

Cyber Defense Organization

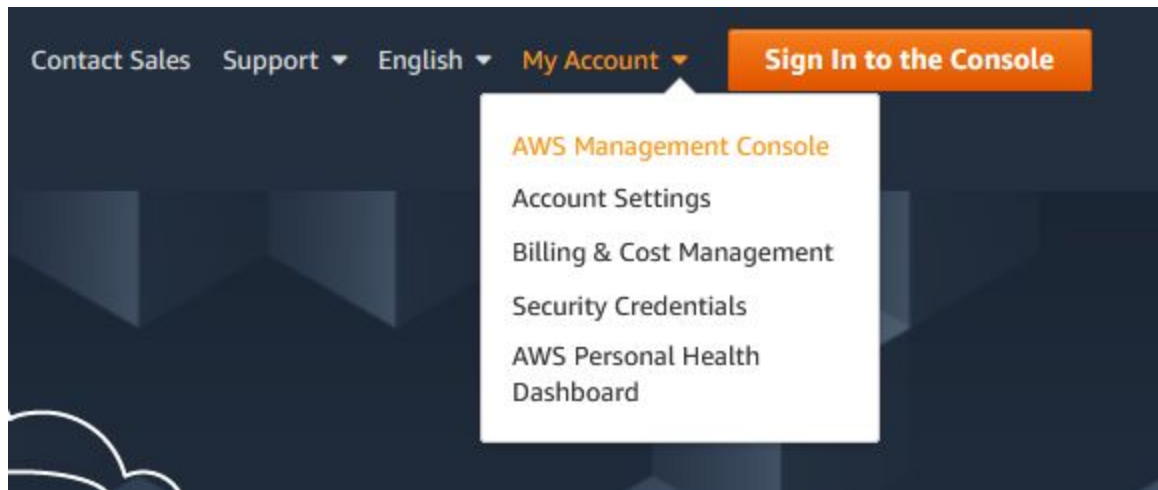


Cloud Security Instructions - Tyler Blanco 11/13/2019

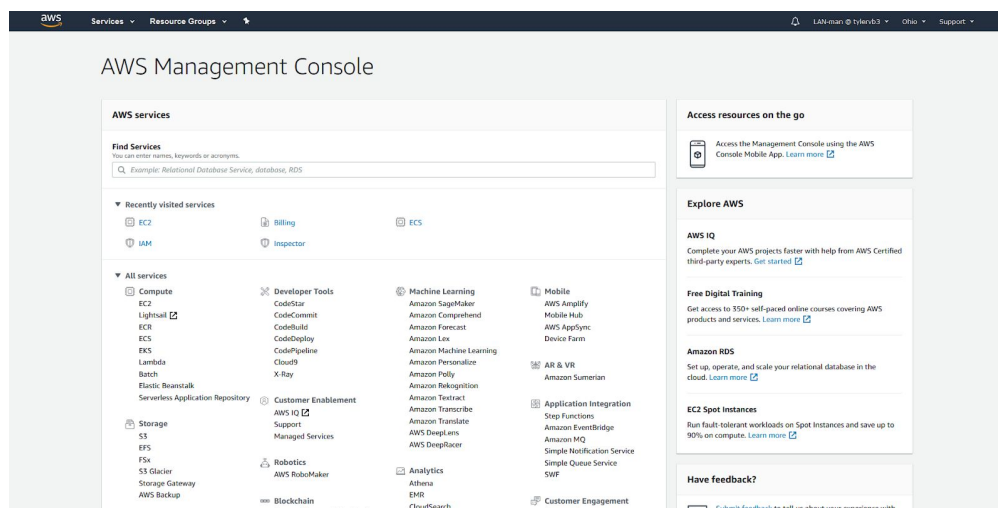
<https://tinyurl.com/CDO-CloudSecurity>

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.

