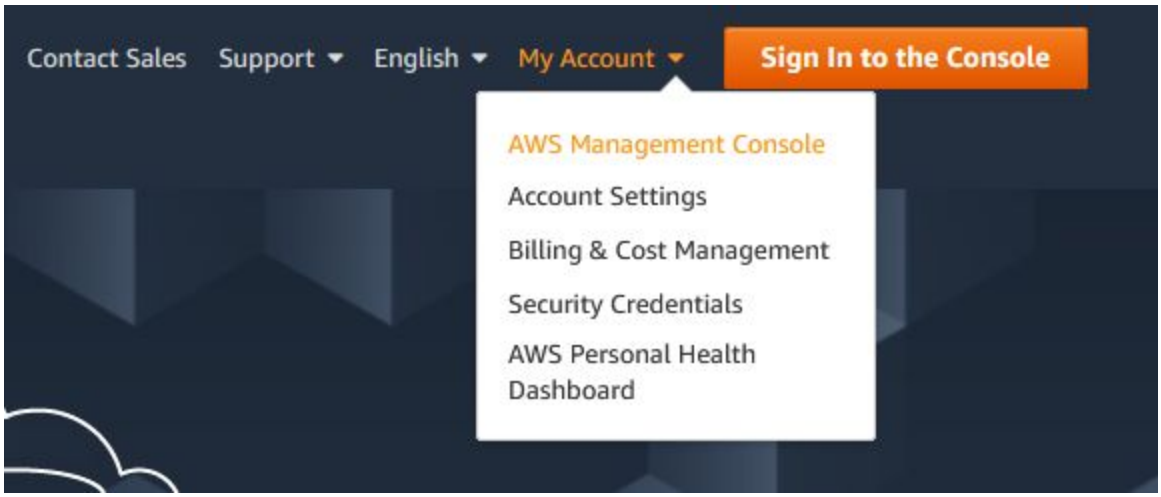
Cyber Defense Organization

Cloud Security Instructions - Tyler Blanco 11/13/2019

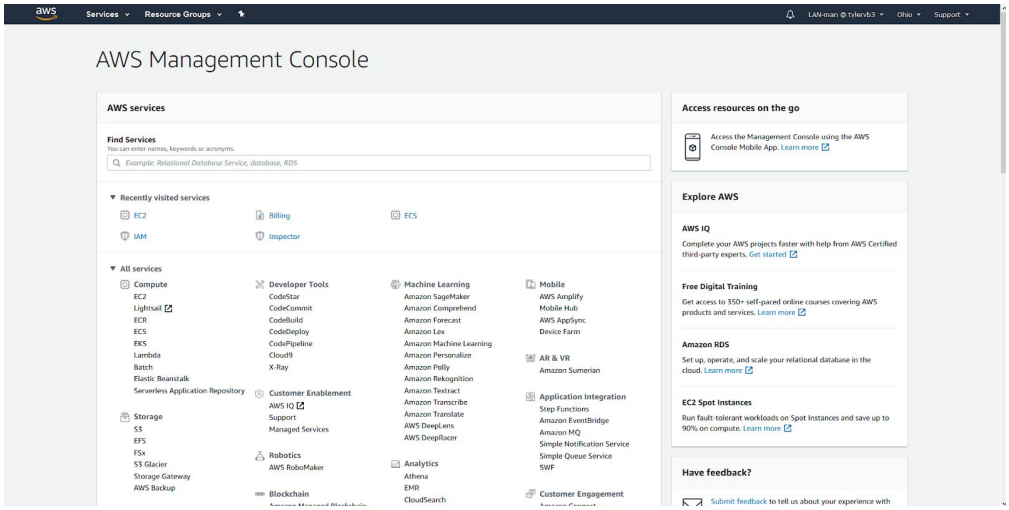
https://tinyurl.com/CDO-CloudSecurity

Get to AWS:

1. Open a browser, go to https://aws.amazon.com/
2. Hover over *My Account* in the top right and hit **AWS Management Console**

