

Addendum

Infrastructure as a Service

June 2020

Contour Data Solutions

4259 West Swamp Road, Suite 301

Doylestown, PA 18902

This Infrastructure as a Service Addendum (this “Addendum”) is subject to and part of the Contour Master Cloud and Managed Services Agreement (the “Agreement”) between Contour Data Solutions LLC (“Contour”) and Customer. Any capitalized terms that are not defined in this Addendum shall have the meanings set forth in the Agreement.

1. Description of Services

- a. The “Private Cloud” Service provides Customer with a single-tenant cloud with dedicated physical servers, a dedicated network for Internet traffic, dedicated storage volumes, and a dedicated cloud management instance. Infrastructure capacity may be allocated to a single data center or multiple data centers at your option.
- b. The “Virtual Private Cloud” provides a multi-tenant virtual cloud with logically isolated resources on shared physical infrastructure, configured as a single virtual data center with networking resources. Each VPC is fully encrypted and isolated from other customer environments.

2. Service Provisioning

- a. **Contour will:**
 - (1) Provide the resources (such as physical servers, physical storage, and physical network devices) needed to provide the IaaS Services.
 - (2) Provide network bandwidth in accordance with the applicable Service Offering.
 - (3) Provide resource pools (memory, processing, primary storage, and networking) with the applicable Service Offering
 - (4) Create Cinch and/or other user accounts and set default system preferences; and
 - (5) Create and configure applicable virtual server templates, as further described below.
- b. **Customer will:**
 - (1) Install and configure custom or third-party applications and operating systems on deployed virtual machines; and
 - (2) Deploy and maintain on-premises and other resources for disaster recovery with the applicable Service Offering

3. Data Recovery

- a. **Contour will provide the following services with respect to Data Recovery:**
 - (1) Data protection, such as routine backups, for cloud infrastructure, including top-layer management and user-management interfaces owned and operated by Contour.
 - (2) Data and infrastructure restoration for the cloud infrastructure, including top-layer management and user-management interfaces owned and operated by Contour.
 - (3) Data protection, such as routine backups, for the data and content accessed or stored on Contour virtual machine’s or storage devices, configuration settings, etc.
 - (4) Data, content, virtual machine, and configuration restorations for assets accessed or stored with Contour.
- b. **Customer will:**
 - (1) Be responsible for backing up applications and their own systems
 - (2) Be responsible for securing access to Systems

- (3) Be responsible for providing anti-virus and malware technologies
- (4) Be responsible for deploying and maintain disaster recovery services with Contour or another provider of disaster recovery solution.

4. Monitoring

- a. **Contour will provide the following services with respect to Monitoring:**
 - (1) Monitoring Contour Cloud infrastructure, infrastructure networks, top-layer management and user-management interfaces, and computing, storage, and network hardware for availability, capacity, and performance.
- b. **Customer will:**
 - (1) Be responsible for monitoring their own Application, systems, and servers
 - (2) Be responsible for Monitoring the assets deployed or managed by Customer, including, but not limited to virtual machines, operating systems, applications, specific network configurations, operating system, or application vulnerabilities

5. Templates

- a. **Customers will also have access to Contour-provided operating system templates to the extent that:**
 - (1) Published templates cannot be accessed from the Service Catalog
 - (2) Published templates cannot be instantiated without modification
 - (3) Published templates cause errors at first run time
 - (4) There are substantial hangs or excessive delays in the retrieval of a template from the Service Catalog
- b. The configuration of a published template affects the virtual machine's interaction with the hypervisor
- c. Time synchronization issues (NTP) exist
- d. **Customer will:**
 - (1) Be responsible for licensing and consumption of 3rd party software
 - (2) Be responsible for maintaining accurate recording for reporting of consumption of 3rd party licensing

