VPC Network Access Controls and CloudWatch Monitoring

Demo

Instructor: In this demonstration we're going to review VPC network access controls and introduce cloud watch monitoring features. Let's get right to it, and look at our default virtual private cloud, and its main network access control list. You noticed that both the inbound and outbound rules have no restrictions. All IP addresses and all protocols are allowed inbound, as well as outbound. You will see a similar configuration for each of the subnets within the VPC, allowing all inbound and outbound traffic. These open access controls will presumably be superseded by tighter controls defined for each instance, but it does

indeed open a door into your VPC where you may have servers and services that are not protected. Within this security group we see that inbound traffic has indeed been restricted to just RDP and SSH.

Now let's take a look at CloudWatch. Any instance that you configure with the CloudWatch checkbox will enable this type of reporting. CPU, memory, bandwidth and other utilization statistics are tracked. You can see similar graphs for Elastic Block Storage, and for S3 buckets if you have it enabled.

AWS cloud trail continuously logs your AWS account activity. Let's set up our first trail. When doing this we need to store trail data somewhere, so we must select an existing S3 bucket or create a new one. We will select an existing one. We don't have our KMS setup yet, so we won't be encrypting our trail right now. However, we do want to capture CloudWatch logs to this trail so we need to check that box.

The trail will live within a CloudWatch Log Group so we need to select or create a new one here. Similarly, we must select or create an IAM user that has the necessary permissions to write to the trail.

Next we have to choose which events to include. Options are for Management, Data, and/or Insights. We'll use the default management settings, and leave the API monitoring options and continue.

After creating the trail we can return to our VPC and enable Flow Logging. This will allow us to capture and analyze high-level network traffic data for anomalies.

We can decide to collect flows on all traffic or just allowed or denied packets. We need to send this stream to the Log Group we previously created. And we need to identify the IAM user that has permissions to write to that Log Group and Bucket. We will except the default AWS format and create our flow.

The Flow Log section in our VPC details now shows our configuration. And that configuration has propagated to each of our 3 VPC subnets.

In about 15 minutes that data will start getting collected, similar to the other events detailed in this stream.