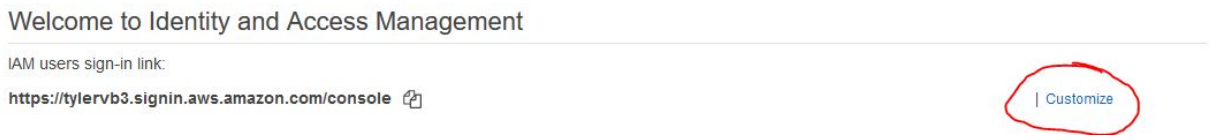


3. Sign into your AWS account.
4. You should see the management console.

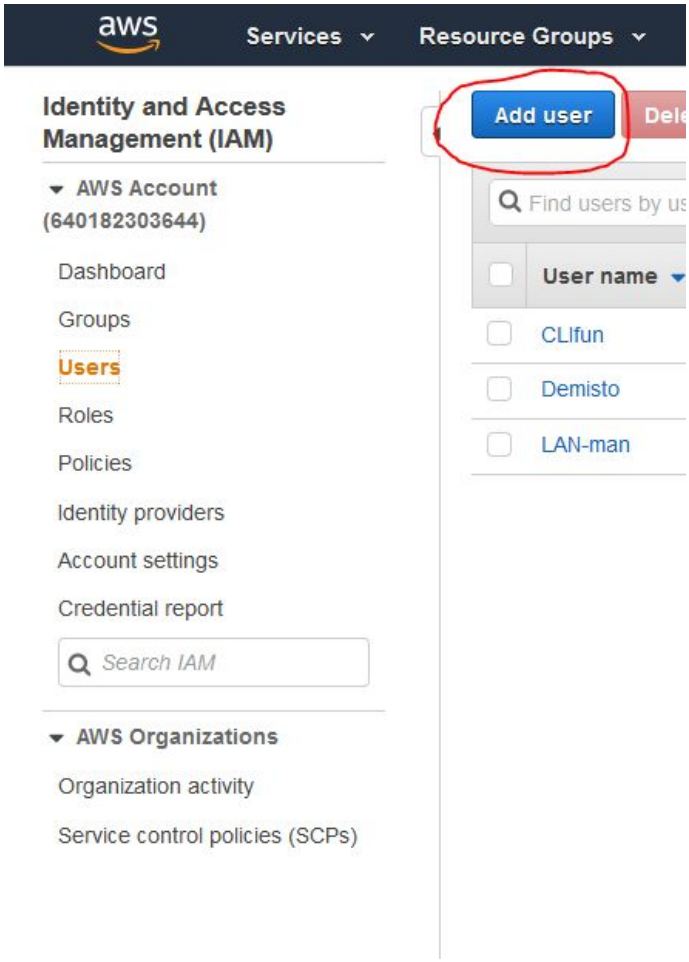


IAM Hands on

1. Open IAM
2. Create an Access ID for your IAM user by hitting customize on the top of the page.

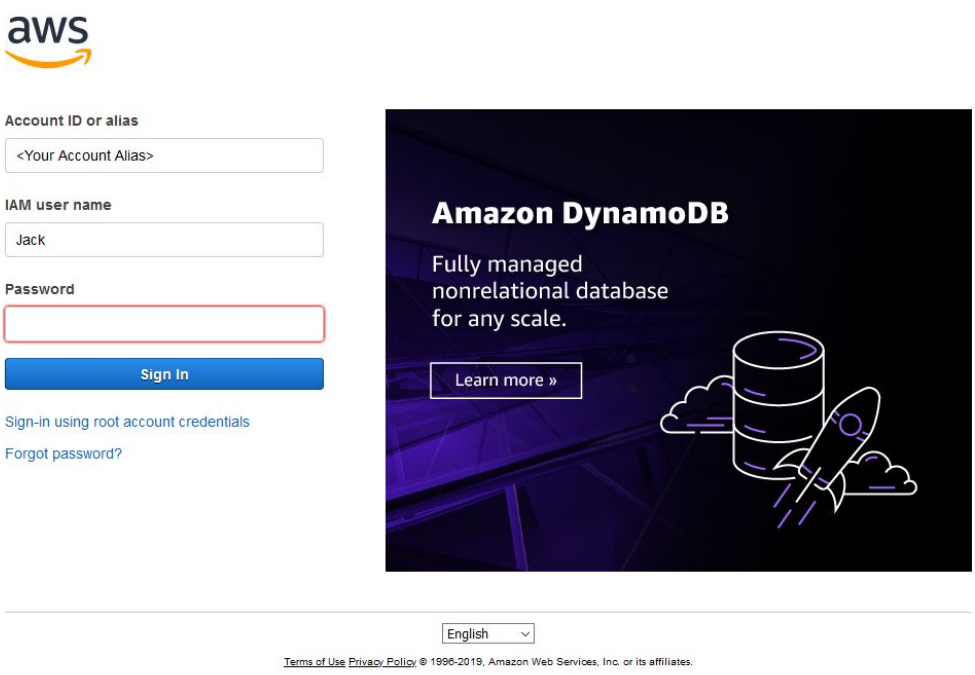


