Monitoring and Alerting Options Available in Google Cloud

Demo

Instructor: In this demonstration we're going to review some of the monitoring and alerting options available in Google Cloud. Once we login to our account, you can see right away that we have some utilization statistics for our app and compute engines. This dashboard is highly configurable, so you can customize it based on your job role and critical information needs.

Let's dive deeper into the monitoring dashboard. We're going to start in the resource dashboard here. First up is cloud storage, and here we can see our list of storage buckets, requests, and/or traffic to and from our bucket, and we can drill into a specific bucket as needed. In the top

right we can select different intervals such as last week or month.

Now we'll jump into the uptime checks. Assuming we have a web application deployed within our app engine, let's create a web monitor. As we expand the advanced options, you see that we can go beyond simple TCP port checking to evaluate headers and responses. We can also enable checks for multiple locations to ensure our application is available, or not, from a specific region. Authentication options are also available. We'll click Save to complete the setup.

We are immediately presented with an option to set up an alert based on the check we just created. We'll click No for no, because we will set this up in a bit. First, we're going to define a second check. This one will be for a compute instance, and specifically TCP Port 22, to make sure that we can access our virtual machine, and then we'll save.

Now we can hop over to Alerting and set up a new policy. When we click on Add Condition, we can select from various default metrics or from a list of uptime checks. Next, we need to configure notification options. This could include SMS, email, Slack and several other options. We're going to use email for our tests, and then save our alert. You will see our two uptime checks in the lower left that we just created.

Let's go to our VM instance and configure some additional monitoring capabilities. Our test instance here does not yet have a monitoring agent installed. So let's make that happen. Clicking on Not Detected pulls up our action panel where we have to select our operating system and then click Install Agent. We'll go through the prompts here in Cloud Shell.

We can fast forward a few minutes to a point where our installation is completed and the data is available. Once that happens we have access to detailed CPU memory, disk and network utilization statistics for our instance. Jumping back to our main dashboard you'll see that it's populated with additional details which we can monitor.

Now let's see if we can turn our uptime checks from green to red. I'll return to our main dashboard and then drill into our app engine resources, and we'll go ahead and disable our web application.

Next, we'll head into our compute engine to shut down our test virtual machine. When we go back over to our monitoring dashboard you can see that our status already is changing. Our web monitor is red because all checks failed, whereas our instance check is yellow because tests from some regions passed while others did not.

We can see that email alerts were indeed sent, meeting our notification expectations, and when we return to

our monitoring dashboard we see
that both checks are now completely red.