Infrastructure as a Service (IaaS)

Service Description

Last Updated: May 18, 2018

Contour Data Solutions, LLC.
4259 West Swamp Road, Suite 301
Doylestown, PA 18902
www.contourds.com

Contents

1. Introduction

Contour Cloud Infrastructure as a Service (IaaS) is a group of secure cloud service offerings operated by Contour Cloud, giving IT organizations a platform to extend their cloud infrastructure and software deployments seamlessly beyond their data centers.

1.1 Contour Cloud

Contour Cloud is owned and operated by Contour Data Solutions. Contour Cloud is built on enterprise grade platforms and deployed across four data centers in North America. Contour Cloud provides consistent networking and security for applications running on-premise or in the cloud. Our platform utilizes a single management console, *Cinch*, and a common application programming interface. Contour Cloud offers numerous benefits including:

- **Micro-Segmentation Security Policies** Contour Cloud provides control over East-West traffic between native workloads running in private and public clouds. Security policies are defined once and applied to workloads. These policies are supported in multiple, regions and support a multi-cloud strategy. Policies are dynamically applied based on a rich set of constructs, such as workload attributes and user-defined tags. Rogue or compromised workloads can also be automatically quarantined.
- **Network Control and Portability** Contour Cloud provides consistency and control over network policies, while also offering portability. Precise control is given over networking topologies and addressing, providing capabilities such as stretching subnets across availability zones. Provisioning and management of networking and security policies across cloud accounts can be greatly simplified and standardized through the use of templates.
- **Increased Visibility Across Clouds** Contour Cloud improves visibility and analytics for native workloads in the cloud using existing and familiar network management tools.
- **Consistent operations** Contour Cloud brings a standardized and consistent operational model to applications running natively in public clouds. A single management console and common APIs allows cloud teams to simplify their operations and scale across a growing number of public cloud environment leveraging existing automation tools. Existing Day 2 operations tools can be used to provide end-to-end monitoring, troubleshooting and auditing.

1.2 *CINCH*

CINCH is Contour Cloud's proprietary automation platform, enabling self-service to easily create, modify and manage all of your infrastructure and cloud data. ***CINCH*** makes it easy to find information, manage your account and instantly connect with your Contour team. ***CINCH*** components include:

- ***CINCH* Dashboard** provides a quick overview of your entire account. Instantly view all recent activity, including bills, reports and tickets.
- ***CINCH* Solutions Center** provides real-time status of your active components, ability to manage your components and add additional components on the fly.
- ***CINCH* Management Center** provides details on your individual Contour Cloud instances including IP addresses, hardware specs, inventory items, bandwidth usage and scale optimizer to set rules for potential traffic spikes.
- ***CINCH* Security Center** provides you the insight to see all your security patches and KPI data
- **Contour Cares Support** provides updates on existing tickets and gives you the ability to open new tickets and contact our support team.
- ***CINCH SLAs*** provides real-time insight into your systems and whether or not Contour is hitting our agreed upon SLAs.

1.3 Technical Documentation and Training

An on-boarding process may be provided for all of our clients when requested. Documents, training and hand-on training outlining key concepts with usage examples are available.

1.4 Legal Terms

Use of the Contour Service Offerings is subject to the Terms and Conditions of the Master Managed Services Agreement (MMSA) Service Support

1.5 Service Support

Contour Cloud Network Operations Center (NOC) will provide support for problems that you report, related to our cloud offerings. The NOC can be reached via the Cinch Portal. Support will be provided to any client with an active subscription.

2. Contour Cloud IaaS Service Options

Contour Cloud Infrastructure as a Service (IaaS) offering has three types of service:

- **Virtual Machines** service provides multi-tenant, pay-as-you-go, virtual servers that can be created and managed individually through the Contour *Cinch* Portal.
- **Virtual Data Center (VDC)** service provides a private, reserved, virtual data center, with logically-isolated resources on shared physical infrastructure, configured as a single virtual data center with access to configure advanced networking services.
- **Dedicated Private Cloud (DPC)** service provides a single-tenant private cloud with dedicated computing servers, layer 2 network isolation for workload traffic, dedicated storage volumes, and dedicated cloud management instances. Infrastructure capacity may be allocated to a single virtual data center or to multiple data centers.

