

Home / AWS / Guided Lab / Introduction to Amazon GuardDuty

Introduction to Amazon GuardDuty

Level: Fundamental

Amazon Web Services Amazon GuardDuty



0h 28m 47s left



End Lab

Open Console

Validation

Lab Credentials

User Name ⓘ

Whiz_User_80425.26221120



Password ⓘ

4ded46a3-985f-4ef2-86f4-dd5328088ela



Access Key ⓘ

AKIAQ66O26BYOQF7TIQA



Secret Key ⓘ

4SgTqn6SQ7v/uUVNuUzO5RJ7M8f4TR8e0/De892o






Lab Resources


No Lab Resources Found

Support Documents

1. FAQs and Troubleshooting

Need help?

-  How to use Hands on Lab
-  Troubleshooting Lab
-  FAQs

[Submit Feedback](#)[Share](#)[Lab Overview](#)[Lab Steps](#)[Lab Validation](#) Cloud Security Engineer Security

Lab Steps

Task 1: Sign in to AWS Management Console

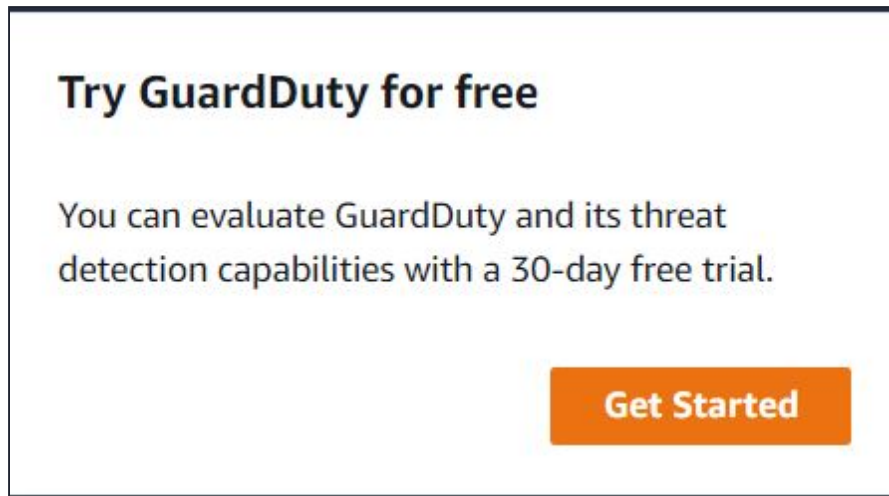
1. Click on the **Open Console** button, and you will get redirected to AWS Console in a new browser tab.
2. On the AWS sign-in page,
 - Leave the Account ID as default. Never edit/remove the 12 digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.
 - Now copy your **User Name** and **Password** in the Lab Console to the **IAM Username and Password** in AWS Console and click on the **Sign in** button.
3. Once Signed In to the AWS Management Console, Make the default AWS Region as **US East (N. Virginia) us-east-1**.

Note: There is no Validation function for this lab.

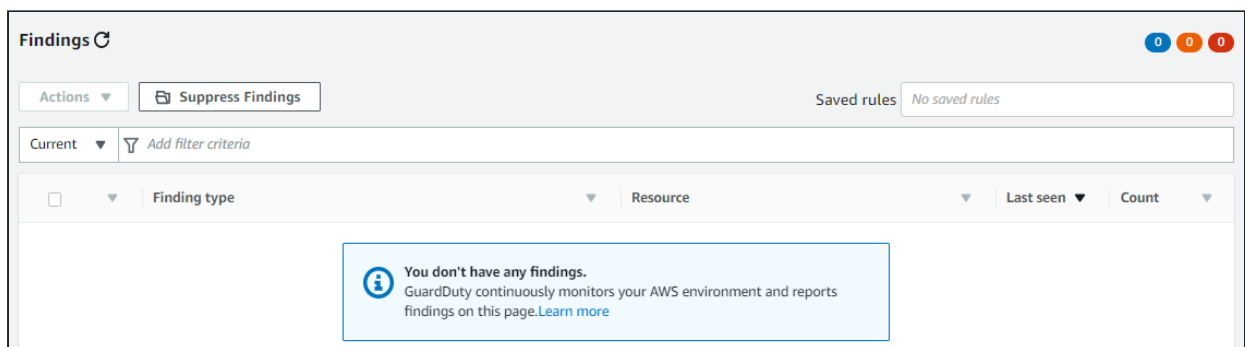
Task 2: Enabling Amazon GuardDuty

1. Make sure to choose the **US East (N. Virginia) us-east-1** region in the AWS Management console dashboard, which is present in the top right corner.

2. Navigate to the **Services** menu at the top and click on **GuardDuty** in the **Security, Identity and Compliance** section.
3. Click on **Get started**.



4. Click on **Enable GuardDuty**. With one click, the service will be enabled.



5. In the **Findings** page, you will see the warning **You don't have any findings** because there is no malicious activity happening in your AWS Account. **Ignore** the warnings, wherever you find.

