Case Study

Speed Development in the Cloud

THE CHALLENGE

Our customer maintained an unclassified research lab environment for developing innovative new applications and testing various types of equipment. Due to the lab's success, the customer wanted to expand usage across multiple different research organizations focused on communications, analytics, quantum computing, and other disciplines.

The expansion would substantially increase the number of users with access to the environment and the need to collaborate with academia on certain projects. The current on-premise, isolated IT infrastructure posed several challenges. There were periods when testing and development activities surged and times when IT resources went unutilized. It was very difficult to transfer the technologies developed, once mature, from research to operations because vastly different underlying IT infrastructures were used.

THE SOLUTION

Leveraging our experience architecting similar environments, Stratus developed a secure, scalable hybrid cloud solution to give researchers the ability to setup and configure new development and testing environments on demand. This solution was designed to support multiple research organizations with different needs and allow access to both cloud and on-premise resources. In lieu of setting up multiple isolated physical labs that use separate IT infrastructure, researchers now leverage resources within the cloud to better orchestrate development and testing activities during periods of surge. The environment is also built on the same AWS core architecture used by operations, allowing these research organizations to more easily transition technologies once they are mature.

Stratus employed AWS Workspaces using multi-factor authentication to facilitate secure, central access to the research environment. Once inside, researchers can gain access to project-specific environments that connect AWS resources such as EC2, S3, and RDS with on-premise hardware using a combination of networking services.

Additionally, the environment has robust security auditing and reporting enabled using a combination of ELB, S3 Bucket Policies, Security Groups, SNS, SQS, and CloudWatch. Access management and resource constraints are enforced by user, group, and role through IAM; and CloudFormation templates ensure accounts and environments can be programmatically set up and consistently replicated when the technology is ready to be transitioned to production