.
4. It is recommended that the Partner/Customer then access each VM via console to modify networking to match the IP addresses chosen in the VPG creation steps (and therefore in vCloud).

*Express*Restore Disaster Recovery Process

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.

Based on how Zerto is initially configured, the Restore Time Objective is less than one hour per server. The Restore Point Objective is less than 15 minutes per server. These objectives are dependent on the servers' rate of change and the size of the protected group.
When failover is complete, it is recommended that the Partner/Customer 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)

*Express*Restore DRaaS Professional Services

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:

*Express*Restore DRaaS Professional Services		
Service Change Fee - Simple	*(per incident)*	$ 25.00
Service Change Fee - Normal	*(per incident)*	$ 150.00
Consultation Time	*(per hour)*	$ 125.00
Restore	*(per server)*	$ 150.00

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.

Desktop as a Service

Desktop as a Service (DaaS) provides Green Cloud Partners with virtual Windows 2008 or 2012 Servers in the Green Cloud public cloud, which are delivered to users as dynamic or static virtual desktops. The desktop experience will be similar to a Windows 7 or Windows 8 operating system experience. Green Cloud DaaS utilizes Horizon DaaS by VMware for management and provisioning of desktops and the Green Cloud IaaS products for management of group services, such as file serving, Active Directory, and domain management.

This service is ideal for partners wishing to offset customer hardware cost when required to upgrade or replace costly PCs, or when compliance requirements, server age, and/or virtualized applications are required.

DaaS Service Options

The primary objective of DaaS is to provide the Partner with the ability to manage and administrate multiple desktop configurations from a centralized point, allowing for simpler software, configuration, and compliance management for many end-users.

Partners are required to have deployed separately a Green Cloud IaaS solution, within which must reside a Windows Active Directory (AD) server, also referred to as the "Utility" server. Partners may choose for Green Cloud to manage the AD users through the Professional Services offering.

Green Cloud will assist with the initial template (gold pattern) creation and customization for up to two (2) patterns, will provide deployment training, and will provide a basic networking configuration as part of the initial product setup.

The Service Options for the product are:

- Dynamic or Static virtual desktops
- Dynamic desktop resource groupings available:
    - 1 vCPU, 4GB vRAM, 50GB OS image
    - 2 vCPU, 8GB vRAM, 50GB OS image
- Static desktop resources available:
    - 1 vCPU, 4GB RAM, 50GB OS image
    - 2 vCPU, 8GB RAM, 50GB OS image
    - 2 vCPU, 16GB RAM, 200GB OS image
- Configuration for public access to the virtual desktops

Standard customer service and frontline technical support included (Professional Services available)

DaaS Prerequisites

- Assigned and available engineering resource(s)
- Partner sales and desktop support strategy for DaaS (Green Cloud does not provide desktop or application level support)
- Active Directory support (Professional Services available)
- Active Green Cloud IaaS service
    - For each new tenant, an additional Network & Security Bundle is required

After delivery of the environment, it is the Partner's responsibility to notify Green Cloud in the event of any major server changes that could impact the performance of the Desktop as a Service (DaaS) product. The following Partner changes may impact the ability for the environment to be supported by Green Cloud:

- Change of ISP or local area networking (which could impact site-to-site connectivity or firewall rules)
- Modification to firewall rules disallowing public or private access
- Active Directory changes (to specified Organizational Unit, DaaS Admin Group, DaaS User Group, and/or Domain Join User)
- Stopping, powering off, or removing the Utility server in the Customer IaaS environment

DaaS Implementation Plan and Timeline

Through the Implementation Plan, Green Cloud will pre-provision the DaaS environment and provide two (2) "gold patterns." Green Cloud will also initially configure network access and the user/administration interface credentials.

The Partner responsibilities include configuring Active Directory and providing relevant AD information for connectivity to the DaaS environment. The Partner is also responsible for managing any locally installed applications, maintaining operating system(s), and all desktop support requests following the delivery of the environment.

Green Cloud recommends that periodic copies of the partner managed and created patterns are regularly exported and archived for future retrieval. Please contact Green Cloud Operations for assistance.

It is expected that the Partner following and adhere to any written procedural documentation provided by Green Cloud.

