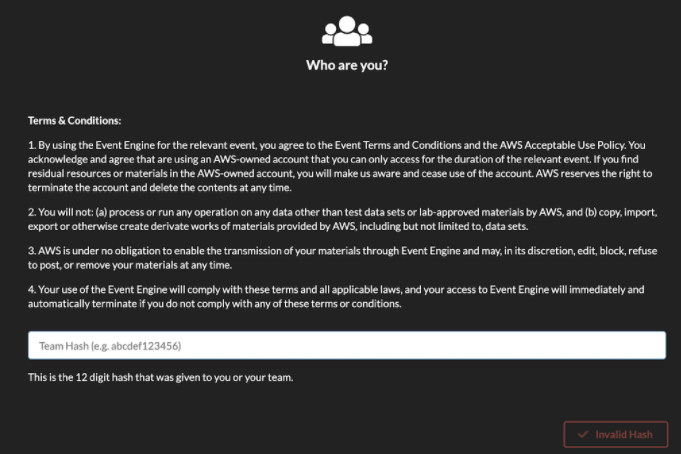
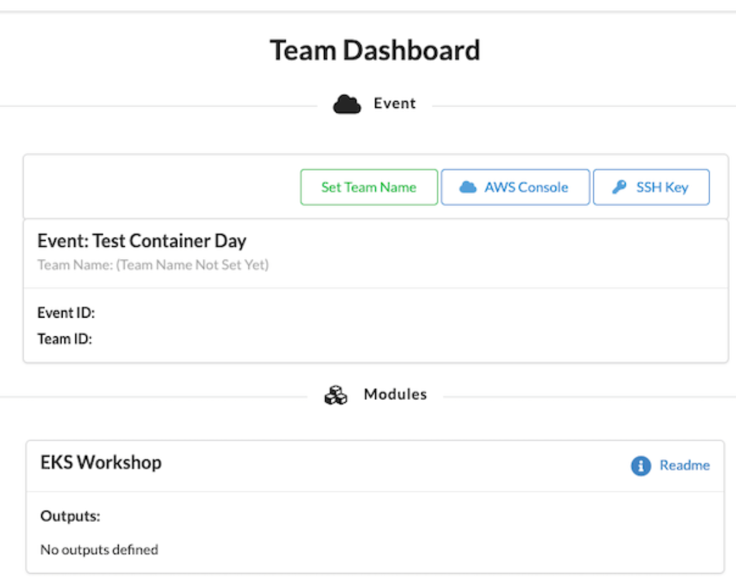
**1. Connecting to the AWS EventEngine**

To help you get hands-on as quickly as possible, we pre-created an AWS environment for each participant. You will need the EventHash code, which will be shared by the speaker and your email address to track your unique session.

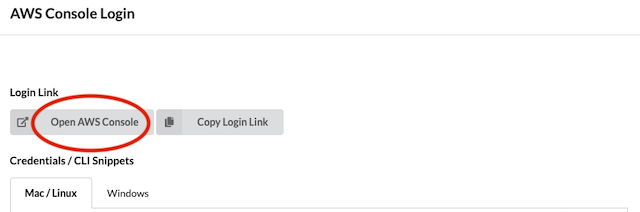
Connect to the AWS Event Engine by browsing to <https://dashboard.eventengine.run/>  
- Enter your unique hash and the click on proceed. 