2.1 Service Objects

Each type of service includes the capability to access these objects and manage them to align with different consumption and administrative models:

- **vCPU** stands for virtual central processing unit. One or more vCPUs are assigned to every Virtual Machine within a cloud environment. Each vCPU is seen as a single physical CPU core by the VMs operating system.
- **vRAM** stands for virtual random-access memory. In a virtualized computing environment, physical memory is partitioned into virtualized physical memory. Virtual memory management techniques are used to allocate additional memory to a virtual machine. Virtual RAM (vRAM) is the amount of RAM that a hypervisor allocates to a virtual server.
- **Storage** scalable, cost-effective, and resilient cloud-based storage that can be managed through the Contour *Cinch* Portal.
- **Virtual Machine (VM)** first class objects in the Contour Cloud; they may be created and managed individually. Virtual Machines can be created and managed through the Contour *Cinch* Portal.
- **Networks** may be managed through the Contour *Cinch* Portal for edge gateway configuration and common use case such as NAT mappings, firewalls rules, and VM-to-network assignment. Advanced

settings configuration and management such as VPN setup, load balancing and network creating can also be done through the Contour *Cinch* Portal.

3. Service Operations

The following outlines Contour's roles and responsibilities in the delivery of the IaaS. While specific roles and responsibilities have also been identified as being owned by you, any roles or responsibilities not contained in this document are either not provided with the service or assumed to be your responsibility.

3.1 Service Provisioning

Contour may provide the following provisioning services:

- Implementation of service objects (physical servers, physical storage and physical network devices) needed to support contracted resource pools.
- Providing initial network resources including default Public IP address.
- Providing initial resource pools (memory, processing, primary storage, and networking) when applicable.
- Creating the initial administrative user accounts in the Contour Cloud *Cinch* portal.

Customer will be responsible for the following provisioning services:

- Providing corporate resource assistance for establishing site to site connectivity.
- Creating user accounts in the Contour Cloud *Cinch* portal, and changing default system preferences as needed.
- Creating and configuring applicable Virtual Machines, Virtual Data Centers and Dedicated Private Clouds using deployment templates.
- Installing and configuring customer or third-party applications and operating systems on deployed cloud service options.

3.2 Data Recovery

Contour may provide the following services with respect to data recovery:

- Data protection, such as routine backups, for the Contour Cloud infrastructure, including top-layer management and user-management interfaces owned and operated by us.
- Data and infrastructure restoration for the Contour Cloud infrastructure, including top-layer management and user-management interfaces owned and operated by us.

You will be responsible for the following services with respect to data recovery:

- Data protection, such as routine backups, for the data and content accessed or stored on the Contour Cloud VMs or storage devices, configuration settings, etc.
- Data content, VM, and configuration restorations for assets accessed or stored on your Contour Cloud account.

3.3 Monitoring and Management

Contour may provide the following services with respect to Monitoring:

- Monitoring the Contour Cloud infrastructure, infrastructure networks, top-layer management and user-management interfaces, and computing, storage, and network hardware for availability, capacity, and performance. We will also provide you with a VDC and VM level view of compute and storage resource utilization and availability.

Customer will be responsible for the following services with respect to Monitoring:

- Monitoring the assets deployed or managed within your Contour Cloud instance, including, but not limited to virtual machines, operating systems, applications, specific network configurations, operating systems or application vulnerabilities, etc.

