Cloud Deployment Architecture Plan

Trent Broderick

University of Maryland Global Campus

November 10th, 2020

**Executive Summary**

This document is meant to help clear up BallotOnlines position on how it plans to run “cloud-ready” applications in the cloud. Email, Software Development and Backup and Archiving are the three main cloud ready applications that are focused on. After evaluating several providers, the Cloud team has narrowed down a provider for each cloud ready applications while focusing its process on cost, performance, vendor lock-in and ability to meet general requirements.

It is asked of the executive team to carefully read through this document, look at the proposed architecture diagrams, and plan to move forward with the current plans for BallotOnline to become more Cloud Native.

**Scope**

The scope of this document contains the evaluation and plans for the architecture and surrounding capabilities for E-Mail, Software Development, Backup and Archiving cloud native applications. Included along with these services is a cloud native solution for monitoring as well as potential limitations. Each service offering was evaluated and considered thoroughly to ensure BallotOnline has a solution that is not only reliable but helps avoid vendor lock in.

By avoiding Vendor lock in and leveraging a few services to ensure that if BallotOnlines relationship with its cloud vendor does not work out, BallotOnline can move with its exit strategy and keep most of these services intact with little migration. By prioritizing avoiding Vendor Lock in and leveraging managed services only when needed, BallotOnline positions itself to be a highly available, highly mobile, and highly Cloud Native.

Included in this scope are diagrams to help illustrate the overall architectural goals this document describes.

**Evaluation of Cloud Service Offering Architecture for E-Mail**

The workload requirements for this service in a Recovery Time Objective of 15 minutes, Recovery Point Objective of 0 minutes (no loss of data allowed), mailboxes able to handle 5,000 emails at a minimum, completely managed and offers multi-factor authentication and encryption support. The two main services that will be considered for email will be Office365 and G-Suite. While our main workloads are hosted in Amazon, these services are known for their UI, user adoption and ease of use.

One major benefit that both email clients offer that is not always thought about is collaborative cloud-based programs such as Word Online and Google Docs, these included services will be important for teams to collaborate on projects and legal documents. While comparing both offerings from Microsoft and Google, one major issue arises. Google does not post its pricing for its Enterprise class tier which includes features needed such as 0 data loss and IAM access controls for increased compliances. However, while Microsoft posts its pricing, it seems to be more expensive than G-suite where prices are posted. For example, the services of Office 365 E3 are $20/user, the much similar tier at Google is $18/user. At scale, $2 can mean the difference of $20,000 a month or $240,000 a year for 10,000-member organization. Given the costs and general benefits, I am recommending G-Suite as the go-ahead email solution for BallotOnline.

**Evaluation of Cloud Service Offering Architecture for Software Development**

While tools like Elastic Beanstalk are great for a team leveraging Amazon, they increase the risk of vendor lock in. The goal of these cloud native solutions is to provide our team with a great experience when interacting with these apps, not increase the chances of having a painful exit strategy experience. With that being said, BallotOnline will be leveraging Cloudify Premium as its Platform as a Service software development environment.

Cloudify supports built in workflows, full life cycle management, a highly available solution that includes security features such as multi-authentication and SSO that will be eligible for use through the G-Suite (Cloudify, 2020). Pricing is done on a subscription basis and offers a 24x7 SLA. The software development environment is priced on the amount of VMs needed and additional SLAs BallotOnline requires. While tools like AWS Beanstalk are free, they do not offer the flexibility or multi-cloud options that Cloudify do. Using Cloudify gives BallotOnline greater agility in the future should the vendor relationship not work out.

**Evaluation of Cloud Service Offering Architecture for Backup and Archiving**

Since BallotOnline will be leveraging Amazon EC2 for compute, as a storage solution, Amazon S3 makes a ton of sense for ease of use and backups. With the ability to store millions of objects in millions of buckets globally, Amazon S3 can meet a majority of the needs from a performance, cost, capacity and availability requirements. Amazon AI helps users better utilize the storage they pay for in a storage tier. They also use AI to help decide what archives are best suited for Glacier and Glacier Deep Archive. Utilizing Amazon in this way is a great plan and if there is ever a need to exit amazon, Back Blaze and Wasabi offer cost effective s3 compliant bucket storage that can be utilized in a pinch. However, this will not be the only place backups are stored.