- You will see the below screen

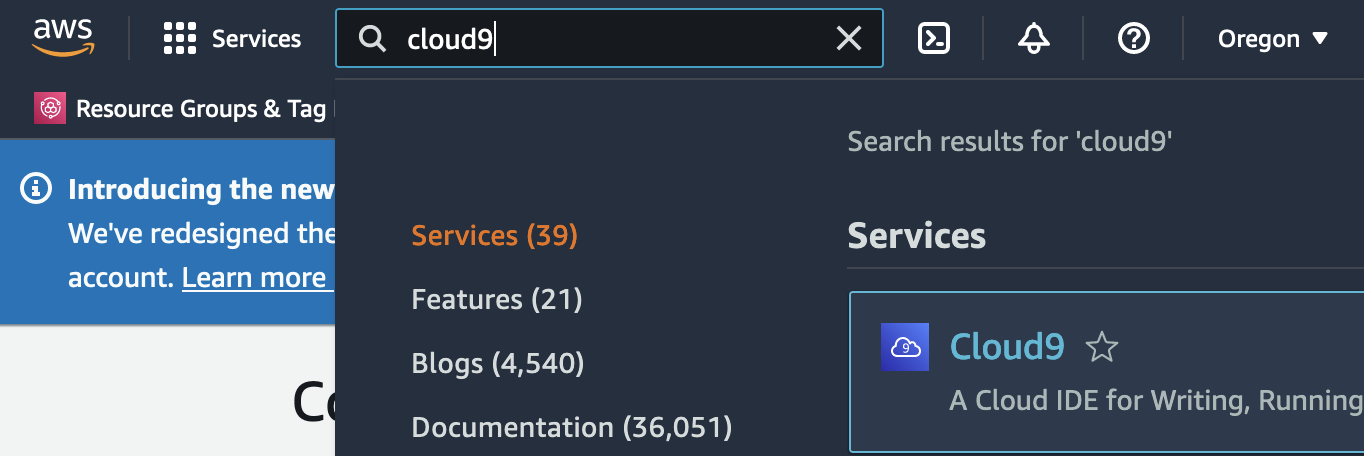


- Click “ReadMe” under Modules and copy commands (Aws s3 cp..) that you need to run after opening a cloud9 instance once you login to the AWS Management Console from your EventEngine team landing page.

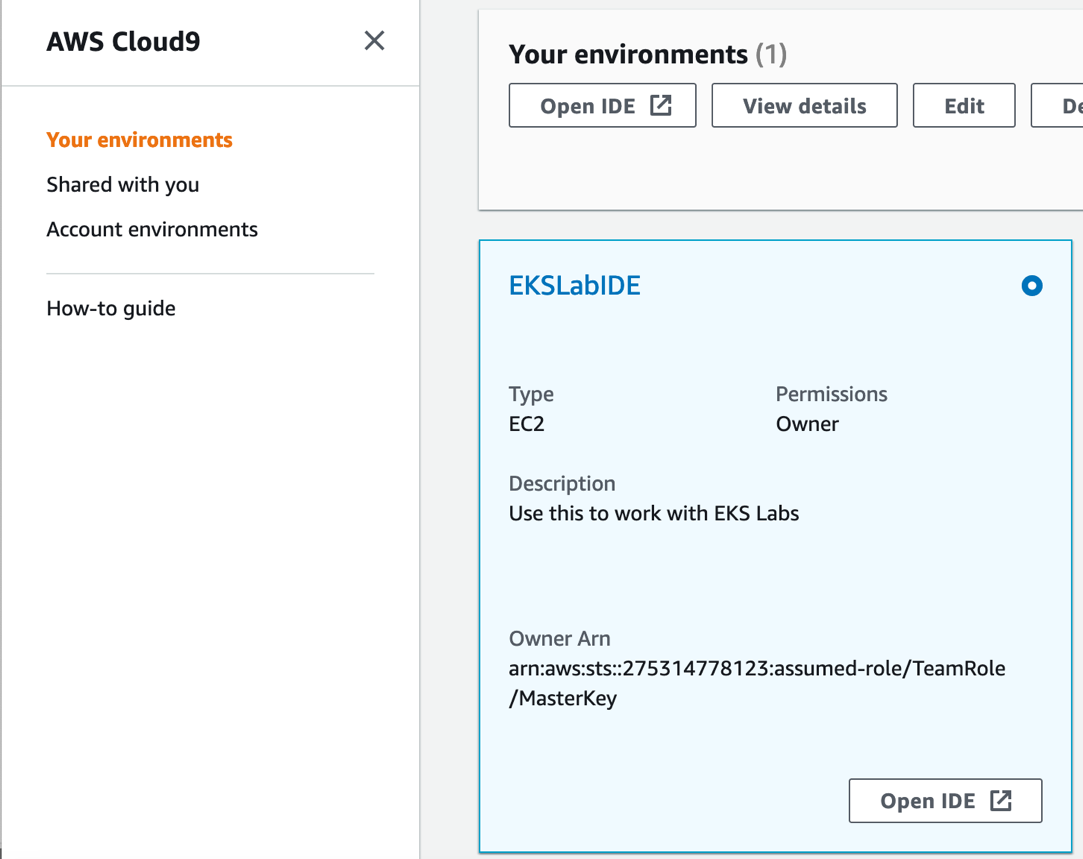
- Click on AWS Console button, and Click on the Open AWS Console button to launch the AWS Management Console. You don’t have to copy and credentials from here. If you’re previously logged in to any AWS account, you would need to first log out from there.