3. Don't forget that Unique Access ID, it is how you are going to login later.
4. Go to **Users** on the left and hit *Add User*.



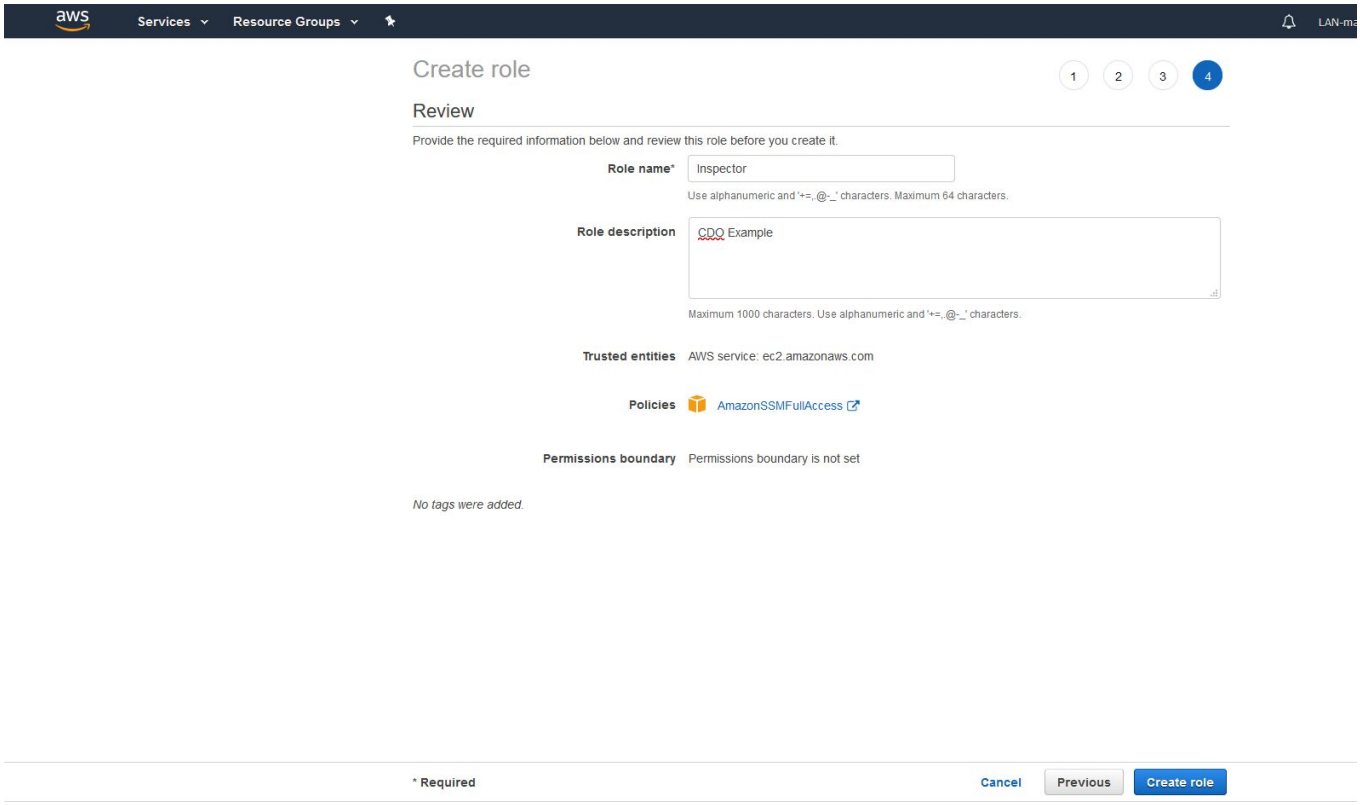
5. Name the User **Jack**
6. Select '*AWS Management Console access'*
7. Make a custom password and dont forget it.
    a. Uncheck *Require Password Reset*
8. Hit **Next**, on the bottom right.