6. Virtual Server Deployment Templates

- a. Contour will provide a catalog of supported virtual server deployment templates that you may deploy into your Contour environments for Private Cloud and Virtual Public Cloud. Contour will maintain and update these templates from time to time. Templates that are provided by Contour may be removed at any time. Customer is responsible for selecting, deploying, and configuring templates appropriate to its needs, and for activating related licenses, and maintaining compliance with such license terms.
- b. In order to comply with Contour's legal obligations to its third-party licensors, Customer will not be permitted to export, download, or remove certain templates or any installed forms of certain templates for installation or use outside of the IaaS Service Offering. Customer may implement or import virtual server deployment templates if it has sufficient legal rights to deploy and use the software and information contained in such templates

7. Networking Services

- a. **The Contour Platform includes the following network services as a part of the core cloud**

subscription:

- (1) Network Address Translation (NAT): Separate controls for Source and Destination IP addresses, as well as port translation.
- (2) Dynamic Host Configuration Protocol (DHCP): Configuration of IP pools, gateways, DNS servers, and search domains.
- (3) Firewall: Our Firewall Management service provides 24x7 firewall administration, and response to security and device health events.
- (4) Site-to-Site Virtual Private Network (VPN): Uses standardized IPsec protocol settings to interoperate with all major VPN vendors.
- (5) Static Routing: Static routes for destination subnets or hosts.
- (6) Dynamic Routing: Supported protocols include OSPF and BGP. This feature is available when customer subscribes to Direct Connect offering.
- (7) Blended Internet with BGP.

8. Tools

a. Clients will also have access to Contour-provided Tools, including:

- (1) Contour Tools Installation and Configuration
- (2) Contour Tools for optimization
- (3) Performance tuning as it relates to Contour tools and drivers

b. Customers are responsible for the following:

- (1) Your organization, virtual data center, or organization network administration, configuration, and modification.
- (2) User-deployed and configured assets such as virtual machines, custom developed or third-party applications, custom or user-deployed operating systems, network configuration settings, and user accounts.
- (3) Operating system administration including the operating system itself or any features or components contained within it.
- (4) Performance of user-deployed virtual machines, custom or third-party applications, your databases, operating systems imported or customized by you, or other assets deployed and administered by you that are unrelated to services provided by Contour.

9. Change Management

a. Contour will:

- (1) Maintain processes and procedures to intended to ensure the health and availability of the Contour Cloud and infrastructure in the Contour Area (as defined in Section 10 below); and
- (2) Maintain processes and procedures to release new code versions, hot fixes, and service packs related to the Contour Cloud components in the Contour Area.

b. Customer is responsible for:

- (1) Custom or third-party applications, databases, and administration of the Customer Area (as defined in Section 4 above); and
- (2) Administration of self-service features, up to the highest permission levels granted to you, including but not limited to virtual machine and network functions, backup administration, user configuration and role management, general account management.

10. Security

- a. “Contour Area” means the areas of the Contour infrastructure and systems for which Contour has sole administrative control. “Customer Area” means the portions of the systems where Customer assumes full or partial control, permission, or access to modify an environment.
- b. **Contour will use commercially reasonable technical and organizational measures designed to provide the following:**
 - (1) Physical security measures intended to protect Contour’s data centers from physical security breaches.
 - (2) Information security measures intended to protect the Contour Area.
 - (3) Network security measures intended to protect the Contour Area.
 - (4) Monitoring for potential security events in the Contour Area; and
 - (5) Patching and vulnerability management of the systems Contour uses to deliver the IaaS environment, including the application of patches it deems critical for the target systems. Contour will perform routine vulnerability scans of the Contour Area intended to identify critical risk areas for the systems it uses to deliver the IaaS service. Critical vulnerabilities will be addressed in a commercially reasonable manner.
- c. **Customer is responsible for:**
 - (1) Information security measures to protect the networks, information systems, data, content or applications in the Customer Area, including without limitation any patching, security fixes, encryption, access controls, roles and permissions granted to Customer’s internal, external, or third-party users;
 - (2) Network security measures to protect the networks, including software defined networks, within the Customer Area, including measures such as maintaining effective firewall rules, exposing communication ports only as necessary to conduct business, preventing and promiscuous access.
 - (3) Monitoring for potential security events in the Customer Area.
 - (4) Security monitoring and response for the Customer Area, including detecting, classifying, and remediating all security events in the Customer Area, through the use of such measures as vulnerability scanning tools or monitoring tools, or that are required for Customer’s compliance or certification program; and
 - (5) Identifying and remediating compromised virtual environments within the Customer Area and resolving all related issues. Contour reserves the right to suspend all or any portion of the Service Offerings if compromised environments are detected by Contour to protect Contour’s infrastructure and business operations.
- d. Customer is required to utilize a reputable anti-virus program to protect the Customer Area, which must be running, up to date, and properly configured.

