

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**

A screenshot of the AWS sign-in modal. It shows several options: AWS Management Console (which is highlighted), Account Settings, Billing & Cost Management, Security Credentials, AWS Personal Health Dashboard, and a large blue button labeled "Sign In to the Console".

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

A screenshot of the AWS Management Console homepage. The left sidebar lists various AWS services like EC2, S3, Lambda, and CloudWatch. The main content area shows sections for AWS services, access resources on the go, explore AWS, and have feedback. A search bar at the top is empty.

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>

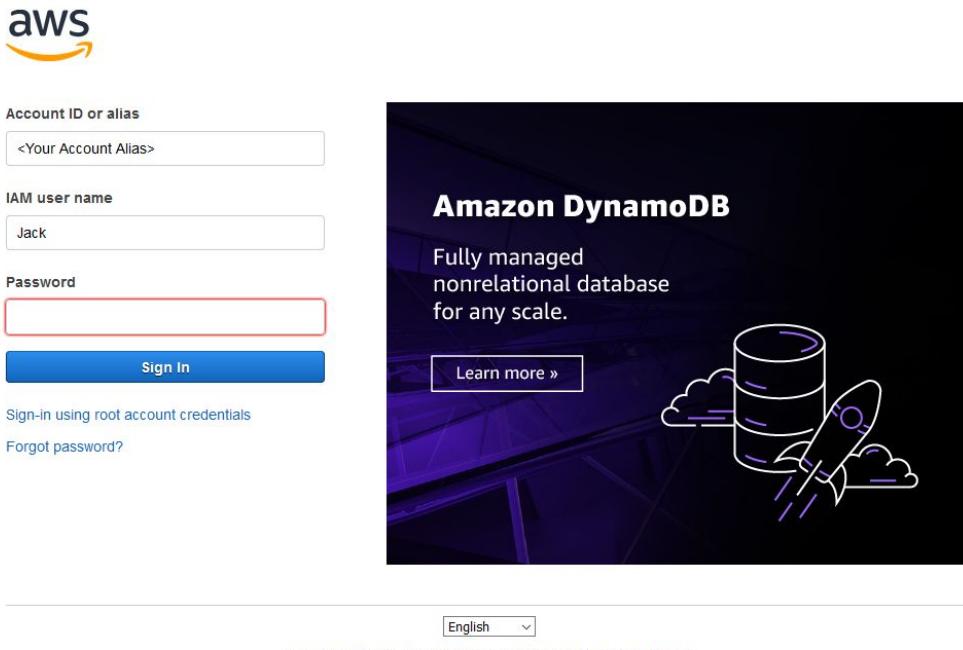
| Customize

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*.

The screenshot shows the AWS IAM console interface. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, and 'Resource Groups' dropdown. Below the navigation bar, the main title is 'Identity and Access Management (IAM)'. On the left, a sidebar menu lists several options: 'AWS Account (640182303644)', 'Dashboard', 'Groups', 'Users' (which is currently selected and highlighted in yellow), 'Roles', 'Policies', 'Identity providers', 'Account settings', and 'Credential report'. A search bar labeled 'Search IAM' is located below the sidebar. In the main content area, there's a large blue button labeled 'Add user' which is circled in red. Below this button is a search bar with the placeholder 'Find users by us'. Underneath the search bar is a table with a single column labeled 'User name'. The table contains four rows, each with a checkbox and a user name: 'CLIfun', 'Demisto', and 'LAN-man'. At the bottom of the table is a 'Delete' button. To the right of the main content area, there's a red circle highlighting the 'Customize' link in the top right corner of the page header.

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**.

AWS Services Resource Groups LAN-m...

Create role

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 CDO 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.

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, or use Auto Scaling to automatically manage the number of instances based on demand.

Number of instances Launch into Auto Scaling Group

Purchasing option Request Spot instances

Network Create new VPC

Subnet Create new subnet

Auto-assign Public IP

Placement group Add instance to placement group

Capacity Reservation Create new Capacity Reservation

IAM role Create new IAM role

Shutdown behavior

Enable termination protection Protect against accidental termination

Monitoring Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy
Additional charges will apply for dedicated tenancy.

Change instance type

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	Protocol	Port Range	Source
SSH	TCP	22	Custom Anywhere
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 X

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 its configuration wizard, since I am going step by step just hit cancel all the way on the right.

A screenshot of the Amazon Inspector Assessment Setup page. The page has a header "Welcome to Amazon Inspector" and a sub-header "Assessment Setup". It contains two sections: "Network Assessments (Inspector Agent is not required)" and "Host Assessments (Inspector Agent is required)". Both sections have checkboxes and detailed descriptions. At the bottom, there are four buttons: "Run weekly (recommended)", "Run once", "Advanced setup", and "Cancel". A red arrow points from the left towards the "Cancel" button, which is circled in red.

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 Guarduty.

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

The screenshot shows the AWS GuardDuty settings interface. On the left, a sidebar lists 'Findings', 'Settings' (which is selected and highlighted in orange), 'Lists', 'Accounts', 'What's New', and 'Usage'. Below this is a 'Partners' section with a link. The main content area has a header 'PERMISSIONS' with a note about using a service role. A button 'View service role permissions' is present. The next section, 'Findings export options', contains a note about automatic sending to CloudWatch Logs and a frequency dropdown set to 'Update CWE and S3 every 6 hours (default)'. The final section, 'Sample findings', contains a note about helping to visualize and analyze findings, followed by a button 'Generate sample findings'. A red oval highlights this button.

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!