Disaster Recovery Plan
for
AllCode

April 11, 19

Proprietary Statement

This document contains confidential and proprietary information and is the property of MobileAWS, LLC dba AllCode. This document is submitted to you in confidence, on the condition that you and your representatives have, by receiving it, agreed not to reproduce or copy it, in whole or in part, or to furnish such information to others, or to make any other use of it, and to return it to MobileAWS upon request. The previous statement shall not apply to the extent that such statement violates any federal or state laws requiring such information to be made available to the public.

In the event this document results in a contract, you may retain this document for use, including making any necessary copies related to the products and services covered by such contract.

Major Goals of This Plan

The following list contains the major goals of this plan:

- To minimize the interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

Personnel to be involved in the DR Process

Personnel			
Name	**Position**	**Telephone**	**Email Address**

Application and Inventory Profiles

AllCode runs solutions on AWS. These solutions leverage Amazons Simple Storage Service, Amazons Elastic Compute Cloud instances, Amazons Relational Database Service, Amazons Route 53, and Amazons Elastic Load Balancing Services.

Amazon Simple Storage Service (Amazon S3) provides a highly durable storage infrastructure designed for mission critical and primary data storage. Objects are redundantly stored on multiple devices across multiple facilities within a region, designed to provide a durability of 99.999999999% (11 9s). AllCode runs AWS in conjunction with CloudFront, which distributes the content redundantly across the globe

Amazon Elastic Compute Cloud (Amazon EC2) provides resizable compute capacity in the cloud. In the context of DR, the ability to rapidly create virtual machines that you can control is critical. AllCode creates primary EC2 instances in N. Virginia, and redundant instances in Oregon. Deployment code is written to roll out to instances in both regions.

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. AllCode leverages RDS in multiple regions by having a master running in North Virginia, and read replica running in Oregon.

Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. It gives developers and businesses a reliable, cost-effective way to route users to Internet applications. AllCode leverages DNS endpoint health checks and the ability to failover between multiple endpoints in different regions. For each EC2 instance in N. Virginia, we will provision an Elastic IP address. Elastic IP addresses are static IP addresses designed for dynamic cloud computing. However, unlike traditional static IP addresses, Elastic IP addresses enable you to mask instance or Availability Zone failures by programmatically remapping your public IP addresses to instances in the Oregon region. For DR, we always pre-allocate some IP addresses for the most critical systems so that their IP addresses are already known before disaster strikes. This simplifies the execution of the DR plan.

Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables you to achieve even greater fault tolerance in your applications by seamlessly providing the load-balancing capacity that is needed in response to incoming application traffic. Just as you can pre-allocate Elastic IP addresses, you can pre-allocate your load balancer so that its DNS name is already known, which can simplify the execution of your DR plan.

Application name	Critical? Yes/No	Fixed asset? Yes/No	Machine Type	Machine Instance
	X	X	EC2	t2.large
		X	EC2	t2.large
	X	X	EC2	t2.large
		X	EC2	t2.large
	X	X	RDS	db.t3.large
		X	RDS	db.t3.large
	X	X	EC2	t2.large
		X	EC2	t2.large
	X	X	RDS	db.t3.large
		X	RDS	db.t3.large
AWS S3 Bucket	X	X		
AWS ELB	X	X		

Information Services Backup Procedures

Infrastructure

EC2 Instances – We enable Amazon Data Lifecycle Manager to automate the creation, retention, and deletion of snapshots to back up our Amazon EBS volumes for our AWS EC2 instances. We store snapshots at a 24-hour interval.

RDS Instances – We have RDS configured to perform daily automated backups that are saved for one month. The backup window is between 9:56 – 10:26 UTC (GMT). In addition, we leverage multi-site AZ on our RDS instances which enables us to go Hot- Hot.

Personal Computers

All personal computers are backed up using CloudBerry Backup, which uploads the files to S3 . The copies of the personal computer files should be uploaded to the system on Monday at 9:56 – 10:26 UTC (GMT), just before a complete save operation of the system is done. It is saved with the normal system save procedure. This provides for a more secure backup of personal computer-related systems where a local area disaster can wipe out important personal computer systems.

Disaster Recovery Procedures

For any disaster recovery plans, the following three elements should be addressed:

Emergency response procedures

To document the appropriate emergency response to a fire, natural disaster, or any other activities in order to protect lives and limit damages.

Backup operations procedures

To ensure that essential data processing operational tasks can be conducted after the disruption.

Recovery actions procedures

To facilitate the rapid restoration of a data processing system following a disaster.

Disaster Action checklist

1. Plan initiation
   a. Notify the senior management.
   b. Contact the team members in the Personnel to be involved in the DR Process
   c. Determine the degree of a disaster.
   d. Implement an appropriate application recovery plan dependent on the extent of the disaster.
   e. Monitor the progress.
   f. Contact all other necessary personnel, both user and data processing.
   g. Contact vendors, both hardware and software.
   h. Notify clients and users of the disruption of service.
2. Follow-up checklist:
   a. List teams and tasks.
   b. List all personnel and their telephone numbers.
   c. Establish the user participation plans.
   d. Determine the applications to be run and in what sequence.
   e. Identify if new EC2 and RDS instances are needed.
   f. Establish the primary vendors for assistance with problems incurred during emergency. In this case, AWS.
   g. Ensure that all personnel involved know their tasks.

