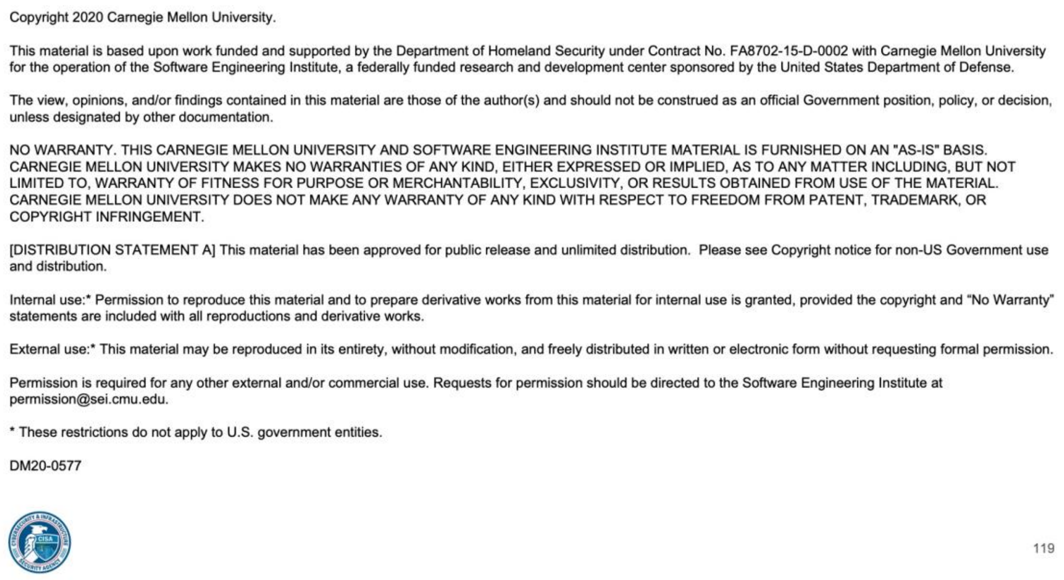
Deploying a Web Application Within Google Cloud and Adding Security Configurations

Demo



Instructor: In this demonstration we are going to deploy a new web application within Google Cloud, and follow up with some security configurations for that application.

Google provides some easy to follow tutorials to get one acclimated to their cloud platform. We are going to walk through one of those to get started.

First we select our project.

Then we initiate Cloud Shell, which is a built-in command-line tool for the console.

Once started we can download a sample "Hello World" application and proceed with the installation steps.

The tutorial will have us take a quick look at the go code and the yaml file which is used to facilitate the application install.

Next we execute the command to run the application. This will let us view the page before we publish to our app engine.

Speaking of which, we need to first create an application within our project. We can do that with a gcloud command.

Once that completes, we can deploy our Hello World application.

Note the URL that our application will use. And also see here that several files have been uploaded to Google storage. We'll have to check on those in a bit.

When we are done-done we can visit our URL to see our running web app.

Our next recommendation is to view the App Engine dashboard to verify things are working as expected. But, it will be a little while until we see any relevant statistics since we just got things set up.

We can also take advantage of the security scan service available in Google Cloud. When we click on Security Scans it takes us to the security center, where we can see several other services and configuration options. We are going to focus on setting up a security scan.

As with most things within Google Cloud, enabling this service sets up an API to support the execution.

Now we will create a scan. There isn't a great deal of parameters available to us here. The URLs you would like scanned, and when this test will be scheduled are the minimum options that need to be considered. We will save our scan, and then click run scan to get things started.

While we are waiting for that to finish, let's take a look at IAM in Google Cloud. When we go to that dashboard, we see a list of users assigned to our project, their name, and associated roles. Note the API accounts that have been automatically added to the project to support tasks like that security scan.

If we wanted to, we could add additional users to this project, and also specify the roles they would be assigned. For example, App Engine Deployer or Admin may be required for one or more software developers.

If we click manage roles, we get the full list of those, and we can easily drill down to see the specific permissions assigned to each.

Returning to our scan, we see that we have one issue. Basically, the results indicate something is fishy because there are few resources on my web site. I'm pretty sure I can accept that risk.

Let's quickly take a look at the firewall rules. Here we could define specific allow and deny polices for network-based access to our application engine.

We mentioned storage during the install, so let's review what happened there. There are actually 3 buckets that have automatically been created for us. We can do a little digging around in here to see what was posted to these folders as part of that application install. We see configuration files, and even the source code of the application, along with the yaml used to configure our deployment. Let's do a couple tests, just to see who has access.

I'll copy the URL, open another browser, and see if I can access the source code of our application. Hmm, we are prompted to save the file, and now I can open it and view the source. This concerned me at first, and then I realized I was actually signed in to google in that other browser as well. So, lets sign out and try to access that URL again. Sure enough, I cannot. Instead, I am prompted to enter the credentials of an account that has the appropriate access granted within my project.