Duration	Milestone/Requirement	Responsibility
	Sales Order	Partner and Green Cloud Channel Manager
2-4 days	DaaS Environment Setup and Customer Preparation	GC Advanced Services
1-2 days	DaaS Environment Delivery	Partner & GC Advanced Services

**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.

Sales Order

Responsibility: Partner and Green Cloud Channel Manager
Estimated Timeframe: n/a

1. DaaS Proposal created and delivered to Partner/end-customer via DocuSign
    a. Proposal includes Desktop as a Service (DaaS) product, specifying number and type of desktops
    b. New Partners are required to remit an initial Partner setup fee; for each additional tenant (Location) there is also a required Tenant setup fee
    c. Partner must have an existing (or order at this time) Green Cloud IaaS service

   d. If it is known at the time of the Proposal that Professional Services are needed, or the scope of the engagement is to exceed the below process, then a Statement of Work (SOW) is to be generated and executed along with the Customer Proposal
2. The executed Customer Proposal (agreement) is received via DocuSign. NOTE: Provisioning cannot begin until the fully executed agreement is in-hand at Green Cloud.
3. DRaaS Proposal marked Sold and Work Order is generated. The Work Order is assigned by the Advanced Services manager to an engineer (1 business day)

DaaS Environment Setup and Customer Preparation
Responsibility: GC Advanced Services
Estimated Timeframe: 2-4 business days)

1. Deliver to the partner the introductory email with pre-configuration Active Directory requirements and VPN connection settings form (unless Public Access is requested).
2. As needed, provision new Utility server to house AD and DHCP
3. Configure initial networking (CVR, site-to-site VPN, dtRAM public access, etc).
4. Setup DaaS Service Center
5. As needed, configure dtRAM appliances for Public Access
6. Setup DaaS Enterprise Center
7. Validate DaaS Desktop Portal
8. Green Cloud creates initial templates (up to 3 total)

DaaS Environment Delivery
Responsibility: Partner & GC Advanced Services
Estimated Timeframe: 1-2 business days)

1. Deliver to partner provisioning email with DaaS portal URL and credentials.
2. Upon initial login, the Partner will configure required Active Directory settings.
3. Once AD connectivity is confirmed, Green Cloud will schedule a conference call for training and environment handoff with partner, which will provide instruction for:
   a. Gold Pattern creation
   b. Desktop deployment
   c. Pool management
   d. AD pre-requisites and configuration tips
   e. Network management guidance

Disaster Recovery

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

DaaS Professional Services

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:

DaaS Professional Services		
Service Change Fee - Simple	*(per incident)*	$ 25.00
Service Change Fee - Normal	*(per incident)*	$ 150.00
Consultation Time	*(per hour)*	$ 125.00
SysAdmin Services (Active Directory)	*(per user/per month)*	$ 5.00

Backup as a Service

Backup as a Service (BaaS) provides Green Cloud Customers and Partners with a remote, secure, cloud-based storage destination for existing server infrastructures utilizing Veeam Backup & Replication (version 8). Green Cloud's infrastructure is leveraged as an additional or replacement backup repository. This service better enables Customers and Partners to fulfill the "3-2-1" rule: maintain three (3) copies of data, store on two (2) different types of media, and keep at least one (1) copy offline, e.g. in the Cloud.

BaaS Service Options

The Service Options for this product include a choice between Standard or Premium service:

- Standard
  - Repository is located in a single data center (choice of Greenville, SC or Nashville, TN locations).
  - Repository disk space is provisioned in 500GB increments.
- Premium
  - Repositories located in two data centers. Data transferred to the repository from the premise is regularly archived by Green Cloud to the second data center.
  - Repository disk space is provisioned in 500GB increments.
  - WAN acceleration available (premise must have Veeam 8 Enterprise Plus)

Included with all BaaS services are:

- 5 VMs can be backed up for every 500GB of storage purchased (additional VMs can be configured for additional cost per VM)
- 10Mb/s port speed (additional bandwidth available at additional cost based on speed)
- Automatic repository disk space increases when usage exceeds 90% of allocated space (regular rates apply)

Required Green Cloud services for each BaaS environment are:

- Customer or Partner must be currently utilizing Veeam Backup & Replication (version 8). Green Cloud cannot license, provide, or install this application.
- Sufficient bandwidth from the premise to the Green Cloud infrastructure so support the backup file transfers

Snapshots vs Backups vs Replication

Snapshots are not the same as backups and shouldn't be used in the same way for Disaster Recovery planning.

Here's why:

A **snapshot** is a point-in-time 'picture' of the state of a virtual machine's disk(s) at the instant the snapshot is taken. Snapshots are also usually saved on the same media as the VM, to save I/O when a recovery is needed. Snapshots are not overwritten in the "grandfather-father-son" schema; they live 'side-by-side' until deleted. It is also not optional to retrieve individual files from a snapshot (the entire disk must be mounted and made available; see the 3 data recovery options for snapshots below).

Snapshots are ideal for recovery to the last known good - and recent - VM configuration in case of VM failure.

A **backup** is a full copy of the virtual machine's data and applications, taken while the VM is in a prepared state and is usually saved to separate media (i.e. to a different SAN or a redundant data center). Backup jobs are

typically configured to consolidate the files periodically based on the "grandfather-father-son" schema (or similar). For example, daily backups might be consolidated every 8th day to be replaced by a weekly version. The weekly backups might be consolidated after five weeks, as this is when monthly version created; and the monthly copies are replaced by an annual backup, and so on.