11. Offline Data Transfer Service

- a. Offline Data Transfer is an optional data migration service for the purpose of transferring large numbers of virtual machines, virtual apps, or templates from your local private environments to the Contour Cloud. These migration capabilities support onboarding to the Contour platform, export from the Service Offering, and synchronization of templates between the Contour platform and Customer’s on-premises data centers.

- b. Contour will provide:**
 - (1) A physical storage device shipped to Customer; and
 - (2) After the device is received back by Contour, the transfer of data from the device into Customer's Service Offerings.
- c. Customer is responsible for:**
 - (1) Following the documentation accompanying the storage device.
 - (2) Returning the storage device by Customer's preferred carrier at Customer's expense to Contour within 45 calendar days from Contour's date of shipment.
 - (3) Backing-up and encrypting any data, applications, virtual machines, or other content transmitted via the service.
- d.** Contour will not be responsible for any data loss or any other loss or damage that may occur as a result your use of the Offline Data Transfer service. If any Contour storage device is not received by Contour in equivalent working condition within 45 days from Contour's date of shipment, Customer will pay Contour a replacement fee for any such storage device plus any shipping and handling charges, as each will be assessed by Contour. Customer's use of the Offline Data Transfer service is entirely at Customer's own risk.

12. Direct Connect

- a.** Direct Connect is an optional dedicated networking link that helps connect remote customer data centers, and those in the same facility as Contour, to customer instances in Contour environments. Direct Connect enables customers to leverage high-output and low-latency connections provided by a network service provider. The dedicated connection circuit will consist of the Direct Connect service (which is provided by Contour) and the network connection and service from the customer site into the Contour data center (which is provided by your chosen network service provider, who must have a point of presence in the relevant Contour data center).
- b.** There will be separate network connection fees, for which you are responsible, assessed by your network service provider, and/or Contour.
- c.** The network service provider will provide you networking services and will assess separate fees under separate service contract terms. These separate fees and terms must be managed with your chosen network service provider, which is separate from your relationship with Contour.
- d. As part of this service, Contour will:**
 - (1) Provision, manage and support the Contour side of the connection
 - (2) Coordinate with your selected network service provider to ensure successful circuit provisioning and connection from your Contour instance to the network service provider's point of presence in the relevant Contour data center(s).

13. P2P Connections

- a.** Contour will work with your carrier, or our carrier to provide P2P connections from your infrastructure to the Contour cloud.
- b. You will be responsible for:**
 - (1) Contracting with a network service provider for all private network service connectivity unless you have agreed to have Contour manage the service.
 - (2) Complying with all applicable terms and conditions of the network service provider
 - (3) Providing all applicable network service provider circuit information to Contour Support that is required for provisioning completion.

- (4) Contour will not be responsible for any network connectivity outage that occurs on the network service provider's side of the connection. Contour's Global Privacy Addendum applies in respect of data processed on Contour infrastructure controlled by Contour but not the network connection and service provided by your chosen network service provider

14. Metered Usage

- a. Metered Usage components for Virtual Private Cloud, such as Bandwidth and third-party licenses are available for consumption in excess of subscription levels at any time within the Service Order Form. You are obligated to pay for such Metered Usage components at the then-current rates published by Contour. Such charges will be billed by Contour as agreed upon. A list of Metered Usage components is provided in Appendix A.
- b. Capacity may be added via the Change Request Form or Service Order Form
- c. All Private & Public Cloud On-Demand and SaaS components are considered metered usage.

