

# Disaster Recovery as a Service (DRaaS)

## Service Description

Last Updated: May 18, 2018

The information in this document may not be reproduced in whole, or in part, nor may any of the information contained therein be disclosed without the prior consent of Contour Data Solutions (Contour). A recipient may not solicit, directly, or indirectly, (whether through an agent or otherwise) the participation of another institution or person without the prior approval of Contour.

No representation, warranty, or undertaking expressed or implied, is, or will be made, or given. No responsibility or liability is, or will be accepted by Contour, or by any of its directors, employees, or advisors in relation to the accuracy or completeness of this document, or any other written or oral information made available in connection with this document.

Any form of reproduction, dissemination, copying, disclosure, modification, distribution and or publication of this material is strictly prohibited.

Contour Data Solutions, LLC.  
4259 West Swamp Road, Suite 301  
Doylestown, PA 18902  
[www.contourds.com](http://www.contourds.com)

## Contents

<b>1. Introduction</b> .....	<b>4</b>
1.1 Contour Cloud.....	4
1.2 CINCH.....	4
1.3 Technical Documentation and Training.....	5
1.4 Legal Terms.....	5
1.5 Service Support.....	5
<b>2. Contour DRaaS Service Options</b> .....	<b>5</b>
2.1 Service Objects .....	5
<b>3. Service Operations</b> .....	<b>6</b>
3.1 Service Provisioning.....	6
3.2 Monitoring and Management .....	6
3.3 Service Offering .....	7
3.4 Change Management .....	8
3.5 Security .....	8
3.6 Scenarios.....	9
Scenario 1: Replica Copy.....	9
Scenario 2: Real Time Replication .....	10
3.7 Optional Services .....	10

# 1. Introduction

Contour Cloud Disaster Recovery Service is a managed service that enables you to rapidly recover your data and systems in the Contour Cloud upon declaring a disaster. We guarantee your recovery times, and back them with your choice of a 4-hour, 24-hour, or Custom Service Level Agreement (SLA). Contour will help manage the planning, testing, and, if disaster strikes, execution of your DR processes. All you need is a computer and an Internet connection to remotely access your recovered systems and data from our secure, purpose-built cloud.

## 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.
- **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).

### 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 DRaaS Service Options

Contour Cloud Disaster Recovery as a Service (DRaaS) offering has two types of service:

- **Replica Copy** service provides secure, *image-based backup and recovery* capabilities that enable you to protect important virtual and physical workloads by replicating to and recovering in the Contour Cloud.
- **Real Time Replication** service provides *continuous replication* to the Contour Cloud for mission critical workloads. Workloads are replicated to performance storage with guaranteed compute, memory and storage. Service Level Agreement are defined by Recovery Time Objective (RTO).

### 2.1 Service Objects

All Service offerings includes the capability to access these objects and manage them to align with different consumption and administrative models:

- **Backup Software** image-based backup and recovery for virtual and physical workloads
- **Replication Software** continuous replication for all workloads
- **Virtual Machine (VM)** Virtual Machines can be created and managed through the Contour Cinch Portal on an individual basis.
- **Virtual Data Center (VDC)** provides secure, multi-tenant virtual data center with both physical and logically-isolated resources, configured as a single virtual data center with networking resources.
- **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.

- **Storage** scalable, cost-effective, and resilient cloud-based storage.
  - **High-Performance Storage (Tier 1)**
  - **Standard-Performance Storage (Tier 2)**

### 3. Service Operations

The following outlines Contour's roles and responsibilities in the delivery of the DRaaS. 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 (backup and/or replication software, CPU, RAM, Storage, and network) needed to support contracted resource pools.
- Providing initial network resources including default Public IP address. (One Public IP included in Standard and Premium offering. Additional IPs available)
- Enabling a secure point to point network interconnect (a.k.a. backhaul) via VPN or MPLS from the Contour Cloud network to your corporate network (Primary and Secondary site). Note MPLS is purchased separately from your ISP. MPLS Direct Connect will have an additional monthly charge.
- Creating the initial administrative user accounts in the Contour Cloud Cinch portal.
- Providing access to self-service DR bubble testing.

Customer will be responsible for the following provisioning services:

- Providing corporate resource assistance for establishing DRaaS requirements.
- Providing complete list of systems included in the DRaaS offering. List includes system name, CPU, RAM and Storage requirements, RPO/RTO requirements.