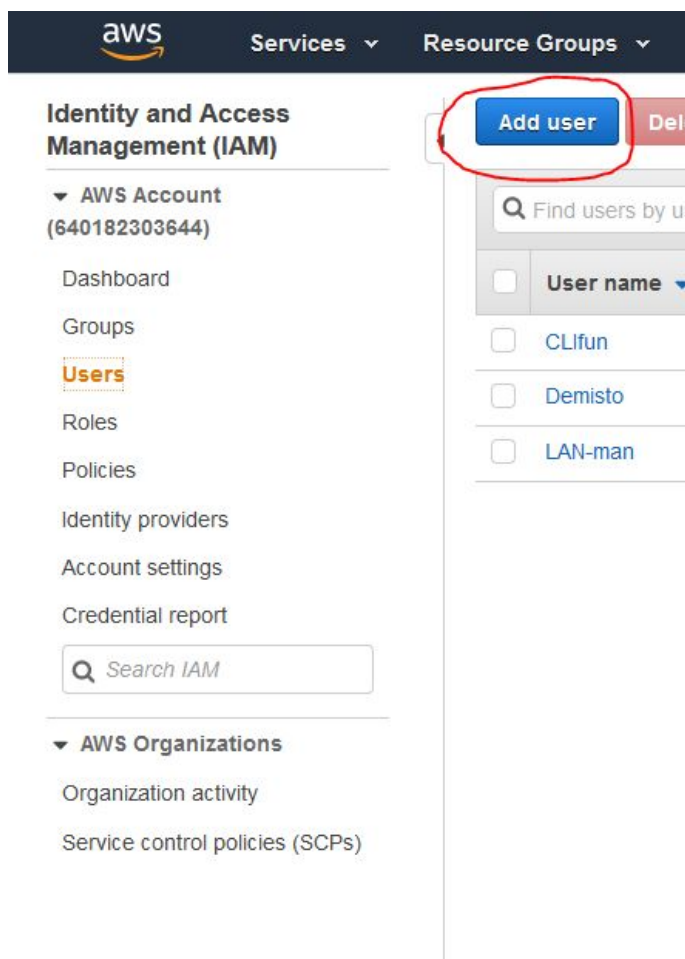
Welcome to Identity and Access Management

IAM users sign-in link:

<https://tylervb3.signin.aws.amazon.com/console>

[Customize](#)

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 don't 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

aws

Account ID or alias

<Your Account Alias>

IAM user name

Jack

Password

Sign In

Sign-in using root account credentials

Forgot password?

Amazon DynamoDB

Fully managed nonrelational database for any scale.

Learn more »

English

[Terms of Use Privacy Policy](#) © 1996-2019, Amazon Web Services, Inc. or its affiliates.

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**.

aws Services Resource Groups

Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name* Inspector
Use alphanumeric and '+=,@-_' characters. Maximum 64 characters.

Role description CDQ Example
Maximum 1000 characters. Use alphanumeric and '+=,@-_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies AmazonSSMFullAccess [↗](#)

Permissions boundary Permissions boundary is not set

No tags were added.

* Required

[Cancel](#) [Previous](#) [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.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of lower prices.

Number of instances ⓘ 1 [Launch into Auto Scaling Group](#) ⓘ

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ vpc-0e70729c75ebd296d (default) [↻](#) [Create new VPC](#)

Subnet ⓘ No preference (default subnet in any Availability Zone) [↻](#) [Create new subnet](#)

Auto-assign Public IP ⓘ Use subnet setting (Enable) [↻](#)

Placement group ⓘ ☐ Add instance to placement group

Capacity Reservation ⓘ Open [↻](#) [Create new Capacity Reservation](#)

IAM role ⓘ None [↻](#) [Create new IAM role](#)

Shutdown behavior ⓘ Stop [↻](#)

Enable termination protection ⓘ ☐ Protect against accidental termination

Monitoring ⓘ ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy ⓘ Shared - Run a shared hardware instance
[Additional charges will apply for dedicated tenancy.](#)

Private IP address ⓘ ☐ Assign Private IP address

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**.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group

☐ Select an existing security group

Security group name: launch-wizard-4

Description: launch-wizard-4 created 2019-11-13T13:17:58.998-05:00

Type ⁱ	Protocol ⁱ	Port Range ⁱ	Source ⁱ
SSH	TCP	22	Custom
HTTPS	TCP	443	Anywhere

Add Rule



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.

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more](#) about [removing existing key pairs from a public AMI](#).