3.4 Incident Response and Problem Management

Contour may provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Infrastructure over which Contour has direct, administrative, and/or physical access and control, such as Contour Cloud servers, storage and network devices.
- Service software over which Contour has direct administrative access and control, such as the Contour Cloud *Cinch* Portal.
- Contour-provided operating system templates to the extent that:
    - Published templates cannot be accessed
    - Published templates cannot be instantiated without modifications
    - Published templates cause errors at first run time
    - There are substantial hangs or excessive delays in the retrieval of a template
    - The configuration of a published templates affects the virtual machines interaction with the hypervisor
    - Time synchronization issues (NTP) exist.
- Contour provided tools, including:
    - Contour Cloud *Cinch* Portal

Customer is responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Your organization network administration, configuration, and modification.
- User-deployed and configured assets such as VMs, custom developed or third-party applications, custom or user-deployed operating systems, network configuration settings, and user accounts.
- Operating system administration including the operating system itself or any features or components contained within it.
- VPN integration.

- Performance of user-deployed VMs, 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 the Contour Cloud Console, Contour Cloud Desktop Portal, or Contour Cloud service.

3.5 Change Management

Contour may provide the following change management elements:

- Processes and procedures to maintain the health and availability of the Contour Cloud *Cinch* Portal or Contour Cloud service components. Please see the Service Level Agreement for maintenance schedules.
- Processes and procedures to release new code versions, hot fixes, and service packs related to the Contour Cloud *Cinch* Portal, or Contour Cloud service components.

Customer is responsible for:

- Management of changes to your VMs, operating systems, custom or third-party applications, and administration of general network changes within your control.
- Administration of self-service features provided through the Contour Cloud *Cinch* Portal, up to the highest permission levels granted to you. Including but not limited to VM and domain functions, and general account management, etc.
- Cooperating when planned and emergency maintenance is required.

3.6 Security

The end-to-end security of Contour Cloud is shared between Contour and you. Contour will provide security for the aspects of the service over which it has sole physical, logical, and administrative level control. You are responsible for the aspects of the service over which you have administrative level access or control. The primary areas of responsibility between Contour and you are outlined below.

Contour will use commercially-reasonable efforts to provide:

- **Physical Security:** Contour will protect the data centers housing IaaS from physical security breaches.
    - **Equipment Location:** Contour Cloud operates in the Unites States. A site selection team determines each data center site. The site selection process includes a rigorous assessment, ensuring that each site has appropriate measures and countermeasures in please.
    - **Data Centers:** We use well-established data center providers to host workloads. Each data center is certified SSAE16. The providers are reviewed by independent third-party auditors to meet the physical security requirements for SOC 1 Type 2/SSAE16 and SOC 2 Type 2. Full reports outlining these specifications are available, upon request, subject to execution of an appropriate confidentiality and nondisclosure agreement.
- **Information Security:** Contour will protect the information systems used to deliver IaaS for which it has sole administrative level control.
- **Network Security:** Contour will protect the networks containing its information systems up to the point where you have some control, permission, or access to modify your networks.

- **Security Monitoring:** Contour will monitor for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of IaaS for which it has sole administrative level control over. This responsibility stops at any point where you have some control, permission, or access to modify an aspect of the Service Offering.
- **Patching & Vulnerability Management:** Contour will maintain the systems it uses to deliver the Service offering, including the application of patches it deems critical for the target systems. Contour will perform routine vulnerability scans to surface critical risk areas for the systems it uses to deliver the Service Offering. Critical vulnerabilities will be addressed in a timely manner.
- **PCI Compliance:** If an environment is identified as PCI compliant, we will enforce Level 1 PCI compliance at the infrastructure level. This includes the security posture, patching, logging, and audit requirements for the Contour Cloud IaaS offering (compute, network, and storage).
- **HIPAA Compliance:** If an environment is identified as HIPPA compliant, we will enforce Level 1 HIPPA compliance at the infrastructure level. This includes the security posture, patching, logging, and audit requirements for the Contour Cloud IaaS offering (compute, network, and storage).