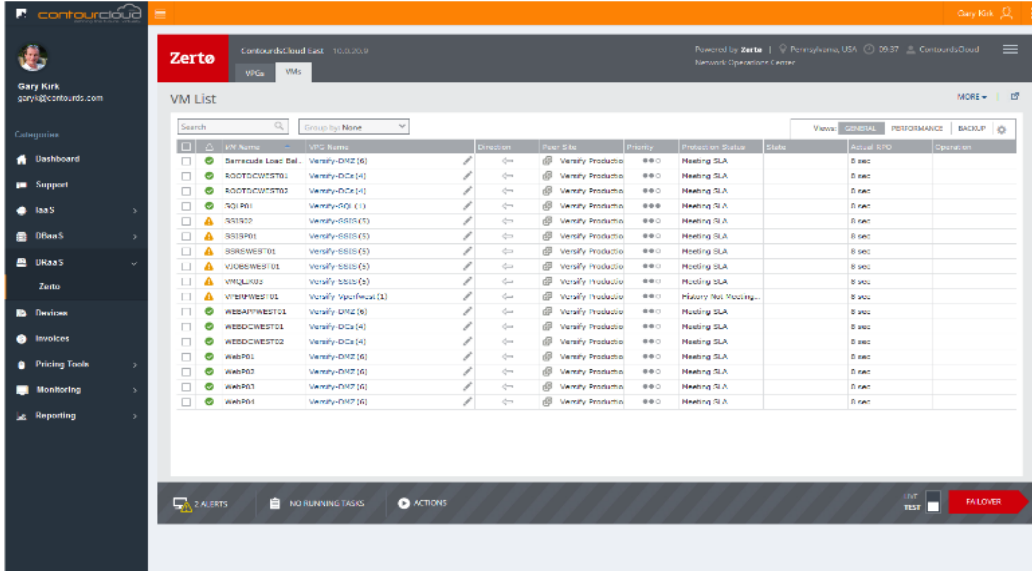
#### 3.2 Monitoring and Management

Contour may provide the following services with respect to Monitoring:

- Monitoring and Management of the Contour Cloud DRaaS infrastructure, infrastructure networks, top-layer management and user-management interfaces, and compute, storage, and network hardware for availability, capacity, and performance.
- Daily monitoring and management of the replication process to ensure all necessary data is replicated to the Contour Cloud in a consistent state acceptable for recovery in a disaster.
- Daily health checks with identification of trends including growth and disaster recovery readiness
- Support in a failover scenario to spin data up in the Contour Cloud help bring data back from the cloud to either the production site or the Contour Cloud.

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

- Monitoring and Managing the assets deployed or managed within your Contour Cloud instance, including, but not limited to virtual machines, operating systems, applications, MPLS / VPN, or application vulnerabilities, etc.



VM Name	VPC Name	Direction	Peer Site	Priority	Protection Status	State	Actual RTO	Operation
Barracuda Lead Mail	Verify-DH2 (6)	↔	Verify Production	***	Heating SLA	0 sec		
R007DC0U75760	Verify-DH2 (4)	↔	Verify Production	***	Heating SLA	0 sec		
R007DC0U75760	Verify-DH2 (4)	↔	Verify Production	***	Heating SLA	0 sec		
SQL01	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL02	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL03	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL04	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL05	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL06	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL07	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL08	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL09	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL10	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL11	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL12	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL13	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL14	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL15	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL16	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL17	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL18	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL19	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		
SQL20	Verify-DH2 (1)	↔	Verify Production	***	Heating SLA	0 sec		

### 3.3 Service Offering

As part of this Service Offering, Contour will work with customer to provide:

- DRaaS environment with Reserved, Dedicated resources (Network, Compute, Storage)
- Customized DR Runbook that ensures every aspect of a failover and failback are documented.
- 24x7x365 access to Contour Recovery Experts
- One annual comprehensive DR test:
  - Automatic Failover settings
  - State of the VM on failover
  - Timing of RTO and Network settings
  - Test and validity of the DR Runbook
  - Network Connectivity (external testing)
  - Actual DNS changes in Production (requires access to DNS)
  - Failback
  - Recovery health
  - Replication monitoring
  - Pre- and Post-Test planning meetings
- One external IP (additional available)

Customer is responsible for:

- Subscribing to Contour Cloud DRaaS as a core subscription and selecting the amount of reserved capacity to meet your requirements.
- Ensuring the appropriate network connectivity type and bandwidth is available between your production environment and the Contour Cloud to support replication requirements.
- Configuring VMs for protection in the Contour Cloud DRaaS subscription and defining a corresponding recovery time objective per machine.
- Developing any custom runbook procedures for test, failure, recovery and failback operations.
- Implementing and executing any recovery tasks that extend beyond the scope of the Contour Cloud DRaaS Service Offering and recovery of VMs as the prime service boundary.
- Ensuring sufficient reserved capacity is available in the Contour Cloud instance to accommodate variable failover workloads.
- Managing your environment after its been recovered in the Contour Cloud.

Additional Items regarding your Contour Cloud DRaaS Service offering:

- Upon Declaring a Disaster and failing over into the Contour Cloud, you will be billed on a per VM basis, until failing back into your environment and removing your VMs from the Contour Cloud. VMs will be billed according to your reserved resource instance in the Contour Cloud.
- You may purchase additional capacity at a daily rate to satisfy short-term failover requirements that exceed original amount of failover capacity based on actual consumption.

### 3.4 Change Management

Contour may provide the following change management elements:

- Processes and procedures to maintain the health and availability of the Contour Cloud Administration Console 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 Administration Console, 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 user consoles, 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.

### 3.5 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 DRaaS from physical security breaches.
- **Information Security:** Contour will protect the information systems used to deliver DRaaS 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 DRaaS 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.

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 DRaaS. 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 DRaaS 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.

## 3.6 Scenarios

### Scenario 1: Replica Copy

This solution provides secure, image-based backup and recovery capabilities that enable you to protect important virtual and physical workloads by replicating to and recovering in the Contour Cloud. Service Level Agreement are defined by Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

## Scenario 2: Real Time Replication

This solution provides real time replication to the Contour Cloud for mission critical workloads. Workloads are replicated to performance storage with guaranteed compute, memory and storage. Service Level Agreement are defined by Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

### 3.7 Optional Services

- Virtual or Physical Active Directory Server
- Additional bandwidth
- Direct Point-to-Point circuits
- Additional Public IPs
- Monitoring and Managed Services