RLDatix™

POLICYSTAT

Backup and Disaster Recovery Plan Outline

Updated April 2018

CONTENTS

Disaster Recovery Plan 3
Redundancy 3
Data Backup 3
Service Restoration From Backups 3
Downtime Monitoring and Notification 4
Customer Communication 4
Incident Post-Mortem 4

Disaster Recovery Plan

PolicyStat, as a software-as-a-service provider (SaaS), has a commitment to maintaining a highly available system. Regardless of any safeguards against downtime, we do understand that it is impossible to account for all potential sources of interruption. The purpose of this backup and disaster recovery plan is to outline what will happen in the case of unexpected downtime and how PolicyStat will move to resolve the problem.

We host our solution with Amazon Web Services (AWS). AWS, an Amazon.com company launched in 2002, is a collection of remote computing services that together make up a cloud computing platform, offered over the Internet by Amazon.com. The most central and wellknown of these services are Amazon EC2 and Amazon S3.

For information on our infrastructure-level protections, the AWS Security Whitepaper details measures taken by our hosting partner for security, availability and recovery.

Redundancy

In order to to maintain the highest service availability to our customers, PolicyStat takes advantage of **component redundancy**. This allows one or more individual pieces in the architecture to fail without affecting the system as a whole. Specifically, PolicyStat uses **geographically redundant** database and application servers so that in any outage up to an entire datacenter, there is no appreciable service interruption.

Data Backup

The most important part of the disaster recovery strategy must be in place before any interruption occurs. PolicyStat backs up customer data on three different levels to ensure data availability in case of disaster.

- Amazon RDS (RDS) provides disk-level backup capabilities via “snapshots”. A full disk snapshot is taken nightly between 2:20 and 4:20 am Eastern time daily. This snapshot is then stored using Amazon's geographically-distributed and fault-tolerant S3 service.
- Taking advantage of MySQL's transaction logs, rolling backups are performed with a **~5 minute resolution** allowing point-in-time recovery for any period during the previous three days.
- Nightly full backups are pulled from S3 and stored on disc drives at the PolicyStat headquarters, adding another layer of redundancy.

With these backup procedures, PolicyStat targets an MTTR (Mean Time to Recovery) of less than 15 minutes

Service Restoration From Backups

PolicyStat leverages cloud computing and deployment automation tools in order to streamline day to day operations. This has significant impact on our disaster recovery strategy as every deployment done as a part of normal operations is a test run for a recovery from backup situation. All system configuration is **automated** so that replacing a server is a matter Disaster Recovery Plan 4 of 6 Updated April, 2018 of performing the same process used for updating the application's code. That,

combined with our frequent application update schedule, ensures that our disaster recovery process is always known to be in working condition.

A major factor in our recovery plan is the ability to deploy our application in multiple **geographically-distributed data centers** through the use of AWS's availability zones. This gives us the ability to deploy in one of the 5 east-coast data centers or 3 west-coast data centers should the need arise.

With the ability to fully restore an entire deployment from scratch in the event of a catastrophic* failure, PolicyStat targets an MTTR of 15 minutes for non-catastrophic failures and 50 minutes for catastrophic failures.

** A catastrophic failure is defined as an event concurrently affecting multiple data centers.*

Downtime Monitoring and Notification

Our recovery plan builds on consistent and reliable backups and on strictly-defined operations processes with a focus on availability notifications. Our application is monitored for a set of user acceptance and systems tests from a **geographically-distributed monitoring service** which sends notifications on failures within a 60-second window. These alerts go out to multiple members of the operations team via email, SMS and voice and there is a clear protocol when notifications are received.

Customer Communication

Communications with PolicyStat customers are critical to the success of our recovery plan. Should service interruption occur, PolicyStat customer service will make every effort to notify affected customers via email and through the Announcements Forum on the support website at http://support.policystat.com. We believe that **open communication** and acknowledgment of any problems is optimal for our clients and for PolicyStat as a company and we are committed to providing insight in to any interruptions.

Incident Post-Mortem

Our recovery does not end once service has been restored. Our goal is to have any issue once and only once and through a series of questions, our goal is to reach the **root cause** of any issue and correct it. We employ the "five whys" process popularized in **Lean Manufacturing** to focus in on the root cause. This analysis is a crucial aspect of improving service availability over the long run, meeting availability goals and promoting customer confidence in our solutions.