DISASTER RECOVERY PLAN

The purpose of this document is to provide an overview of Panorama Education's infrastructure and detail the plan for responding to a catastrophic event leading to a major disruption of services.

Environment Overview

Panorama Education has built its software infrastructure using two technology service providers: (1) Amazon Web Services (AWS) (https://aws.amazon.com/) and (2) Heroku (https://www.heroku.com/).

AWS is an infrastructure-as-a-service (IaaS) provider that provides multiple services that integrate into the Panorama Education platform, including file storage, server resources, databases, and message queues.

Heroku is a platform-as-a-service (PaaS) provider that provides services including database management and back-ups, software deployment, and server management. Heroku is built on top of AWS directly, so that the infrastructure looks like:

Disaster Recovery Environment

As related to disaster recovery, these IaaS/PaaS services and Panorama Education's configuration of each service provides many layers of recovery and resilience to disasters. These include:

Individual Server Failure Detection and Auto-Recovery

During a single busy day, Panorama Education's platform can utilize several hundred virtual servers. This leads to operations approaches that are more automatic and assume that server failures can happen frequently. Both AWS and Heroku continually monitor their servers for unhealthy and failing hardware or systems. These server failures lead to transparent-to-users recovery of these server resources, through an automatic failover to other server resources that are healthy. Panorama Education has configured and designed our routing, web transactions, and background processing to be resilient to these failovers by retrying or processing where they left off.

Database Health Monitoring, Back-ups, and Auto-Recovery

Our primary datastore is provided via Heroku's Postgres database management services. In addition to routine maintenance, they provide Panorama Education with continual offsite back-ups, logical back-ups of the whole database, and "hot-swappable" followers of the primary database that we can manually switch to be the primary database in a matter of minutes. Like the server monitoring above, Heroku monitors the health of our databases and will automatically and transparently migrate them to healthy systems when problems that could harm availability reach near disastrous levels.

Multi-Datacenter Availability

Given the single point of failure of AWS IaaS services for both Heroku and Panorama, we also have considered the worst case scenario of an entire AWS datacenter becoming unavailable. Both AWS and Heroku have the ability to migrate your computer resources to another region. While this is a time-consuming and non-transparent operation, it does provide us with straightforward paths to recovery.

Organizational Monitoring

Organizationally, Panorama Education has 24/7 operational monitoring and alerting of these leading and lagging indicators of disaster. At least one member of the engineering team is always on-call and is alerted to these infrastructure concerns as soon as they are noticed. Panorama Education also has a well-established process of analysis and after-the-outage review to identify and fix systemic problems that are the root cause of outages.

Organizational Testing and Updating of the Disaster Recovery Plan

In addition to actual disasters, Panorama Education's team regularly tests and drills for outages of many types and styles to keep our tools and processes up to date. Additionally, Panorama Education will update the Disaster Recovery Plan as changes in the business/technical environment dictate, and each updated Plan will be made available for review prior to implementation. Any subsequent updates to the Disaster Recovery Plan that cause and/or permit any material reduction in the Services over the initial Disaster Recovery Plan shall be subject to advance written approval.

Catastrophic Failure Modes and Recovery Plans

Below, three levels of failure to the Services are outlined, including the anticipated cause of such a disaster and Panorama Education's procedures to ensure recovery.

1. Faulty Software Upgrade to Panorama's Software Problem: A routine update to Panorama Education's software causes unavailability.
    - Recovery Plan: - After identifying the problem, Panorama Education's team will assess if this is a "roll backward" or "roll forward" situation.
        - "Roll backward": If Panorama Education's team assesses that it is a situation where the software update can be safely reversed and rolled back, then Panorama Education will roll back to the previous software version within an hour.
        - "Roll forward": If Panorama Education's team assesses that the problem is one where the software update needs to be kept in place due to worse negative effects through a "roll back," the on-call engineers will work to produce a fix. That fix, once produced, can be deployed within an hour.

2. Partial or Full Loss of Data Problem: Our primary database has data deleted due to infrastructure failure, incorrect software update, or operational mistake.
    - Recovery Plan: - After identifying the problem, Panorama Education's engineering team would work with their contacts and support staff at Heroku to identify the best path for data recovery. There are multiple paths forward depending on the scale of the data loss:
        - If the data loss had not been replicated to one of the direct follower databases, Panorama Education could swap over to use the follower database in less than an hour.
        - If the data loss had been replicated through our follower databases, Panorama Education can work with Heroku to recreate a version of our database from the moments right before the data loss, so that the data can be recovered. This can take a few hours to recover.
        - If there is a catastrophic failure of all of the entire database infrastructure including all primary and follower databases, then Panorama Education can work with Heroku to recover data from off-Heroku physical backups that can be used to recreate the database. (https://devcenter.heroku.com/articles/heroku-postgres-data-safety-and-continuous-protection#physical-backups-on-heroku-postgres)

3. Partial or Full Loss of Server Resources Problem: One of Panorama Education's PaaS/IaaS service providers temporarily or permanently loses server resources for an extended period of time.
    - Recovery Plan: After identifying the problem, Panorama Education's team would work with Heroku or AWS to identify the best path for server resource recovery. There are multiple paths forward depending on the scale of the infrastructure loss:
        - If the server outage is isolated to single servers inside Heroku or AWS (i.e. some servers, but not all servers), Panorama Education has the ability to cycle through and replace individual servers within minutes.
        - If the server outage encompasses the entire datacenter (e.g. all of AWS-East in Virginia goes out for more than 48 hours), then we would have to work with Heroku and AWS to migrate to a different region (e.g. AWS-West in Oregon). Both service providers support these operations. It would take 1-2 days to complete the data center migration.