Backups are ideal for retrieval of historical data and files in case of audit or data loss; and while possible, backups are not intended for full VM recovery in case of failure.

Replication is the practice of copying live data from one location to another to maintain a mirrored version of the machine on separate media. Replication is ideal for machines and applications that have very high availability requirements but low retention needs.

BaaS Implementation Plan and Timeline

Green Cloud will manage the initial creation of the BaaS repository and provide access information and credentials necessary for the Customer and/or Partner to configure backups to be directed to the new repository.

The Partner/Customer responsibilities include configuring the local premise to utilize the Green Cloud repository as a destination. Partner and Customer also agree to follow any written procedural documentation provided by Green Cloud.

Duration	Milestone/Requirement	Responsibility
	Sales Order Site Survey	Partner, Customer, and Green Cloud Channel
1-2 days	BaaS Repository Setup	Green Cloud Operations

**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 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.

Sales Order

Responsibility: Partner, Customer, and Green Cloud Channel Manager
Estimated Timeframe: n/a

4. BaaS Proposal created and delivered to Partner/end-customer via DocuSign
5. Proposal includes Backup as a Service product, specifying “Standard” or “Premium” level service. The order will specify a preferred data center location, and the volume of storage required (in 500GB increments). If WAN acceleration is desired, it must be specified in the Proposal of Service. NOTE: Selection of a Networking and Security Bundle is ***not*** required for BaaS service.
    a. If it is known at the time of the Proposal that Professional Services are needed to support the BaaS environment post-installation or post-migration; or if the scope of the engagement is to exceed the process outlined below, then a Statement of Work (SOW) is to be generated and executed along with the Customer Proposal

6. The executed Customer Proposal (agreement) is received via DocuSign. NOTE: Provisioning cannot begin until the fully executed agreement is in-hand at Green Cloud.
7. BaaS Proposal marked Sold and Work Order is generated. The Work Order is assigned by the Operations manager to an Operations technician (estimated timeframe: 1 business day).

BaaS Repository Setup and Customer Preparation

Responsibility: Green Cloud Operations
Estimated timeframe: 1-2 business days

1. Provision new Repository.
2. Ensure that the resources are sufficient to receive backups, as specified in the Work Order.

Order Finalization

Green Cloud will send notification of "Order Completion" via secure email, including the Partner/Customer's specific access credentials

Service Operations

After delivery of the product, it is the end-user's responsibility to notify Green Cloud in the event of any major changes that could impact the performance of the IaaS environment. The following client-side changes will impact the ability for the environment to be accessible:

- Change of ISP or local area networking (which could impact site-to-site connectivity or firewall rules)
- Modification to firewall rules disallowing public or private access
- Significant modifications to backup sizes
- Addition or removal of servers being backed up

Events, Incidents, and Problems will be addressed by Green Cloud per the Incident Resolution process as outlined in the Services Agreement.

BaaS Disaster Recovery Process

In the event that the end-user determines it is necessary to retrieve a particular backup, there is an immediate need to contact Green Cloud. The partner/customer will reach Operations Support at 877-465-1217 or support@gogreencloud.com.

Customers/Partners needing to retrieve backup data from their repository have two basic delivery options:

- "Over-the-Wire:" Green Cloud will increase port speed to 100Mb/s to facilitate internet file transfer
- Physical Media: Green Cloud will move specifically requested data to an encrypted hard drive for shipment (Data Export fees may apply). Please note that the Service Level Objective for this option includes the file copy time as well as applicable shipping and handling time.

BaaS Professional Service Fees

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:

IaaS Professional Services		
Service Change Fee - Simple		$ 25.00
Service Change Fee - Normal		$ 150.00
Consultation Time	*(per hour)*	$ 125.00
Server Export	*(per Virtual Server)*	$ 175.00
Data Import	*up to 1TB*	$ 175.00
	Add'l 5TB increments	$ 100.00

Networking and Security

The Networking and Security services provide Green Cloud Customers and Partners with a range of options from basic cloud access to complex routing and security. The Network and Security Bundle combines popular features and functionality into simple groups to be easily deployed, supported, and managed. Based on the complexity of end-user requirements and any Professional Services selected, the network and security features can be managed directly by the Customer/Partner or by Green Cloud's experienced Operations support team. In addition to the predesigned bundles, Green Cloud offers several complementary services to support customized networking solutions.

Networking & Security Service Options

The primary objective of Networking and Security products is to provide the end-user with an appropriate networking solution for their environment, given their preferred utilization of their virtual environment.