Equinix has rolled out its new Metal platform that includes bare metal servers, some with 100TB of storage per server. While this is available is select locations, these servers are single-tenant and purely bare metal. In the architecture section will be the high-level architecture on how these environments connect. It is important to note here that if AWS has a single point failure in those regions or as an entire platform, this will be another provider BallotOnline can recover and scale up in while AWS fixes its platform problems should they arise.

**Architecture Design for E-Mail in the Cloud**

When drawing up the high-level overview of the email architecture, it is important to highlight that G-Suite is a SaaS solution so BallotOnline is un-aware of the underlying infrastructure. The goal of the design is to ensure only BallotOnline employees are able to access the email server from either a desktop built into the Virtual Private Cloud that only interacts with internet through a locked down virtual routing appliance or a mobile device connected via VPN that interacts with G-Suite through the routing appliance. With the architecture diagram below, BallotOnline is able to keep its locked down style architecture while still providing adequate access to email servers.

Diagram

Description automatically generated

**Architecture Design for Software Development Platform in the Cloud**

The general architecture is much similar for a PaaS such as Cloudify. With Cloudify, we have a much better idea of the underlying infrastructure as they offer highly available solutions across multiple regions. Below is an idea of how both our BallotOnline systems and Cloudify systems look together.

Diagram

Description automatically generated

**Architecture Design for Backup and Archiving in the Cloud**

While it has been determined to use Amazon S3 for storage and Glacier for archiving, there needs to be a secondary location for backups that is not within AWS. The goal and reasoning beyond vendor lock in is to ensure BallotOnline is not opening itself up to single point failures. Equinix Metal is a service that allows direct connections to AWS where backups can be stored and initialized on a bare metal server. This provides us more functionality in a way that if disaster happens, one of our back up points can also become a Disaster Recovery Site.

Diagram

Description automatically generated

**Cloud Monitoring Solution for Backup and Archiving (1–2 pages)**

Amazon CloudWatch is a great tool for monitoring all activity within Amazon to ensure usage charges are kept in check. Key benefits of AWS CloudWatch are observability on a single platform, ease of use, ability to optimize with AI, deeper visibility into our AWS environment as well as actionable insights (Amazon, 2020). Amazon also produces a handy diagram to visualize exactly how CloudWatch works (Amazon, 2020).Timeline

Description automatically generated

The major use case for CloudWatch is not usage cost watching but also ensuring the infrastructure is always on and always available. The logs it collects help ensure that if an issue arises, we have a paper trail to see what may have went wrong and help the team solve for the issue. As far as Equinix Metal is concerned, the servers have a fixed cost with no variation. Since it is in an OPEX model, we can plan for these expenses in the budget with very little if any variations month over month.

**Limitations**

The limitations for all three workloads are based in access control. For example, BallotOnline employees can not simply just connect to the internal of our systems. They will either need to be operating with in a Virtual Desktop Interface or connected via VPN through a gateway. In SaaS and PaaS solutions like Software Development and Email, BallotOnline has limited options in the underlying stack and its architecture. With Backup and Archiving, there is much more opinion in the stack and how it operates. While we are limited to Amazon for low latency fast storage solutions, in all other cases, BallotOnline is easily able to move from cloud vendor to vendor should the exit strategy every be utilized.

**Summary**

To summarize, G-Suite is BallotOnlines email service provider, Cloudify is BallotOnlines software development platform provider, and a mix of S3, Glacier and Equinix Metal will be used to architect the back up and archiving strategy for BallotOnline. While focusing on performance, cost, ease of use, flexibility, avoidance of vendor lock in, capacity and ability to meet BallotOnlines requirements, these providers have checked off all feasible requirements to move forward with the overall design and cloud ready system architecture.

**References**

Amazon Web Services. (2020). *Amazon CloudWatch*. Amazon Web Services, Inc. https://aws.amazon.com/cloudwatch/

Cloudify. (2020, October 5). *Cloudify Orchestration Platform - Multi Cloud, Cloud Native & Edge*. https://cloudify.co/