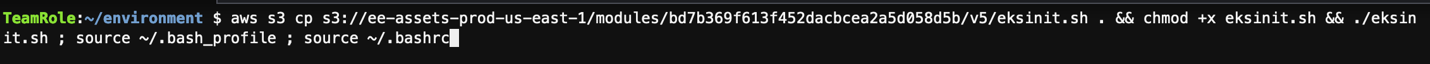
- You will already have an EKS cluster and Cloud9 environment. A few additional steps are required to configure Cloud9 and install the tools which are available in the readme link in the Event Engine Dashboard. Search “Cloud9” in AWS console. Cloud9 is a managed IDE that we will use to run kubectl to interact with the EKS cluster later to simulate Kubernetes Findings.



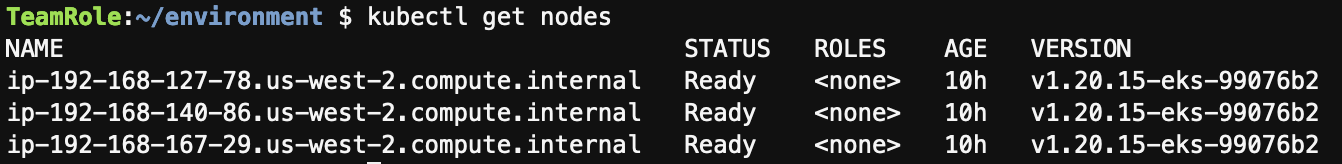
- You will be able to find EKSLabIDE cloud9 instance pre-deployed. Click Open IDE.



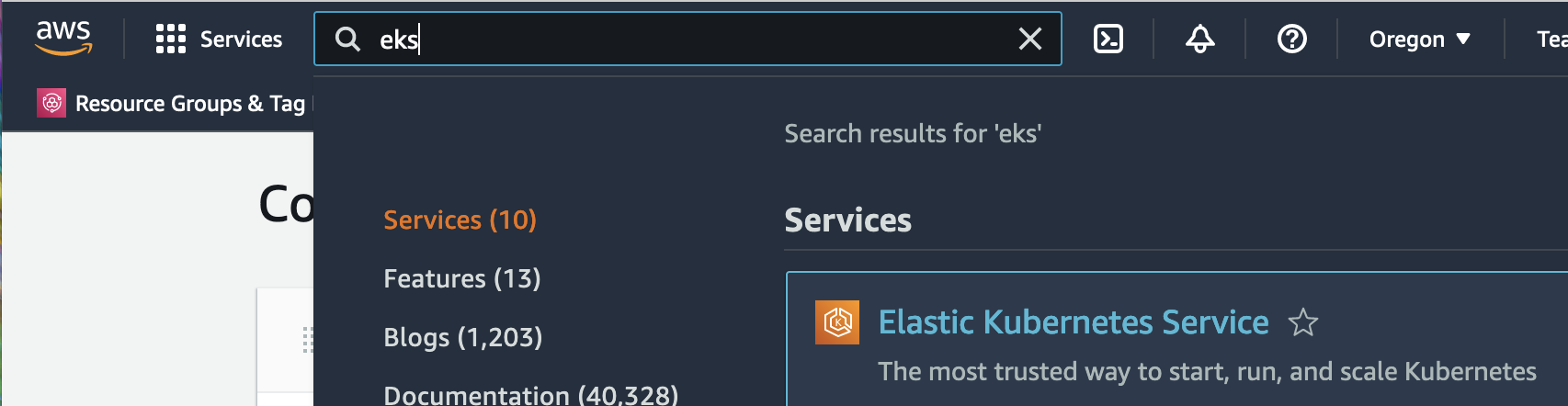
- Run commands that you copied from the readme file.