The Service Options for the product are:

- Choice of Networking and Security bundle (see below), each of which includes:
- One (1) public, static IP address
- At least 10Mbps Public Internet Port speed
- Virtual Stateful firewall
- Internal cross connect
- Standard customer service and frontline technical support included (Professional Services available)

Network & Security Bundles:

Advanced Firewall (w/ Standard Routing) Features

- Cisco Powered (ASAv) appliance
- 10Mbps to 500Mbps Public Internet Port Speed
- Customer managed NAT, static routing, and Firewall (managed services available)
- Zone-Based Firewall and Deep Packet Inspection
- Full IPsec site-to-site VPN support
- Service Policies (Rate Limiting, Quality of Service)
- High Availability optional

Advanced Routing (w/ Standard Firewall) Features

- Cisco Powered (CSR-SEC) appliance
- 100Mbps to 500Mbps Public Internet Port Speed
- Customer managed NAT, static routing, and Firewall (managed services available)
- Zone-Based Firewall
- Full IPsec site-to-site and SSL VPN support
- Advanced Routing (MPLS, PBR, VRF-Lite), BGP4, IGPs
- Service Policies (Rate Limiting, Quality of Service)
- Netflow
- High Availability optional

Premium Bundle Features

- Cisco Powered (CSR-IPB + ASAv) appliances
- 100Mbps to 500Mbps Public Internet Port Speed

- Customer managed NAT, static routing, and Firewall (managed services available)
- Advanced Firewall (Stateful, Zone-Based, Deep Packet Inspection)
- Advanced Routing (MPLS, PBR, VRF-Lite), BGP4, IGPs
- Full IPsec site-to-site and SSL VPN support
- Service Policies (Rate Limiting, Quality of Service)
- Netflow
- High Availability optional

Additional Networking and Security Service Options:

Virtual Private Networking

- IPsec site-to-site
- SSL user based
- managed by virtual appliance*

Private Interconnection

- Private bandwidth circuit to the desired data center (via MPLS/NNI)
- Optional managed customer premise equipment
- NNI port (10Mbps, 100Mbps, or 1 Gbps)

Public Internet Port

- Required for collocated services and Private Cloud
- Available speeds from 10Mbps to 500Mbps

Colocation

- Rack Unit(s)
- Basic or Redundant Power

Internal cross connect(s)

- choice of fiber or copper
- private internet port speed

Managed Router/Firewall services available (See Professional Services)

- Initial installation and setup included
- Patches, OS upgrades, configuration backups included
- Availability monitoring (up/down) and device security included
- Utilization reports available upon request
- Managed Router/Firewall service is not required for the following virtual appliance configuration requests:
  - DHCP: pool management
  - NAT: Source (SNAT) or Destination (DNAT) rule modification
  - Firewall: Allow/Denys rule modification
  - Static Route modification
  - Site-to-Site VPN peer modification

* *Based on bundle selected*

Service Requirements

- With the exception of colocation, the customer must have purchased and provisioned IaaS, DRaaS, Private Cloud, or DaaS services to receive any Networking & Security products
- One (1) Networking & Security Bundle is required per IaaS virtual datacenter and/or logically separated customer network (in the case of Bulk Resource provisioning)
- For VPN networks, the customer by default is expected to provide their own premise hardware capable of establishing an IPsec VPN tunnel. Green Cloud provided hardware is available for lease

After delivery of the product, it is the end-user's responsibility to notify Green Cloud in the event of any major network or routing changes that could impact the performance of the Networking and Security features being provided. The following client-side changes will impact the ability for the environment to be fully supported at Green Cloud:

- Changes to local or wide area network address schema
- Changes to Internet Service Provider or premise equipment
- Changes to routing tables, firewall rules, carrier's routing, virtual appliance, and/or virtual server configuration
- Removal, suspension, or power cycling of virtual appliances

Networking & Security Implementation Plans and Timelines

Green Cloud will deploy a basically configured virtual appliance, based on the work order received. The basic configuration will include insuring outbound Internet access from the virtual server environment and permitting RDP and/or SSH for remote access depending on virtual appliance and virtual server type. RDP and SSH traffic will be configured using Network Address Translation (NAT) and a randomly selected "high" port number in an effort to prevent unauthorized access.

Additional networking and security support is available for more complex routing and firewall configuration needs; refer to Professional Services product description for more details on Managed Router/Firewall support.

The Partner/Customer is responsible for adhering to written procedural documentation provided by Green Cloud.

Duration	Milestone/Requirement	Responsibility
	Sales Order	Partner, Customer, and Green Cloud Channel
1-2 days	Virtual appliance deployment (default configuration) Remote access (RDP or SSH) provided	Green Cloud Operations

VPN Networking

For **IPsec site-to-site VPN** networking, Green Cloud will provide a VPN Connection Settings form to obtain particular details for the "peer" end of the connection. The "local" end will be configured in the vShield Edge (for Basic bundle) or a Cisco virtual appliance (for Advanced and Premium bundles).