Customer should address:

- **Information Security:** You are responsible for ensuring adequate protection of the information systems, data, content or applications that you deploy and/or access on IaaS. This includes, but is not limited to, any level of patching, security fixes, data encryption, access controls, roles and permissions granted to your internal, external, or third-party users, etc.
- **Network Security:** You are responsible for the security of the networks over which you have administrative level control. This includes, but is not limited to, maintaining effective firewall rules, exposing communication ports that are only necessary to conduct business, locking down promiscuous access, etc.
- **Security Monitoring:** You are responsible for the detection, classification, and remediation of all security events that are isolated with your IaaS account, associated with VMs, operating systems, applications, data, or content, surfaced through vulnerability scanning tools, or required for a compliance or certification program in which you are required to participate and which are not serviced under another Contour security program.

3.7 Storage

Contour Cloud includes block storage as a part of the core subscription. There are two storage options available with a Dedicated Private Cloud and Virtual Data Center instance: Standard Storage and SSD-Performance Storage. These two storage options allow for (1) growth of virtual machine disks (VMDKs) without downtime, and (2) the flexibility to migrate from one tier to the other as needed. You can also mix and match storage types per workload as needed.

3.8 Networking Services

The service offerings include the following network services as part of the core Dedicated Private Cloud and Virtual Data Center cloud subscription offerings:

- **Network Address Translation (NAT):** Separate controls for source and destination IP addresses, as well as port translation.
- **Dynamic Host Configuration Protocol (DHCP):** Configuration of IP pools, gateways, DNS servers, and search domains.
- **Firewall:** Next Generation Firewall
- **Load balancing:** Simple and dynamically configurable virtual IP addresses and server groups.
- **Site-to-Site Virtual Private Network (VPN):** Uses standardized protocol settings to interoperate with all major VPN vendors.
- **Static Routing:** Static routes for destination subnets or hosts.
- **Dynamic Routing:** This feature is available if you subscribe to the Direct Connect offering.
- **High Availability:** High availability ensures an active Edge on the network in case the primary Edge VM is unavailable.
- **Syslog Export:** Support for syslog export for all services to remote servers.

You may also subscribe to optional add-ons—Advanced Networking Standard or Advanced Networking Premium:

- **Distributed Firewall:** Distributed Firewall is a hypervisor kernel-embedded firewall that provides visibility and control for Contour Cloud workloads and networks. It delivers close to line rate throughput to enable higher workload consolidation on physical servers. It is available only with a Dedicated Private Cloud Subscription that includes the Advanced Networking Standard or Advanced Networking Premium add-on.

3.9 Migration

Contour can perform migration of VMs and templates between the Contour Cloud and other environments, such as data centers or evaluation environments. Export, transport and import can be supported in multiple different formats including Physical Servers, VMWare (all) and the Open Virtual Machine Format (OVF). Offline Data Transfer services are also available for migration on request.

In addition to the basic network-based operations of machines being imported the following use cases are supported:

- Extend a single layer-2 network from your private VMware environments to the Contour Cloud so you can migrate VMs while retaining the same MAC address. This allows those VMs to communicate with other VMs in the private vSphere or vCloud Director environments.

- Synchronize your Contour Cloud catalog with your private VMware catalog so that all authorized users or your private VMware environment use the same templates.

3.10 Hybrid Cloud Manager (Optional)

If you have a Dedicated Private Cloud subscription, Contour Cloud offers a seamless option for extending your on-premises network to the cloud by creating an optimized, software-defined WAN to increase stretched network performance, enabling networks to stretch in the cloud yet perform almost as if they were

local. Hybrid Cloud Manager also enables bi-directional migration of workloads as well as the migration of NSX security policies to Contour Cloud Advanced Networking services.

With Hybrid Cloud Manager, you will have the following capabilities:

- Zero or low downtime migration between on-premises data center(s) and Contour Cloud
- Accelerated migration for improved performance
- Network extension using Contour Cloud's L2VPN-based extension feature, so you can stretch multiple L2 segments in one tunnel from on-premises vSphere environment(s) to Contour Cloud, so VMs can migrate to Contour Cloud while retaining the same IP and MAC address
- High performance network extension for increased network throughput over Direct Connect
- NSX distributed firewall policy migration – enables the Disaster Recovery Service for a Dedicated Private Cloud and allows all replication traffic through Hybrid Cloud Manager Cloud Gateway service for higher throughput performance.