9. Go to *Attach Existing Policies Directly*
    a. *Search for AWSCloudTrailFullAccess*
    b. Check it off and then hit **Next.**
10. Skip tags, hit **Next**, and review your actions.
11. Hit Create User on the bottom right.
12. Test it out, logout and sign back in with your Account Alias

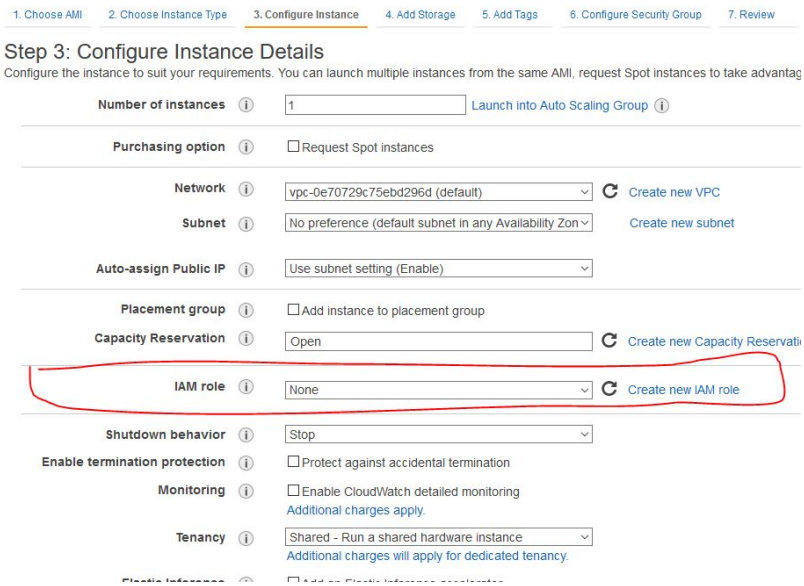


Inspector Hands On

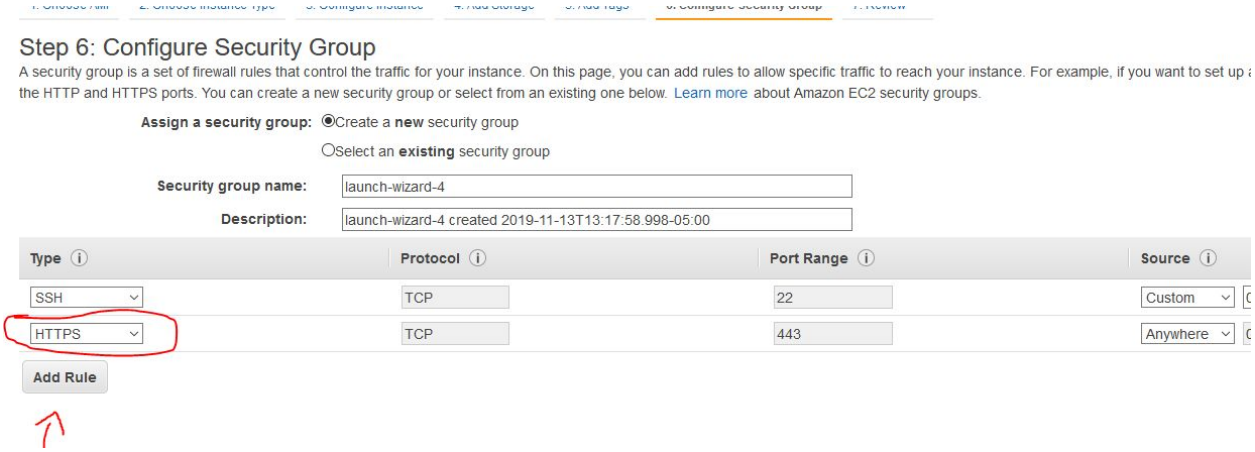
1. Return to the IAM Dashboard, You can hit **Services** in the top left to return to your Management Console.
2. Now hit **Roles** on the left side and click *Create Role*.
3. ***EC2*** will be using this service so go ahead and select that.