Necessary firewall rules will be updated to allow data to traverse the VPN in both directions (peer-to-local and local-to-peer).

Once the initial configuration is made, any subsequent modifications to the site-to-site VPN tunnel may require a change fee. A monthly recurring charge for Managed Router/Firewall service is available for Partners and/or Customers with a high number of configuration change requests.

For **SSL user VPN** environments, Green Cloud will provision an OpenVPN virtual appliance in the Partner/Customer's virtual datacenter (VDC). NOTE: The VDC's resources consumed by the OpenVPN appliance will be added to the Organization by default and are not separately chargeable. A public IP will be assigned to a network interface in the appliance and a customer/location-specific URL mapped to that IP to allow web-based access to the SSL client.

The Partner/Customer will be able to obtain, download, and install the OpenVPN client from the customer-specific URL to each desktop/end-user requiring SSL VPN access. User accounts will be directly provisioned by Green Cloud.

The Partner/Customer is also responsible for completing the VPN Connection Settings form (for site-to-site), providing usernames and desired passwords (for SSL user VPN) and adhering to written procedural documentation provided by Green Cloud.

Duration	Milestone/Requirement	Responsibility
	Sales Order VPN Connection Settings Form (IPsec only)	Partner, Customer, and Green Cloud Channel Manager
1-2 days	Virtual appliance configuration Firewall update (IPsec only) User account setup (SSL only)	Green Cloud Operations

Interconnection Options

Green Cloud will order a private interconnect circuit (aka bandwidth) from the customer premise to the data center of choice from an underlying carrier within one business week of receiving the Work Order. A site survey will be delivered to determine the managed router's configuration, including but not limited to local area networking, firewall and VPN requirements, and interoperability with existing premise equipment.

Typically, broadband circuits are delivered between thirty (30) and one-hundred-twenty days (120) from the time they are ordered, depending on the premise's location with respect to the carrier's network, the type of circuit ordered, and the viability of entrance facilities. Green Cloud will coordinate with the carrier and the customer/partner's technical and on-site contacts with respect to information gathering (site survey) and scheduling.

Once a Firm Order Commitment (FOC) date is received from the carrier, Green Cloud will ship a pre-configured device to interconnect the circuit with the partner/customer's network. Physical installation can be completed by the partner/customer with remote direction from Green Cloud, or an authorized installation partner can be scheduled.

Prior to the "cutover" date, Green Cloud will configure internal cross-connects and a private interconnect port, as needed, at the data center.

The Partner/Customer is responsible for providing a complete and accurate site survey, providing uninterrupted power to the hardware, managing the local area network configuration (unless otherwise specified), and adhering to written procedural documentation provided by Green Cloud.

Duration	Milestone/Requirement	Responsibility
	Sales Order	Partner, Customer, and Green Cloud Channel
5 Days	Order placed for private circuit	Green Cloud Operations
30-120 Days	Carrier installation of private circuit	Carrier
	Delivery of pre-configured premise equipment	Green Cloud Operations
	Cross Connects and Private Interconnect Port configuration	Green Cloud Operations
	Installation of premise equipment	Partner/Customer or GC Install Partner
1 Day	Scheduled LAN cutover to private circuit	Green Cloud Operations, Customer/Partner, and/or GC Install Partner

Colocation

For each physical device requiring colocation, Green Cloud will reserve the requested number of rack units, configure basic or redundant power, complete all pre-wiring, and configure necessary private interconnect ports. After installation, additional physical work can be requested of Green Cloud and is subject to a Smart Hands fee (this work may be sub-contracted to an authorized partner).

The Partner/Customer is responsible for any and all costs of shipping equipment to and from the data center and pre-configuring the collocated devices for remote access (once connected to the Green Cloud network or carrier's termination equipment). The Partner/Customer is also responsible for adhering to any written procedural documentation provided by Green Cloud.

Duration	Milestone/Requirement	Responsibility
	Sales Order	Partner, Customer, and Green Cloud Channel

5-10 Days	Setup rack units, power, pre-wiring, and private interconnect ports	Green Cloud Operations (or GC Install Partner)
	Shipment and pre-configuration of equipment	Partner/Customer
2-3 Days	Physical installation of equipment	Green Cloud Operations (or GC Install Partner)

**some timeline estimates dependent on Partner/Customer scheduling with Operations, on-site access, and communication methods*

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

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.

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

Networking & Security Professional Services

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:

Networking & Security Professional Service Fees		
Service Change Fee - Simple	*(per incident)*	$ 25.00
Service Change Fee - Normal	*(per incident)*	$ 150.00
Consultation Time	*(per hour)*	$ 125.00
Smart Hands	*(per incident)*	$ 50.00
Managed Router/Firewall Service	*(per router per month)*	$ 100.00

Professional Services

Professional Services provide Green Cloud Customers and Partners with complementary engineering labor and skills to implement a new, or enhance an existing, cloud infrastructure.

