Case 05: Managing Implementation

A lot of the customers we see are in the Enterprise space, so their needs are very similar. This example came from a Financial Services company. We often see similar requirements among FinServ companies.

A Finserv customer had this interesting business requirement...

- Encryption in transit and at rest for all developer operations
- Follows Google Best Practices
- All Keys must be managed by Company - they wanted to own the keys

The real trick here is that the structure and solution had to be put into production at one time. It couldn't be built in parts into production. It had to be all working when it went into production. That caused us to think about what parts were inherent, and what parts we could automate. So we ended up using a Jenkins pipeline and Deployment Manager templates for parts of this automation.

We mapped that to technical requirements like this…

- Use Google Authentication.
- No Public IP access unless through bastion host.
- No Operations team access to the production environment. That means "no ops" - everything is automated.
- Minimize downloaded keys.
- Keys accounted for via business logic application.

All of the Google APIs are encrypted in transit, and authenticated. So that requirement was inherited and automatic. The production team needed operations access but without handing them keys. So what we did is implemented all operations in deployment pipelines using Jenkins and Deployment Manager. The business logic was implemented using python in the Deployment Manager templates.

And this is how we implemented that technical requirement.

- All Google APIs are encrypted in transit, and authenticated.
- Production has operations team access - all deployment pipelines via Jenkins and Deployment Manager. Business Logic in python templates in Deployment Manager.
- The Cloud SDK was not installed in local machines - Cloud Shell ensures no keys are downloaded.
- Service Account keys when needed for off-Google Cloud clients are managed via deployment pipelines.

There are two kinds of operations actions; on-Google Cloud actions and off-Google Cloud actions. For on-Google Cloud actions, we didn't install the Cloud SDK on local machines. Instead, we set them up to use Cloud Shell. That ensured that no keys were downloaded. For off-Google Cloud actions,the Service Account keys were managed via the deployment pipelines. Any time there is a need for off-Google Cloud access, the clients are managed via the deployment pipelines. So that means there is full audit, control, and records of those keys, who had access to them, and when and where they were used.