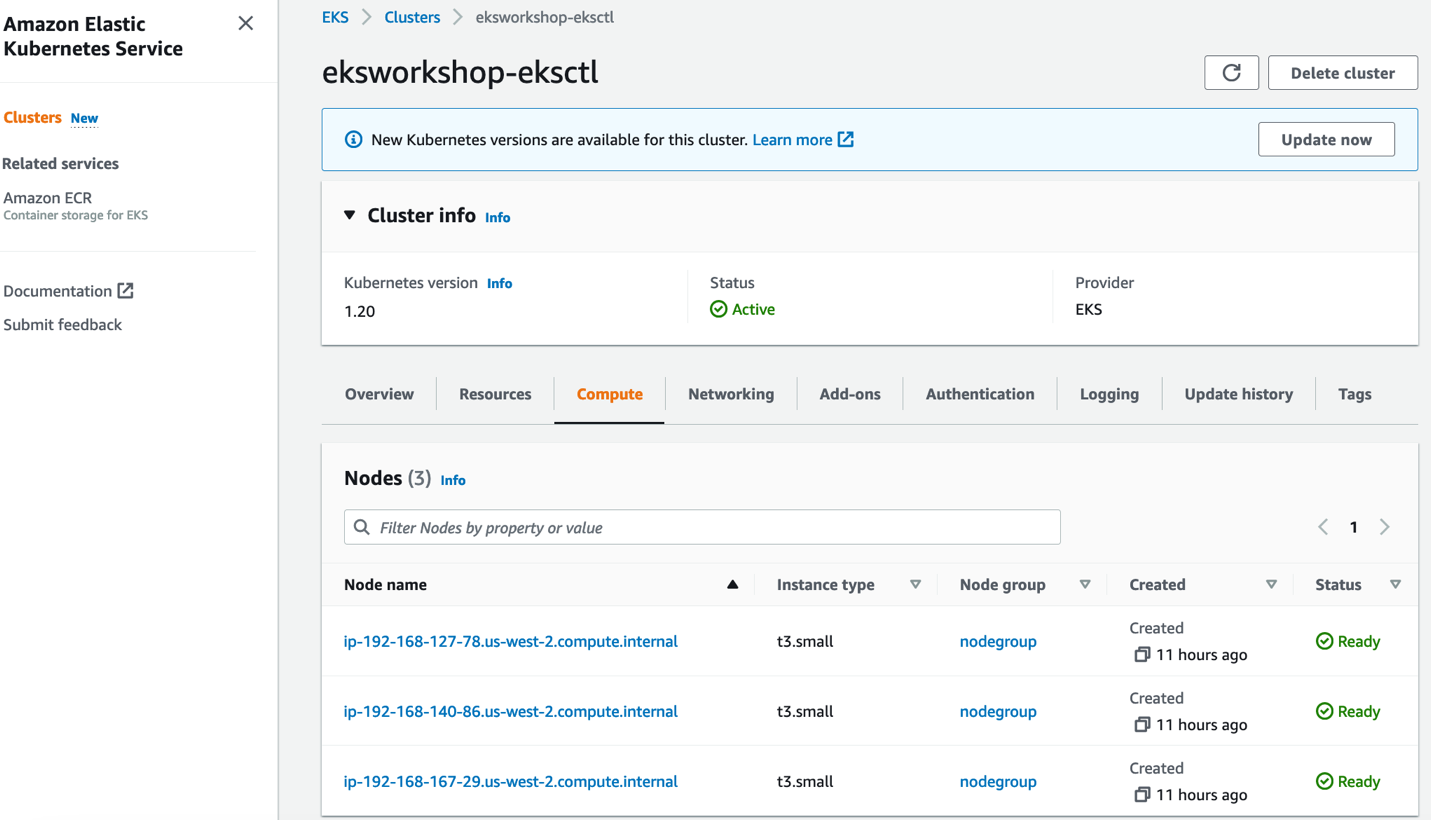


- Check if *kubectl get nodes* command works. If nodes are ready, we’re good to go.