Green Cloud is solely channel focused and will only sell products and services through an authorized partner. Professional Services do not supersede or replace a Partner's existing IT services or contracts with end-users, but instead these services are intended to augment the Partner's offering when there is a need identified.

The primary objective of Professional Services is to provide the Partner with engineering or otherwise technical resources to complete cloud projects.

The services offered are:

- Consultation time
- Data and Server Migration services
- Windows Server Administration (for DaaS/VDI environments)
- Networking & Security management
- Service Change Requests

Consultation Time

Consultation time is defined as billable hours from a certified Green Cloud NOC or Sales engineer for the purpose of designing, troubleshooting, maintaining, or monitoring a customer's or partner's hardware, software, or networking infrastructure, whether hosted at Green Cloud or on the customer premise.
Consultation Time is only billed as a result of an executed service agreement or Statement of Work, and is billed in one (1) hour increments only.

Data and Server Migration services

Green Cloud will import a provided server image or will manage the migration from the customer's physical or virtual server(s) to a virtual datacenter environment. Green Cloud can also assist with the physical import of large data when it is not feasible to transfer through other means.

Simple Server Migrations

In a simple server migration, the customer/partner provides to Green Cloud a copy of the existing physical or virtual server in standard VMware virtual machine disk (VMDK) format. Green Cloud will accept the VMDK via physical media, then transfer and convert that image into a Virtual Appliance/Virtual Machine in the customer's designated Virtual Datacenter (VDC).

Once the virtual machine is created, Green Cloud will provide restricted remote access capability (RDP) and management credentials (vCloud Director) to the customer and/or partner for further configuration of server applications, OS firewall settings, server networking, firewall and NAT rules, et cetera. Written instructions for management via vCloud Director will also be provided.

This migration is not considered "managed" as the creation of the VMDK image is dependent on the customer and/or partner, and the timing of the end-user's transition to the virtual server is dependent on the receipt of a usable VMDK image.

End-user downtime will occur from the time that the local server is powered off (sometime after the VMDK image is created) until the time that the server is powered on as a virtual machine in the data center, and remote access is available. This downtime is inclusive of the shipping time necessary to transmit the media with the VMDK image from the customer/partner to Green Cloud's offices.

Please note that advanced coordination with Green Cloud Operations is required for after-hours or weekend migrations, and additional charges may apply.

The customer and/or partner are responsible for local network and end-user desktop changes necessary to access and utilize the migrated virtual server.

Advanced (Managed) Server Migrations

In an advanced server migration, also known as a managed server migration, Green Cloud may leverage the user of a network attached storage device (NAS) and/or replication software to coordinate migration of large server environments and/or servers that have low threshold for extended downtime during the cutover.

There are two options for advanced server migrations, depending on the use case. For small-to-medium sized environments that have servers with downtime requirements greater than one hour (4 hours on average), migration via StorageCraft is available. For those environments with a transition timeframe closer to one hour per server, or for larger infrastructures, migration via Zerto is preferred.

Via StorageCraft

Green Cloud will provide a fully configured Synology NAS, remotely install the StorageCraft software on a customer server, and manage the off-site synchronization of incremental server changes to the cloud.
Once the incremental server changes replicated to the Green Cloud environment are in sync with the local changes, the migration date can be scheduled with the end-user.

Prior to the migration time, the customer and/or partner will be asked to cease all changes on the local servers, so that a final backup incremental can be obtained and transferred. End-user downtime will begin at this step and continue until the time that the incremental is fully transferred, and the Green Cloud Operations technician can convert the replicated data into virtual machine(s). The average conversion time is approximately 1 hour per server.

Please note that advanced coordination with Green Cloud Operations is required for after-hours or weekend migrations, and additional charges may apply.

The customer and/or partner are responsible for local network and end-user desktop changes necessary to access and utilize the migrated virtual server.

Via Zerto
Green Cloud will provide a fully configured Seagate or QNAP NAS, remotely install the Zerto software, and configure the recovery environment to accept the protected server group.

Once the physical environment is seeded, the migration date can be scheduled with the end-user.
Prior to the migration time, the customer and/or partner will be asked to cease all changes on the local servers, so that no end-user changes are lost. End-user downtime will begin at this step and continue until the time that

the Zerto failover is fully complete. The average failover time is approximately 1 hour for typically sized environments.

Please note that advanced coordination with Green Cloud Operations is required for after-hours or weekend migrations, and additional charges may apply.

The customer and/or partner are responsible for local network and end-user desktop changes necessary to access and utilize the migrated virtual server.