4. Hit **Next**.
5. On the policies screen, search for AmazonSSMFullAccess, check it off and hit next.
6. Again, skip the tags and go to the review screen, name the role **Inspector**
7. Finalize by hitting **Create Role.**



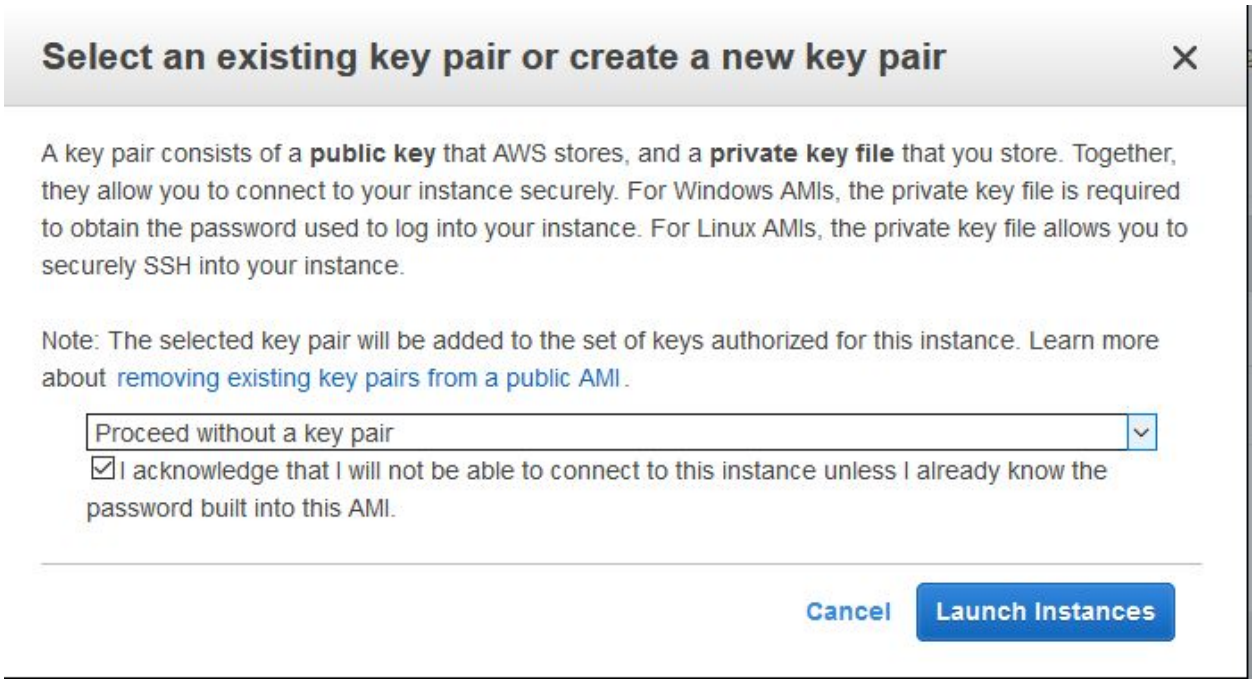
8. Now, go back to your **Services** on the top left and search for EC2.
9. On the left hit **Instances** and then *Launch Instance.*
10. Select the first AMI '**Amazon Linux 2 AMI (HVM), SSD Volume Type'** and hit **Next.**
11. Leave the defaults for the Instance Type and hit **Next.**
12. On Step 3, let's attach that role you just made to our new instance.