Proceed without a key pair



☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

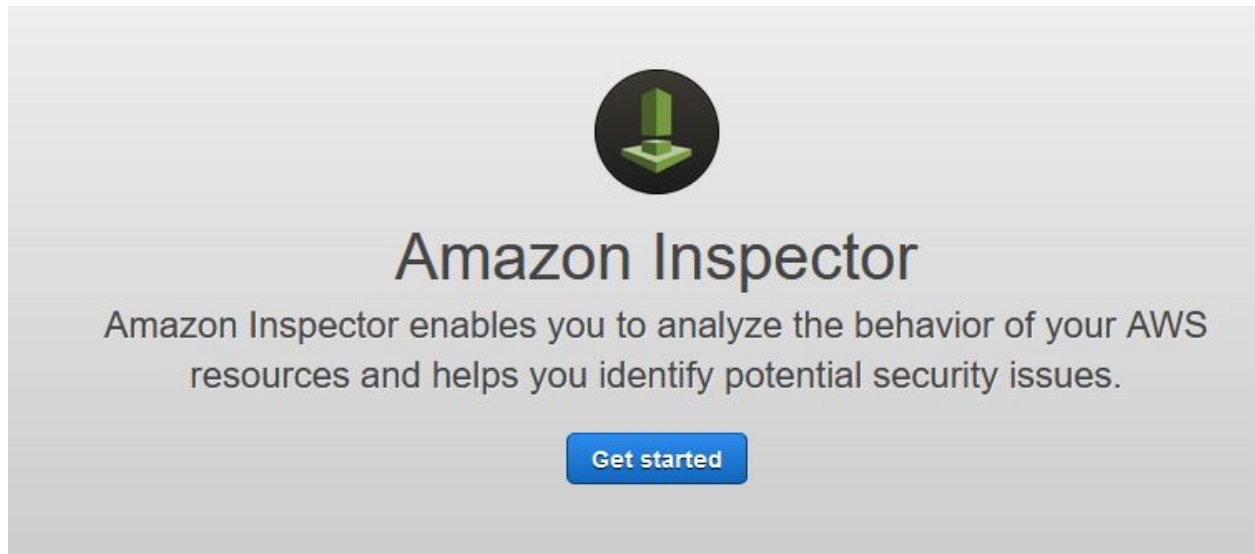
Cancel

Launch Instances

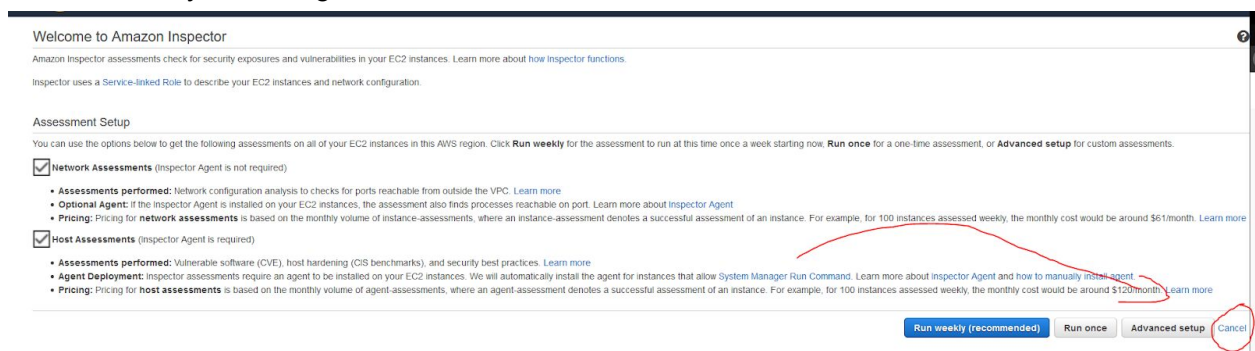
16. Congrats, you just created a virtual computer on the Cloud.

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**.

- Name the Template
- Select the Target Group you just created.
- Select the *Common Vulnerabilities and Exposures* Package.
- Set the duration to 15 Minutes.
- Then uncheck the Assessment Schedule on the bottom.
- Hit **Create and Run**, on the bottom left.