Data Import/Export services

For transfers of large quantities of data, Green Cloud can arrange to receive physical media at the data center and manage the data transfer to/from a virtual machine. Green Cloud can also temporarily provide encrypted USB drives or network attached storage devices.

Windows Server Administration (for DaaS/VDI environments)

Windows Server Administration for DaaS/VDI environments is defined as the management of Active Directory profiles and charges are based on the total number of users configured in the managed environment on a recurring monthly basis.

Managed Router/Firewall (Recurring Charge)

Green Cloud will manage the configuration and updates for virtual router and firewall appliances, physical devices collocated in the data center, and/or customer premise equipment. Also included in this service are patches, OS upgrades, availability monitoring, and device security. Utilization reports available upon request. Service charges are applied on a per device basis, recur monthly, and will supersede the one-time Change Request Fees typically applied to Green Cloud provided network appliances (e.g. Cisco ASAv, Cisco CSR).

Managed Router/Firewall service is not required for the following virtual appliance configuration requests:

- DHCP: pool management
- NAT: Source (SNAT) or Destination (DNAT) rule modification
- Firewall: Allow/Denys rule modification
- Static Route modification
- Site-to-Site VPN peer modification

Smart Hands

Smart Hands is necessary to manage the shipping, handling, and receipt of media or devices to and from our headquarters or data center. Smart Hands is required for physical (re)configuration changes for all collocated equipment.

Service 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 same business day and does not require customer re-design or end-user scheduling.

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.

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.

Implementation Plans and Timelines

Below are high-level implementation plans and timelines for some of the professional services that are offered:

Simple Migration

Duration	Milestone/Requirement	Responsibility
	Sales Order Site Survey	Partner, Customer, and GC Channel Manager
1 day	Request to complete site survey sent to Technical POC and/or Partner	Green Cloud Operations
*	VMDK created and shipped	Partner and/or Customer
1 day	VMDK received, transferred, converted to Virtual Machine. Remote access provided	Green Cloud Operations
	End-user configuration, local area network/OS finalization	Partner and/or Customer

1. Upon receipt of the site survey, information is transferred into the Work Order.
2. Provision new Organization, Virtual Datacenter (VDC), Edge Gateway, and Organization Network in the destination vCloud Director site.
3. Ensure that the VDC resources are sufficient to run all of the replicated VMs during a failover.
    a. If resources are not sufficient, Partner/Customer and Green Cloud Channel Manager are engaged to adjust the Work Order and be notified of pricing change.
4. *Upon receipt of the server image (VMDK), Green Cloud Operations will transfer and convert the image into a virtual appliance/virtual machine in the customer's VDC.
5. If no other migration work or Professional Services are ordered, skip to "Networking & Security Setup"

Advanced (Managed) Migration

Duration	Milestone/Requirement	Responsibility
	Sales Order Site Survey	Partner, Customer, and GC Channel Manager
1 day	Request to complete site survey sent to Technical POC and/or Partner	Green Cloud Operations
1-3 days	NAS Configuration (if applicable)	Green Cloud Operations
*	NAS and encrypted USB drive Shipped (if applicable)	Green Cloud Operations
*	On-site NAS installation, remote access provided (if applicable)	Partner and/or Customer
1-3 days	Seed data obtained and transferred to encrypted USB drive (if applicable)	Green Cloud Operations
*	Upon completion of seed data transfer, USB drive shipped to Green Cloud (if applicable)	Partner and/or Customer
1-2 days	Seed data received, transferred. Setup finalization	Green Cloud Operations
7-14 days	Data sync obtained	Green Cloud Operations
*	Cutover date scheduled	Partner and/or Customer
1 day	Cutover completed	Green Cloud Operations
	End-user configuration, local area network/OS finalization	Partner and/or Customer

NAS Configuration
Responsibility: Green Cloud Operations
Estimated Timeframe: 1-3 business days

6. Upon receipt of the completed Site Survey, the Green Cloud technician will compare the protected servers' specifications to the Work Order. If there are any discrepancies, the order may be stopped until clarification is received. In some cases, resources may be changed on the Work Order which in turn will modify billable charges, but by no more than +/-25%.
7. The partner and dealer manager will be notified that the work order cannot be completed when protected servers are:
    a. Currently licensed under the OEM channel with Windows Server 2003 or earlier, or
    b. Running Windows Small Business Server of any version, or
    c. Virtual servers running within a physical host and not listed individually on the Work Order, or are
    d. Not Windows servers (i.e. UNIX/Linux machines not supported).
8. Based on the consumed disk space amounts, the NAS will be configured with appropriately sized hard disk drives. The NAS' operating system will be installed, configured and optimized to receive incremental backups from the local servers once on premise.