Recovery start-up procedures for use after a disaster:

Notify AllCode senior management of the need to implement a recovery plan.
Guaranteed delivery time countdown begins at the time the client is notified of recovery plan selection.
Disaster notification numbers is xxx.xxx.xxxx.
This telephone number is in service 24x7.

Recovery plan–Web Application

In the event that the web apps go down, we will take the following steps:

1	Notify clients of the nature of the disaster and the need to select the website recovery plan via telephone.
2	Confirm in writing the substance of the telephone notification to the client within 48 hours of the telephone notification.
3	Confirm that the website can failover from N. Virginia region to Oregon region without data loss.
4	If the failover can take place, then change the DNS on the ELB to point to the Oregon EC2 instances.
5	If the failover cannot take place, then confirm that you have access to the EBS and RDS backups on S3. If access to the backups is available, then proceed to Restoring the Entire System.
6	Begin normal operations as soon as possible:
7	Ensure the web applications for all clients are running.

Restoring the Entire System

In the event that you cannot failover from N. Virginia to Oregon via the DNS because the Oregon region is down is non-responsive, then you may need to take the following steps. Prior to taking these steps, please confer with the team specified in the Personnel to be involved in the DR Process.

To restore your entire system to the state before the disaster, you will need to restore the EBS and RDS snapshots. The EBS and RDS snapshots are currently stored in the AWS on S3 in the xxxx\ec2 and xxxxx\rds directories in the regions of North Virginia and Oregon. Please confirm that you can access these files.

Next, you'll need to find a working AWS Region. Try North California and Ohio first. The next steps are:

1	Provision the new AWS Region
2	If you don't have access to the key pair, setup a new private key pair to use for the EC2 instances
3	Setup the VPC
4	Lockdown the VPC to allow only http, https, and ssh traffic
5	Setup the appropriate EC2 instances with the private key. The EC2 instances should be the same machine types as in Application and Inventory Profiles
6	Attach the EBS snapshots from S3 to the EC2 Instances
7	Provision the appropriate RDS instances. The RDS instances should be the same as in Application and Inventory Profiles
8	Upload the RDS Instance backups from S3. For MySQL use my the following link

9	Configure the EC2 instances to communicate with the RDS instances. The RDS instances will be new, which will require you to have new connection strings. Please ensure that the you are making use of the appropriate users with access to the appropriate restored dbs.
10	Verify the S3\CloudFront content is accessible. LPS makes use of ~1,000,000 images uploaded to S3. These images are required in the Facility console. Contex makes use of signed pdfs to ensure that parents have granted access to have doctors review their concussion information.
11	Configure SSL certificates for the EC2 instances. In a pinch, leverage Cloudflare if you don't have access to the private and public keys. Cloudflare will require you to shift the DNS from AWS.
12	Sanity check the environment.
13	Test the environment thoroughly before changing the DNS
14	Change DNS Entries
15	Roll out to production

Testing the Disaster Recovery Plan

In successful contingency planning, it is important to test and evaluate the plan regularly. Web applications are volatile in nature, resulting in frequent changes to equipment, programs, and documentation. These actions make it critical to consider the plan as a changing document. Use these checklists as your conduct, your test, and decide what areas should be tested.

Item	**Yes**	**No**	**Applicable**	**Not applicable**	**Comments**
Select the purpose of the test. What aspects of the plan are being evaluated?					
Describe the objectives of the test. How do you measure successful achievement of the objectives?					
Meet with management and explain the test and objectives. Gain their agreement and support.					
Have management announce the test and the expected completion time.					
Collect the test results at the end of the test period.					
Evaluate the results. Is recovery successful? Why or why not?					
Determine the implications of the test results. Does the successful recovery in a simple case imply the successful recovery for all critical jobs in the tolerable outage period?					
Make recommendations for changes. Call for responses by a given date.					

Item	Yes	No	Applicable	Not applicable	Comments
Notify other areas of results. Include users and auditors.					
Change the disaster recovery plan manual as necessary.					
Recovery of individual application systems by using files and documentation stored off site.					
Reloading of the EC2 and RDS instances from the backups on S#					
Ability to recover and process successfully without key people.					
Ability of the plan to clarify areas of responsibility and the chain of command.					
Effectiveness of security measures and security bypass procedures during the recovery period.					
Ability of users of real-time systems to cope with a temporary loss of online information.					
Ability of users to continue day-to-day operations without applications or jobs that are considered noncritical.					
Ability to contact the key people or their designated alternates quickly.					
Availability of important forms and paper stock.					
Ability to adapt plan to lesser disasters.					

○