13. Hit **Next,** until you get to **Step 6 : Security Groups**
14. On the bottom, click add new rule and Allow **HTTPS** traffic from **ANYWHERE.**

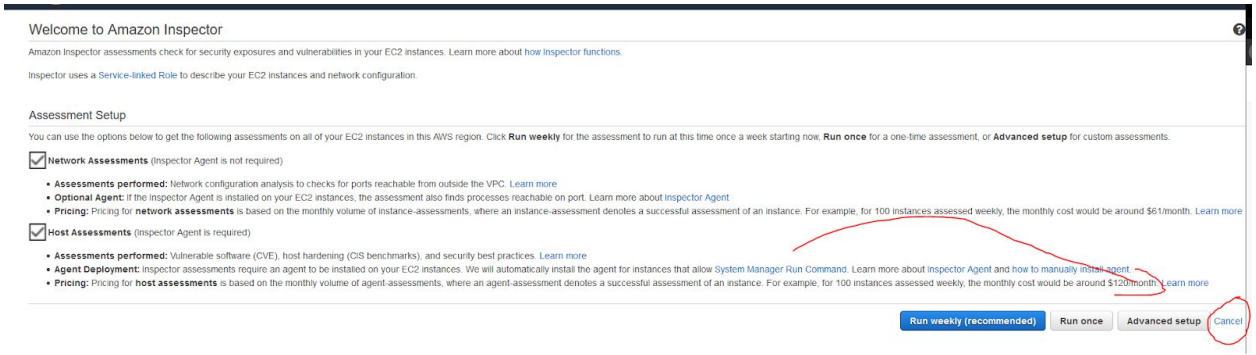


15. Click Review and Launch on the bottom, then upon clicking **Launch**
    a. Click *Proceed without a key pair.*
    b. Check off that you are aware and hit Launch Instances.



16. Congrats, you just created a virtual computer on the Cloud.
17. Now, go back to your **Services** on the top left and search for *Inspector*.
18. Hit *Get Started.*