9. Green Cloud technician will configure the cloud environment to receive the incremental files relayed by the NAS
10. Green Cloud will ship the NAS and an encrypted USB drive to the address specified in the Site Survey. If no specific address is entered, the shipment will default to the service address on the Work Order.

NAS Installation
Responsibility: Partner or Customer
Estimated Timeframe: 1 week (requested)

1. Upon receipt of the NAS, the customer and/or partner are asked to follow the installation instructions provided in PDF format via email:
    1) Plug the included AC adapter into a power outlet and the back of the Synology.
    2) Plug the provided Ethernet cable into the RJ45 port on the back of the Synology and into the selected RJ45 Ethernet port on the local LAN switch.
    3) Connect the encrypted USB drive to the Synology using both prongs of the provided Y-cable and unlock the drive by entering the provided code and pressing the unlock button in the bottom left.
    4) Press the blue power button on the face of the Synology.
2. Once the NAS is installed and powered on, the customer and/or partner are asked to contact Green Cloud.
3. Green Cloud will verify remote access to the NAS and at least one server on which to install ImageManager software for replication job management.

Seed Data
Responsibility: Green Cloud Operations and Partner/Customer
Estimated Timeframe: 1-3 business days

6. Green Cloud will remotely install ImageManager software for replication job management. To complete the installation, a reboot of the server must be completed.
7. Green Cloud will request that the server be rebooted at the earliest convenience to the customer and/or partner.
8. When the installation is complete, and initial backups are running, the customer and/or partner will be notified.
9. Typically on the next business day, Green Cloud will verify that the incremental backups are being received in the cloud and start the full backup of the server(s) to the encrypted USB drive which is connected to the NAS.
10. When backups are complete, the partner and/or customer are requested to disconnect the USB drive, enclose it in the provided packaging, and return to Green Cloud using the provided pre-paid shipping label.

Server Synchronization
Responsibility: Green Cloud Operations
Estimated Timeframe: 5-15 business days

5. Upon receipt of the seed data via the encrypted USB drive, Green Cloud will upload into a secure, segregated customer environment.
6. Green Cloud will configure the retention, verification, and consolidation settings to maintain the synchronized data from the on premise customer NAS.

7. Once the incremental files are maintaining synchronization with the premise server, Green Cloud can schedule with the Partner/Customer the cutover date.

IaaS Environment Setup and Customer Preparation
Responsibility: Green Cloud Operations
Estimated Timeframe: 1-3 business days, concurrent to sync

3. Provision new Organization, Virtual Datacenter (VDC), Edge Gateway, and Organization Network in the destination vCloud Director site.
4. Ensure that the VDC resources are sufficient to run all of the replicated VMs during a failover.
    a. If resources are not sufficient, Partner/Customer and Green Cloud Channel Manager are engaged to adjust the Work Order and be notified of pricing change.

Cutover Date
Responsibility: Green Cloud Operations and Customer/Partner
Estimated Timeframe: 1 business day

1. On the scheduled cutover date, the customer/partner will be asked to disconnect or power down the server(s) to be migrated so that a final incremental file can be transferred.
2. Upon successful transfer of the final incremental, Green Cloud will begin the conversion of the server files saved in the customer's cloud environment into virtual appliances/virtual machines in the customer's VDC.
3. Once all servers can be powered on and accessed successfully, Green Cloud will continue with the Networking & Security Setup.

Data Import

For transfers of large quantities of data, Green Cloud can arrange to receive physical media at the data center and manage the data transfer to/from a virtual machine. Green Cloud can also temporarily provide encrypted USB drives or network attached storage devices.

Upon receipt of physical media, devices will be connected and a transfer initiated in the same business day. The duration of the transfer is dependent on the volume of data to be moved, and the type of device provided.

**some timeline estimates dependent on Partner/Customer scheduling with Operations, on-site access, and communication methods*

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

Professional Service Fees

Professional Services Standard Fee Schedule		
Service Change Fee - Simple	*(per incident)*	$ 25
Service Change Fee - Normal	*(per incident)*	$ 150

Consultation Time	*(per hour)*	$ 125
Migration/Implementation - Simple	*(per Virtual Server)*	$ 150
Migration/Implementation - Advanced	*(per Virtual Server)*	$ 300
IaaS Server Restore	*(per Virtual Server)*	$ 100
IaaS Data Import	*up to 1TB*	$ 175
	5TB increments	$ 100
IaaS Server/Data Export	*(per Virtual Server)*	$ 175
DRaaS Server Restore	*(per server)*	$ 150
Smart Hands	*(per incident)*	$ 50
Managed Router/Firewall	*(per appliance/per month)*	$ 100
SysAdmin Services (DaaS)	*(per user)*	$ 5
DaaS Pattern Restore	*(per pattern)*	$ 100