SECURE, DEPENDABLE AWS GOVCLOUD DEPLOYMENTS

Summary

Government contractors must often ensure their solutions meet quality and privacy requirements. Our client faced two such obligations: proper protection of Personally Identifiable Information (PII) and high availability to meet Service Level Agreements (SLAs). Our client elected to deploy their software to the Amazon cloud and follow DevOps best practices paired with modern tooling.

Unfortunately, the regulated aspect of their data complicated this significantly. To meet these requirements, our client needed to deploy into AWS GovCloud. Unfortunately, as we have blogged about in the past, GovCloud presents enough of a difference from standard AWS datacenters that common tools often break.

FP Complete was tasked with setting up a secure, compliant, highly available, and easily maintained cluster.

Industry: Government contractor
Project Type: DevOps
Technology Used: AWS, GovCloud, Terraform, Nomad

Project Requirements

- Hosting for a web-based Software as a Service (SaaS) product
- Compliance with all regulations for data storage and transit
- Hosting within the AWS GovCloud datacenter
- Isolated environments for development, QA, and production
- Integration with Continuous Integration/Continuous Deployment (CI/CD) pipelines
- Automated deployment
- Autoscaling in response to load
- Auto recovery from unhealthy nodes
- Declarative infrastructure

The Solution

The most popular orchestration management solution at the time was Kubernetes. However, from previous projects, we knew that there were still some idiosyncrasies around Kubernetes support within GovCloud. To minimize risk, we opted to deploy Nomad. Nomad provides a similar feature set to Kubernetes but relies on less cloud services for a reliable deployment, making it an ideal choice at the time for a GovCloud setup.

We used Terraform to declaratively specify the infrastructure necessary for hosting the Nomad cluster, along with dependencies like the Consul service discovery framework. This allowed us to iterate quickly, and later deploy matching clusters for the development, QA, and production

environments. To reduce hardware costs, we parameterized these scripts to choose smaller instances in the non-mission-critical environments.

Further work was necessary to ensure proper adherence to regulatory guidelines. We leveraged AWS Key Management Service (KMS) to provide encryption-at-rest within databases, and ensured TLS encryption for data in transit, both from the outside world into the load balancer, and from the load balancer to the cluster itself.

Later, to provide further security, we deployed Hashicorp Vault for secure credentials management.

New Challenges for FP Complete

This project revolved around regulated data, GovCloud, and Nomad. While all three are concepts that we have worked with individually in the past, this was the first project to combine all three. Integration went well and presented less of an obstacle than we would have expected.

Conclusion

Both high availability deployments and governance of regulated data are challenging problems in their own rights. Combining both into a single set of requirements is particularly difficult. We are thrilled that the combination of tools we selected integrated well, supported the AWS GovCloud environment fully, and delivered a stable platform for our client.