Disaster Recovery

Management Console, Mobile Auditor And Enterprise Intelligence

Q1 2017

rizepoint

2890 East Cottonwood Parkway, Suite 250
Salt Lake City, UT 84121
(801) 285-9810

Contents

1. Introduction

This document summarizes the disaster recovery strategy for RizePoint cloud-based software and mobile device applications. In the event that the RizePoint enterprise platform becomes unavailable for normal operations, RizePoint IT will enact its plan to reestablish operations at a designated recovery site. This document assumes a relatively high level of technological expertise and is provided to answer questions from vendors or prospective RizePoint customers.

2. Definitions

2.1 Roles and Authority

- ESO (Enterprise Security Office) – The Enterprise Security Office consists of the CTO, Director of IT, and Principal Architect. The ESO is responsible for the development of policies or procedures as they relate to the operation of the RizePoint Enterprise Platform.
- IT – The Information Technology team is led by the Director of IT and has full responsibility for the execution of policies developed by the ESO, and the day to day operations of RizePoint Technology.
- Account Executives – Account Executives are responsible for end-user communication during incidents, as well as general questions regarding the account.
- Executive Management – Executive Management including the CEO, CFO and CTO have final authority regarding policies administered by the Enterprise Security Office.

2.2 Backup Policy

RizePoint performs backups of data files from application systems. Additionally, RizePoint maintains a formal Backup Policy, which applies to all critical systems, equipment, and data owned and operated by RizePoint. This includes all machines and hardware residing within its colocation facilities. All backup data is stored on disk, with no removable media being used.

Backups are completed using a two-phase process:

Phase 1: Daily incremental backups are taken for all data and documents. Full backups are performed weekly. A third backup is performed for point-in-time data restoration. All SQL data is encrypted prior to backup process.

Phase 2: Data is replicated daily from the primary data center to offsite electronic storage with full encryption.

For further details regarding the RizePoint backup policy and procedures, refer to the "RizePoint Security Practices and Policy" document. This document is available online at http://trust.rizepoint.com or by request from RizePoint Customer Service.

3. Disaster Recovery Policy

Maintaining access 24/7/365 to RizePoint technology is the top priority of the Enterprise Security Office. As such, resiliency and redundancy are built into every layer of the application architecture. RizePoint has adopted a Pilot Light design for its Disaster Recovery Strategy. This means that backups, as well as standby images, are retained at an offsite location, but are not actively taking traffic during normal operation.

In the event that the RizePoint platform becomes unavailable under normal production, RizePoint IT will enact its plan to reestablish operations. This plan involves activating dormant virtual machines using a virtual network running Microsoft's Windows Azure Infrastructure as a Service (IaaS). For RizePoint corporate systems, the designated recovery site is the ViaWest SLC04 Data Center located at 572 Delong Street, Salt Lake City, Utah 84104.

RizePoint considers any event which causes a total disruption of operations at our primary data center a candidate for invoking our Disaster Recovery Policy.

4. Recovery Point in Time Objectives

The Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for the recovery steps referenced below assume that either Client systems or corporate systems are being restored but not both concurrently. The time to complete incremental recovery activities are stated in number of calendar hours beyond the hour of the formal declaration.

4.1 Client Implementation Systems

24 HR RPO / 120 HR RTO

RTO Day	Action Taken
Day 1	Initiate Recovery Communication Plan (Incident declaration)
Day 1	Impact Assessment complete (1-hour task)
Day 1	Backup files on cloud-based repository are converted to Virtual Machines
Day 2	All core production Virtual Machines are brought online
Day 3	Internal DNS reconfigured. All DNS entries are configured with TTLs no longer than 10 minutes so DNS application will take less than 1 hour to complete (2-hour task)
Day 4	Production environment testing occurs to verify connectivity and configuration
Day 5	External DNS is re-routed, providing Customer access to restored services.

4.2 RizePoint Corporate Systems

Should a disaster incapacitate RizePoint headquarters, email systems hosted by Office 365 will not be affected. Corporate file shares, accounting systems and other utilities are all hosted and have their own offsite disaster recovery scenarios.

5. Customer Data Recovery

In the event that individual customer data has been inadvertently deleted or corrupted, RizePoint will work with the Client to determine the type of recovery required and the data to be selected for recovery, however data recovery requests are managed by RizePoint regardless of the scope of the recovery.

The data recovery process includes the following steps:

1. RizePoint identifies most recent backup available and confirms with Client the data to be recovered.
2. The recovery method is then selected:
   a. Onsite recovery source (4-week retention)
   b. Offsite recovery source (2-year retention)
3. A RizePoint Support ticket is opened with recovery details including:
   a. Dataset to be recovered from target recovery source
   b. Target location on disk for recovery
   c. Recovery Priority (Severity)
4. RizePoint stages and monitors the recovery job progress, then verifies the recovery results and restores Client access.
5. The Client is notified that data restoration is complete.

6. Service availability during fail-over scenario

- During failover, all primary application functionality will be available, excluding Search-Driven Analytics.
- During the public cloud-hosting period, performance may be degraded in the following areas:
  - Audit result processing
  - Management Dashboards
  - Enterprise Intelligence

7. Restoration of Services to Primary Data Center

While services are being provided from a public cloud location, the RizePoint IT team will establish a new physical facility with appropriate infrastructure to restore primary services. At the appropriate recovery time, a maintenance window will be scheduled for the RizePoint platform. Changes to data from the original incident will be restored to the Primary Data Center, and infrastructure will be synced with all updates. Performance and regression testing will be performed to verify application functionality. As a final step, customer-facing URLs will be re-routed from the public cloud back to the Primary Data Center.

This restoration scenario is designed to execute without any interruption of service beyond a scheduled maintenance window.

8. Testing scenarios

RizePoint conducts periodic tests of the Disaster Recovery plan described. For documentation on the results of the most recent test, please see http://trust.rizepoint.com or contact RizePoint Customer Service.

**Note: RizePoint has enacted a new Disaster Recovery testing mechanism for use beginning in Q1 2017. Results for Disaster Recovery scenarios will be made available following these tests.*

9. Incident Management & Communication Plan

All support calls to RizePoint should be directed through RizePoint Customer Service to ensure tracking and documentation of tickets. Contact information can be found at www.rizepoint.com or at http://rizepoint.zendesk.com.

9.1 Client Outage Notification

Client communications regarding site outages (including declared disasters) are managed through RizePoint Customer Service and http://trust.rizepoint.com. In the event of a disaster declaration, Account Executives will be engaged to assist with the communication to-and-from the Client and the Recovery Team.

9.2 Disaster Recovery Plan Activation Notification

Official declarations of disaster scenarios are made by the CTO in concert with the ESO team. When the disaster recovery plan is activated by the RizePoint IT team, immediate notification will be made to all Clients affected by the outage. The notification will include details relevant to the declared event, and the course of action selected by the IT Team and Management team to restore service.

As the plan moves through its recovery points, the objective times will be provided to the Clients and the RizePoint resources will make themselves readily available for all communication to-and-from clients.

10. Conclusion

It is RizePoint's goal to be prepared for any contingency that could impede any part of the RizePoint Enterprise solution and support.

This plan is representative of RizePoint's ongoing commitment to deliver uninterrupted serviceability and reliability of the application for all users.

This Disaster Recovery document is maintained and enforced by RizePoint ESO. This document will be updated as required through regular evaluation, test feedback, or observations made through execution on any declared event.