You may subscribe to Hybrid Cloud Manager Standard, Hybrid Cloud Manager Advanced, or Hybrid Cloud Manager Enterprise.

- Hybrid Cloud Manager Standard provides a 100 Mbps connection per vCenter Server
- Hybrid Cloud Manager Advanced provides a 1 Gbps connection per vCenter Server
- Hybrid Cloud Manager Enterprise provides a multi Gbps connection per vCenter Server

3.11 Offline Data Transfer Services (Optional)

Offline Data Transfer ("ODT") is an optional data migration service for the purpose of transferring large numbers of VMs, vApps, or templates from your local private vSphere or vCloud Director environments to your Contour Cloud environment. ODT may be procured through Contour, and you will use vCloud Connector to invoke the service.

As a part of this service, Contour can:

- Ship a physical storage device to you, permitting you to load VMs, vApps, or templates onto the device and ship it back to us using your preferred carrier. The content that you load onto the device will be encrypted. The decryption key is stored in the Contour Cloud's *Cinch* Portal, thereby ensuring security of your content during transfer.
- Transfer the data from the device into your Contour Cloud instance

Customer will be responsible for:

- Following the instructional documentation accompanying the storage device.
- Returning the storage device to us within 30 calendar days from the date of shipment. If the storage device is not returned within the 30-day period, you will pay us a replacements fee for the storage device plus any shipping and handling, as assessed by us.
- Backing up any data, applications or VMs transmitted via the service; we will not be responsible for any data loss that may occur as a result your use of this service.

This optional service may be subject to additional fees as further described in the Appendix A of this Service Description.

3.12 Data Protection (optional)

Data Protection is an optional service that provides secure, image-based backup and recovery capabilities that enable you to protect important VM data and content hosted in your Contour Cloud environment. Through the Data Protection administration interface available in the Contour Cloud *Cinch* Portal, VM members can be selected for policy-based backup and recovery operations.

Data Protection feature subscription and activation may be requested via Contour Cloud *Cinch* Portal and is subject to additional service fees based on the amount of backup data capacity. Backup data capacity for the service is measured in front end terabytes (FETB) and is described further in Appendix A of this Service Description. Once activated, VM members may be registered and unregistered with Data Protection features on a self-service basis through the Contour Cloud *Cinch* Portal.

As part of this service, Contour may:

- Implement and maintain central service components (backup software appliances, backup and archival storage media and associated network topologies) needed to support Data Protection features.
- Perform routine configuration, maintenance, and optimization services on behalf of the Data Protection environment and in conformance with industry best practices.
- Allocate requisite backup storage based on capacity selections made at the time of subscription enrollment.
- Guarantee storage locality per geographical region for all backup data.
- Provide necessary Data Protection service reporting as requested.

You will be responsible for:

- Subscribing to Data Protection as an add-on feature via Contour Cloud *Cinch* Portal and selecting an amount of backup storage capacity commensurate with your requirements.
- Creating custom backup protection policies that may include, but are not limited to: affinity settings per VDC, scheduling, and retention periods.
- Registering and unregistering individual VM members for scheduled backups using Data Protection.
- Performing any on-demand backups per VM members.
- Performing in-place or out-of-place restores per individual VM.
- Managing any in-guest recovery tasks, including restore operations at the operating system, file systems and/or any application level.
- Managing backup storage capacity and consumption that may include, but is not limited to:
    - Activity reporting, ordering additional storage capacity via Contour Cloud *Cinch* Portal and deleting any backup data in inventory to free up space.

3.13 Direct Connect (optional)

Direct Connect is an optional dedicated networking link that helps connect your remote data centers, and those in the same facility as Contour Cloud, to your instances in Contour Cloud environments. Direct Connect enables you to leverage high-throughput and low-latency connections provided by a network service provider. The dedicated connection circuit will consist of (1) the Contour Cloud Direct Connect service (which is provided by us) and (2) the network connection and service from your site into the Contour Cloud data

center (which is provided by your chosen network service provider, who must have a point of presence in the relevant Contour Cloud data center).

