zuora

Disaster Recovery Policy

Version	Reviewed By	Review Date	Approved By	Approved Date	Notes
Draft	Pritesh Parekh	06/27/2014			
1.0	Alex E., Kate K, Pritesh P., Marlene S., Thomas F., Jeff D., Gail J.	9/29/2014	Marc A.	9/22/2014	
1.1	Tom C.	11/24/2014	Pritesh P.	11/24/2014	Updated RPO to 250ms
1.2	Cari L.	11/11/2015	Atif H.	11/18/2015	Minor updates, including stakeholders
1.3	Atif H.	02/23/2016	Levon S.	02/23/2016	Updated RPO to 15mins
1.4	Atif H., Justin S.	02/27/2016	Andrey K.	05/03/2016	Updated Infrastructure Capability section
1.5	Cari L.	8/1/2017	Kevin M.	8/7/2017	Update TechOps Owner
1.6	Cari L., Naveen B.	3/8/2018	Pritesh P.	3/8/2018	Update to include RevPro
1.7	Howard L., Vivek P.	7/2/2018	Pritesh P.	7/2/2018	Annual Review
1.8	Howard L., Geoff A.	7/15/2019	Bill H	7/15/2019	Update to personnel
1.9	Howard L	7/22/2020	Bill H	7/22/2020	Changed RevPro to Zuora Revenue and updated personnel information
2.0	Anu Veluri	11/09/2021	Anu Veluri	11/09/2021	Annual Review and Update to Contacts
3.0	Naveen Bidhuri, Venkat Venkataraman, Anu Veluri, Michelle Walker	06/09/2022	Anu Veluri	06/09/2022	Annual Review, which included extensive updates

Zuora Disaster Recovery Policy

Last review and/or update date: 06/09/2022

Table of Contents

1. Overview

Zuora's infrastructure provides online services for "around the clock" production operations (24x7x365), as well as disaster recovery. The disaster recovery infrastructure is designed to be able to take over 100% of the Zuora service in case of primary infrastructure failure, referred to as a disaster throughout the remainder of this document.

This policy has been designed to allow Zuora to become operational again in the event of a failure at the primary data center to another data center or region.

This policy was developed with compliance standards/regulations for HIPAA, SOC 1, SOC 2, and ISO 27001 performance criteria for recovering data from emergency or disastrous events in mind; therefore, Zuora has developed its policy to either meet or exceed the data recovery requirements of the standards/regulations identified above.

2. Objectives

The objective of Zuora's disaster recovery policy is to establish a process by which Zuora services will be restored within a timely manner to all customers in the event of a disaster. As such, Zuora has facilities set-up to meet the following recovery objectives:

- Recovery time objective (RTO) for all excluding Zuora Revenue: four (4) hours

- Recovery point objective (RPO) for all excluding Zuora Revenue: less than 15 minutes
- Recovery time objective (RTO) for Zuora Revenue: six (6) hours
- Recovery point objective (RPO) for Zuora Revenue: less than 15 minutes

In other terms, in the event of a disaster, Zuora services will not be down for more than four (4) hours for all Zuora excluding Revenue and six (6) hours for Zuora Revenue. In addition, Zuora will not lose more than 15 minutes of transactions committed by Zuora's customers. This policy will discuss further details as to Zuora's process (which includes Zuora Revenue) for declaring a disaster and procedures that will be performed to ensure the RTO and RPO identified above.

3. Declaring a disaster

A disaster would be declared in the event that Zuora's primary data center services are not available, and the recovery time is expected to be greater than four (4) hours (Zuora excluding Revenue) and six (6) hours (Zuora Revenue).

To initiate the disaster recovery plan, one Business Operations stakeholder and one Technology Operations stakeholder from the table below must vote to cutover to the recovery site.

To establish the voting process, a Priority 0 (P0) incident will be declared, and all stakeholders will be notified of this incident and invited to a virtual war room, which includes a phone/conference bridge and screen sharing capabilities. Note: The war room requirement may be suspended if physical infrastructure or other logistical issues make this impractical.

Business Operations	Technology Operations
Tien Tzuo – CEO email:	Radhi Chagarlamudi - VP, R&D Operations/Office of the CTO email:
Todd McElhatton – CFO email:	Venkat Venkataraman – VP Technical Operations email:
	Mu Yang - VP of Engineering email:
	Naveen Bidhuri – Sr. Director Revenue TechOps email:

3.1 Information Required to be Collected

To assist with the decision process of declaration of a disaster, the following must be provided to all stakeholders in order for a disaster to be declared:

- Nature and breadth of the outage. (i.e., is it isolated to a single region or environment, or does it impact a broader geographic region.)
- Confirmation that the disaster recovery site isn't also impacted by the issue. (i.e., If it's a DDOS attack that the primary data center is unable to mitigate, how do we know that disaster recovery site isn't or will also be impacted.)
- Estimate from primary Cloud provider on how long the region will be unavailable.
- Any known issues with delays in data replication that would result in the disaster recovery site being more than one (1) transaction behind.

4. Execution of disaster

Once a disaster is declared and approved, a disaster recovery operational failover process will be initiated. Below are some of the procedures in place to ensure that a failover can be executed:

4.1 Infrastructure Capability

Zuora's infrastructure is equivalent in terms of capabilities. Zuora has implemented cross data center resilience, where either data center has the capability to provide adequate operating services in case of a disaster. This ensures the ability for any infrastructure to take over 100% of the Zuora service while maintaining service levels.

Software consistency is maintained across all infrastructures as part of the software release process. Each software release or new software adoption is deployed across all environments.

4.2 Data Synchronization

Zuora maintains consistency of data across all infrastructure environments. The methods employed include but are not limited to:

1. Software release process: all software is deployed to all environments, including proprietary Zuora application code as well as packaged software installations
2. Database replication: near real time replication of database data is performed using native database replication technologies
3. File synchronization: files are copied across infrastructures using native replication tools on a frequency schedule required to meet recovery objectives

4.3 Testing and Validation

Testing is done to ensure the disaster recovery environments are up to date and all synchronization mechanisms are functioning properly.

While Zuora currently does not actively perform “full failovers” from one environment to the other, testing and validation is performed at least annually to ensure the Zuora service operates as expected, as well as data consistency remains intact.

Zuora uses lessons learned from testing the recovery of systems to update this plan so that recovery objectives can be met on an ongoing basis.

5. Procedures to Recover from a Disaster

Zuora's Technical Operations team maintains step-by-step procedures to failover from the primary data center. These procedures can be found in Zuora’s internal documentation portal (Confluence) in the TechOps space, in the DR Operational Failover and Failback page.