- Go back to AWS console and search EKS to check the overall configuration of your cluster. (eksworshop-eksctl)

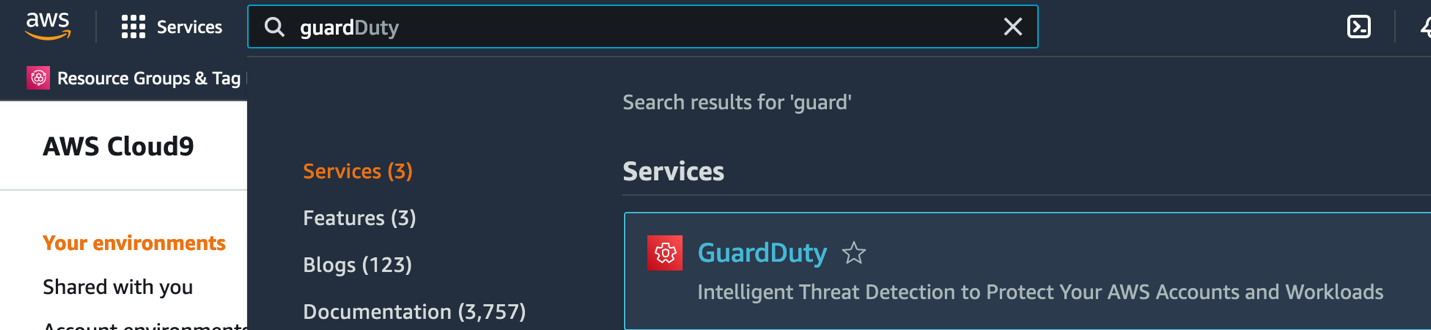


****

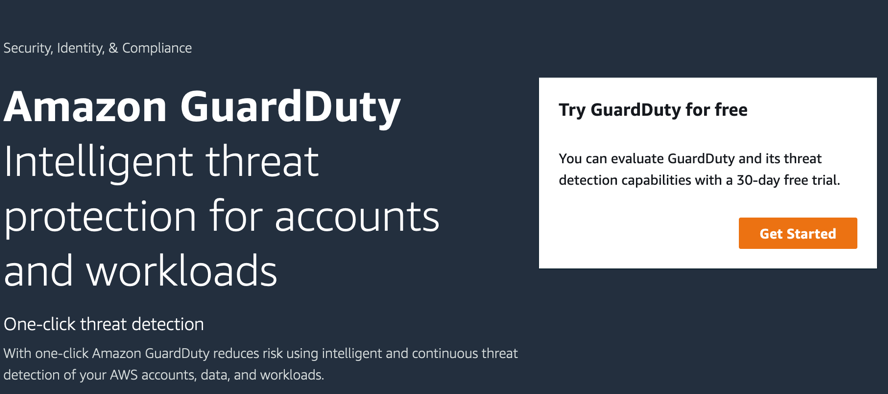
**2. Enable GuardDuty Findings on EKS**

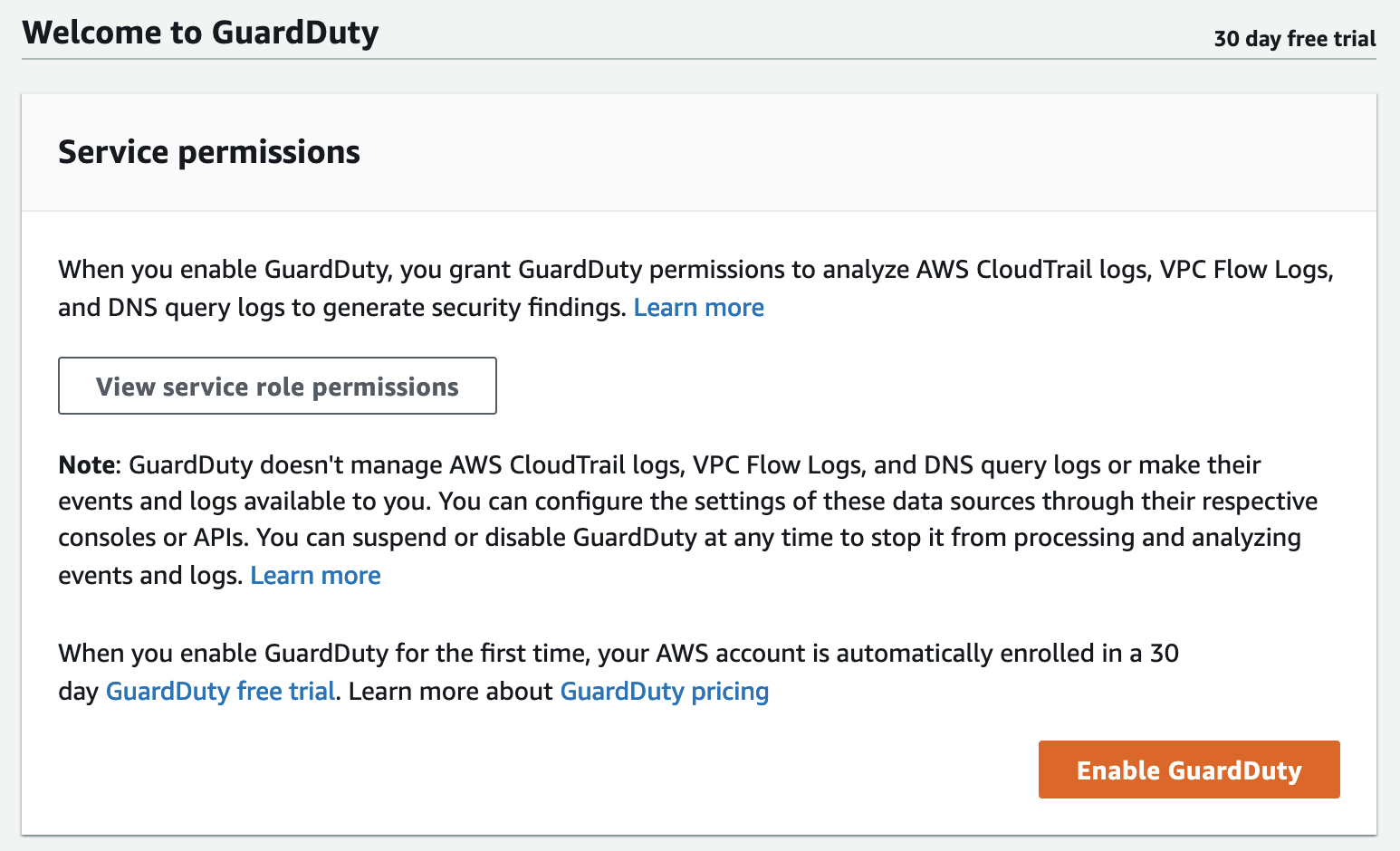
In this section, we will enable GuardDuty and Kubernetes protection.

- Search GuardDuty in AWS console



- Click get started



- Click Enable GuardDuty  


- Check if Kubernetes Protection is enabled.



-Go to *Findings* and you will see you don’t have any findings yet.

**3. Generate Kubernetes Findings on Cloud9 instance.**

In this section, we will generate various Kubernetes findings on your Cloud9 instance.

- Go back to your Cloud9 terminal and clone git repo that has GuardDuty Kubernetes sample findings.  
$ git clone https://github.com/ChanceLee0111/reinforce2022-tdr351/

### Finding type: PrivilegeEscalation:Kubernetes/PrivilegedContainer

### Finding type:Kubernetes/ContainerWithSensitiveMount Incident

-

5. Create a SNS topic

6. Create an EventBridge to filter events

7. Lambda integration (optional)

8. CloudWatch Log groups Log insights (optional)