The Contour Cloud Direct Connect service is available in two versions:

- Direct Connect with Cross Connect: available in all Contour Cloud data centers.
- Direct Connect for Network Exchange: available in select Contour Cloud data centers. This version allows for faster provisioning of the service and connection redundancy when used with validated partners.

Your Direct Connect subscription will only include the port connection service from your chosen network service provider's point of presence in the Contour Cloud data center to your Contour Cloud instance.

Your network service provider will provide networking services and will assess fees (for which you are responsible) under separate service contract terms. These separate fees and terms are separate from your relationship with us.

As part of this service, we will:

- Provide either a 10 Gbps or 1 Gbps connection into Contour Cloud, to which a customer-contracted circuit or connection can be linked.
- Provision, manage, and support the Contour Cloud side of the connection.
- Coordinate with your selected network service provider to ensure successful circuit provisioning and connection from your Contour Cloud instance to the network service provider's point of presence in the relevant Contour Cloud Air data center(s).

You will be responsible for:

- Contracting with a network service provider for all private network service connectivity.
- Complying with all applicable terms and conditions of the network service provider.
- Providing all applicable network service provider circuit information to Contour Cloud that is required for provisioning completion.

We will not be responsible for any network connectivity outage that occurs on the network service provider's side of the connection. Our Data Privacy Addendum applies to data processed on the Contour Cloud infrastructure controlled by us, but not to the network connection and service provided by your chosen

3.14 Object Storage (optional)

Contour Cloud Object Storage is an optional service that provides a scalable, cost-effective, and resilient cloud-based storage solution for unstructured data. The service allows customers to gain instant self-service access to storage capacity, on demand, and scale up as needs expand.

Contour Cloud Object Storage exposes an S3-compatible interface that allows applications programmed from Amazon S3 to work similarly with the Contour Cloud as the object storage provider.

Today's companies must securely collect, store and analyze their data on a large scale. Contour Cloud Object Storage is built to retrieve and store any amount of data from anywhere in the world, using any application. The provided S3-compatible interface means that you have the most supported cloud storage service

available, with integration from the largest community of third-party solutions and systems integration partners.

- The AWS Storage Gateway helps you build hybrid cloud storage, augmenting your existing local storage environment with the durability and scale of Amazon S3. Use it to burst a workload from your site into the cloud for processing and then bring the results back. Tier colder or less valuable data off of your on-premise storage into the cloud to reduce costs and extend your storage investment. Or simply use it to incrementally move data into S3 as a part of backup or migration projects.

Contour Cloud Object Storage feature subscription and activation may be requested via *Cinch*, and is subject to additional service fees based on the amount of storage, network egress, and transactions.
Once activated, the service can be controlled and consumption monitored in real time through Contour Cloud *Cinch* portal with data being fed through the S3-compatible service.

As part of this Service Offering, Contour may:

- Implement and maintain all central service components (such as billing and metering, and identity and access management) needed to support Object Storage features.
- Perform routine configuration, maintenance, and optimization services on behalf of the Object Storage service components in the Contour Cloud. All of these activities will be performed in conformance with industry best practices.
- Allocate requisite object storage capacity based on your requests for the appropriate type of storage.
- Guarantee storage locality per geographical region selected for all object storage data.

You will be responsible for:

- Subscribing to Object Storage powered by Contour Cloud, as an add-on feature, via *Cinch*.
- Creating and maintaining service accounts for Object Storage.
- Creating and managing buckets and objects on Object Storage.
- Managing Object Storage capacity and consumption that may include but is not limited to activity reporting, and managing creation and deletion of buckets and objects.
- Upon termination of your Contour Cloud account, deleting the associated buckets and objects in order to prevent being billed for the buckets and objects created by you.
- Submitting any billing claims within 60 days of the issuance of the bill.