19. AWS will launch it's configuration wizard, since I am going step by step just hit cancel all the way on the right.

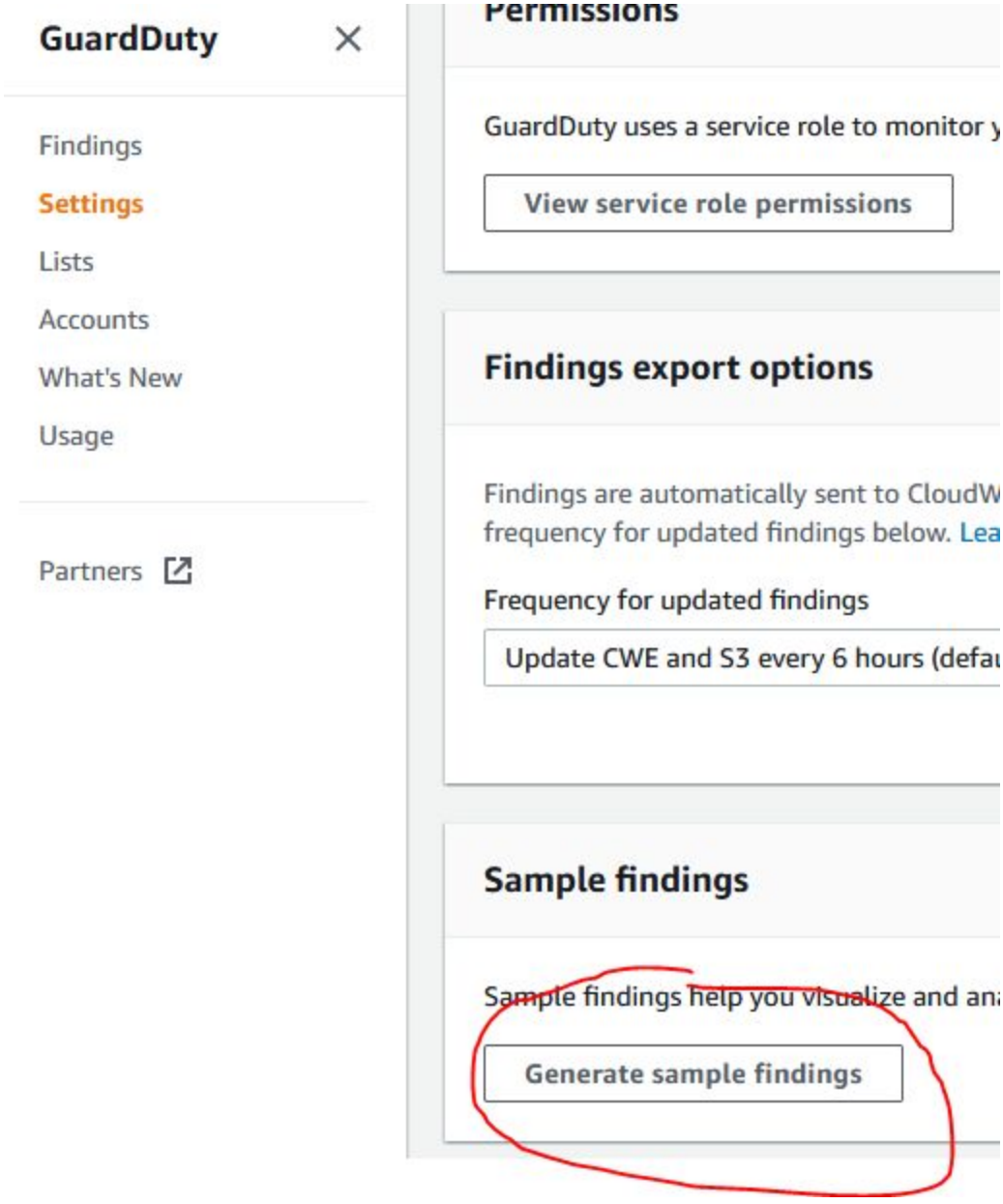


20. Next, hit **Assessment Targets** on the left and then **Create.**
21. Name your target, and then for simplicity sake, Check off *All Instances in this Region*.
22. Next, hit **Assessment Template** on the left and then **Create.**
    a. Name the Template
    b. Select the Target Group you just created.
    c. Select the *Common Vulnerabilities and Exposures* Package.
    d. Set the duration to 15 Minutes.
    e. Then uncheck the Assessment Schedule on the bottom.
    f. Hit **Create and Run**, on the bottom left.
23. This will take 15 minutes, so look up and watch me walk you through the **Web Application Firewall** portion of this Workshop.
24. After 15 minutes, look at your results!

GuardDuty Hands On

1. Now, go back to your **Services** on the top left and search for *GuardDuty*.
2. Hit Get Started for Guarduty.

3. Now hit **Enable GuardDuty**
4. On the left side hit **Settings,** then scroll down to **Generate Sample Findings**.



5. Look Around!

READ THIS IF YOU DO NOT WANT TO BE CHARGED

1. To prevent any charges to your AWS account do the following.
2. Go back to EC2 in your management console, click on *Running Instance*s.

3. Check off your instance that was created, hit **Actions,** hover over Instance State and hit **Terminate.**
4. Now go back to **GuardDuty,** and then settings, then scroll down to the bottom and hit ***Disable GuardDuty.***
5. At this point you will not be charged for anything in AWS, as nothing is running anymore.
6. However, if you do not plan on using AWS again, you can deactivate your account, but I recommend playing with it every now and then :)

THANKS FOR COMING!