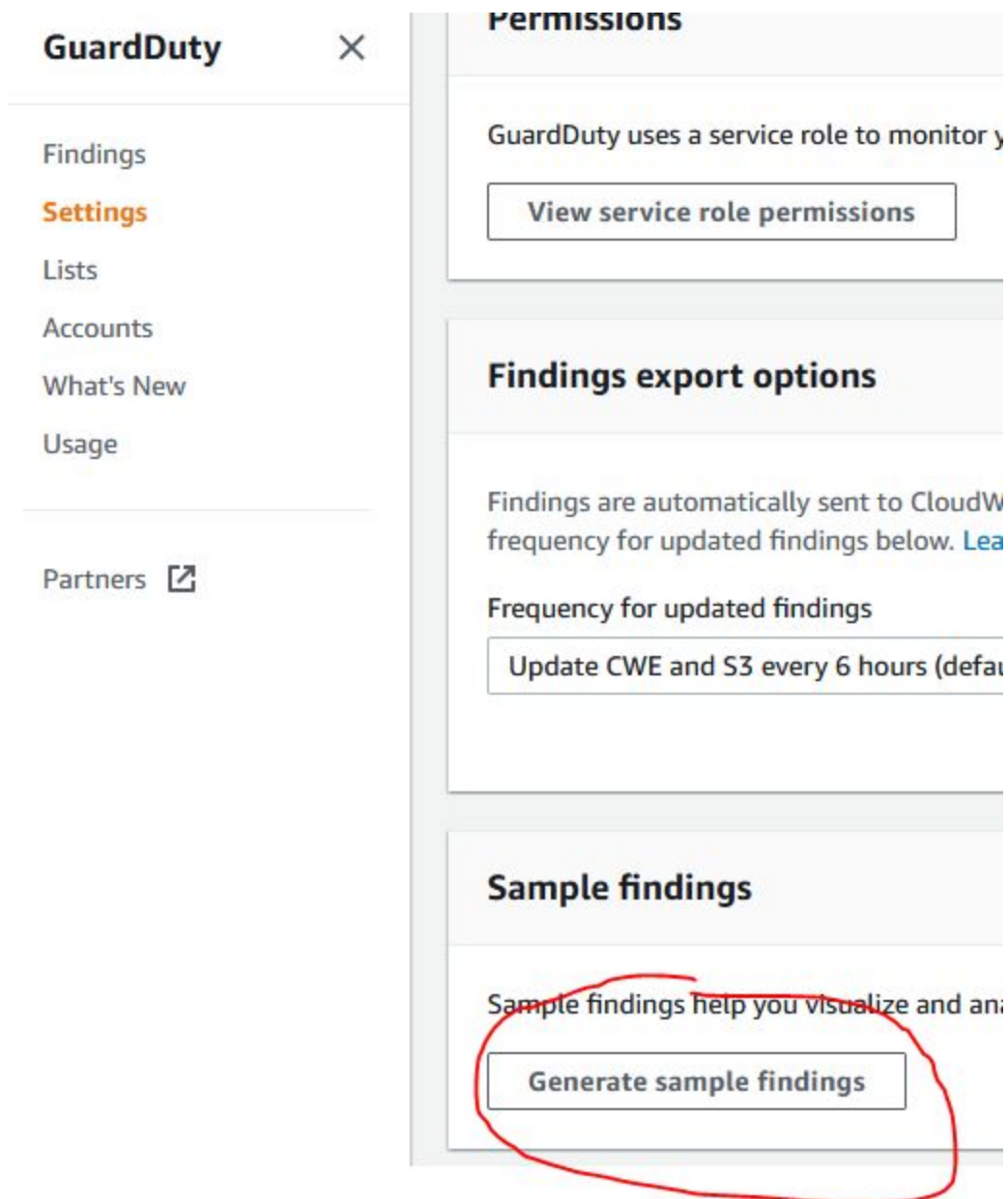
23. This will take 15 minutes, so look up and watch me walk you through the **Web Application Firewall** portion of this Workshop.

24. After 15 minutes, look at your results!

GuardDuty Hands On

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

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 Instances*.

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!