Appendix A

Ordering and Metered Usage Components

This Appendix A to the Service Description outlines the components that may be purchased by the Customer during the initial or subsequent orders and the components that will be billed based on actual usage.

Definitions

Term	Definition
Bandwidth	The network connectivity from your Contour cloud platform to the public Internet using Contour’s Internet service providers.
Billing Date	The date when Contour will periodically bill for the Service Offering. Billing Dates will occur monthly unless otherwise indicated.
Billing Period	The period for which the Service Offering is being billed. Billing Periods are monthly and are related to the provisioning of your SID, unless otherwise indicated.
Burst Bandwidth	The amount of Bandwidth consumed by you in excess of the bandwidth purchased with your Core Components for Virtual Private Cloud
Compute	The allocated virtual processing and virtual memory resources provided to you through your purchased class of service. Compute is ordered in the increments defined below for Public Cloud, Private Cloud, Hybrid Cloud, and Disaster Recovery.
Core Components	Compute, Storage, Bandwidth, IP Addresses and Support for Public Cloud, Private Cloud, Hybrid Cloud, and Disaster Recovery.
Database Size	The size of the SQL database instance provisioned based on CPU and RAM allocation.
Database Storage	The primary SQL database storage, including data files, log files and temp file space.
Elastic Compute	The unreserved virtual processing and virtual memory resources utilized by you during the Billing Period for Public Cloud, Private Cloud, Hybrid Cloud, and Disaster Recovery.
IP Addresses	Used to provide connectivity to the public Internet and Bandwidth is consumed when data is either transferred or received by your Service Offering instance.

Master Service Agreement (MSA)	The actual executed contract agreed upon between you and Contour.
Metered Usage Components	Service Offering elements that are billed based upon actual usage, including any usage in excess of the committed Plan Charges. Metered Usage Components are listed below.
Offline Data Transfer (ODT)	A data migration service where a physical storage device is shipped to you and then returned to Contour for the purpose of transferring large numbers of VMs, vApps, or templates from your local environment to your Contour cloud environment.
Peer-to-Peer (P2P)	A peer-to-peer (P2P) network is created when two or more PCs are connected and share resources without going through a separate server compute.
Plan Charges	Service Offering components that are not billed based upon usage (i.e., those components that you have committed to purchase and are recurring during the subscription term without regard to use). These charges will be invoiced for the then-current Billing Period.
Recovery Storage	The SQL storage of database snapshots and PITR (point in time recovery) backups.
Service Order Form (SOF)	A document listing the cost of each of the services and products you have purchased through Contour.
Statement of Work (SOW)	Outlines the requirements for the products and services Contour will provide.
Storage	Contains block level storage volumes surfaced to you through your purchased class of service. Storage is ordered in the increments defined below or is allocated from within the service.
Subscription Software	Any software provided to you and for which you are billed for its use.
Third-Party Licenses	Licenses for third-party software that are made available to you as optional services (either through the Contour or otherwise).
UOM	The Unit of Measure for measuring usage for billing purposes.
Usage Charges	The service fees for those Service Offering components that are billed based upon usage. These charges will be invoiced.
Failover Test	The act of performing a simulated failover and recovery exercise as part of the Disaster Recovery service and applies whenever one or more virtual machines is included in the test workflow.

Daily Usage Fee	The extra cost associated with operating any virtual machines that have been failed over or recovered under the Disaster Recovery service for longer than the allowed runtime lease.
Runtime Lease	The amount of time (measured in days) that applies to how long a virtual machine can be operational as part of the Disaster Recovery service.

Revision History

Contour Data Solutions Public Information					
Type	Title	Date	Version	Description of Changes	Author
Addendum	Infrastructure as a Service	05/05/2020	1.0	Initial Draft	Rocco Guerriero
Addendum	Infrastructure as a Service	06/03/2020	1.0	Final Release	Rocco Guerriero
Addendum	Infrastructure as a Service	06/08/2020	2.0	Complete review	Rocco Guerriero
Addendum	Infrastructure as a Service	06/08/2020	2.0	Organizational Format / Layout Changes	Rocco Guerriero