Task 3: Exploring Amazon GuardDuty

Settings

1. Click on **Settings** in the left panel.
2. You will see a **Detector ID**. A detector is a resource that represents the GuardDuty service.
3. **Permissions**: GuardDuty uses a service role to monitor your data sources on your behalf.
4. Findings export options: Findings are automatically sent to CloudWatch Events. You can also export findings to an S3 bucket. New findings are exported within 5 minutes.

No need to change anything.

5. Suspend GuardDuty:

- **Suspend GuardDuty:** When you suspend GuardDuty, it stops monitoring your AWS environment and doesn't generate new findings. Your existing findings remain intact and aren't affected.
- **Disable GuardDuty:** When you disable GuardDuty, you not only stop GuardDuty from monitoring your AWS environment and generating new findings, you also lose your existing findings and your GuardDuty configurations. You can't recover the data later.

Lists

1. Click on **Lists** below **Settings**.
2. In the List Manager, you can add the Trusted IP Lists and Threat Lists.
3. **Trusted IP Lists:** Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists.
4. **Threat Lists:** Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists.

Trusted IP lists

Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. [Learn more](#)

+ Add a trusted IP list

| List name | List file URL | Format | Active |
|--|---------------|--------|--------|
| <div><div></div><div>Trusted IP lists Trusted IP lists consist of IP addresses that are whitelisted for secure communication with your AWS environment. GuardDuty does not generate findings for IP addresses that are included in trusted IP lists. Learn more</div></div> | | | |

Threat lists

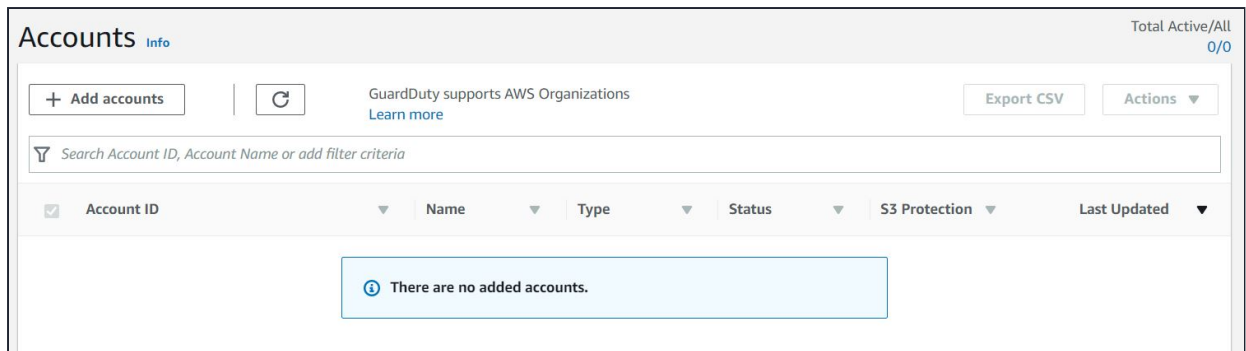
Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. [Learn more](#)

+ Add a threat list

| List name | List file URL | Format | Active |
|--|---------------|--------|--------|
| <div><div></div><div>Threat lists Threat lists consist of known malicious IP addresses. GuardDuty generates findings for IP addresses that are included in threat lists. Learn more</div></div> | | | |

Accounts


1. Click on **Accounts** above the settings.




2. You can invite other accounts to enable GuardDuty and become associated with your AWS account.
3. When an invitation is accepted, your account is designated as the **master** GuardDuty account.
4. The account that accepts the invitation becomes a **member** account associated with your master account.
5. You can then view and manage the GuardDuty findings on behalf of the member account. In GuardDuty, a master account (per region) can have up to 1000 member accounts.


Task 4: Generating Sample Findings

1. Since there are no potential threats in our AWS Account, let us generate some sample findings and learn about them.
2. Navigate to settings, scroll down and click on **Generate sample findings**.
3. To find your sample findings, go to **Findings**.
4. Wait until the loading is completed. On the top-right corner, you should see a number of findings.


Findings 


Showing 56 of 56 9 30 17








































Actions 

Suppress Findings 

Saved rules No saved rules

Current 

Add filter criteria 

|  |  | Finding type |  | Resource |  | Last seen  | Count  |
|---|---|---|---|----------------------|---|---|---|
|  |  |  [SAMPLE] UnauthorizedAccess:EC2/TorPCaller | | Instance: i-99999999 | | a minute ago | 1 |
|  |  |  [SAMPLE] Trojan:EC2/BlackholeTraffic | | Instance: i-99999999 | | a minute ago | 1 |
|  |  |  [SAMPLE] Recon:EC2/Portscan | | Instance: i-99999999 | | a minute ago | 1 |
|  |  |  [SAMPLE] Backdoor:EC2/DenialOfService.Tcp | | Instance: i-99999999 | | a minute ago | 1 |
|  |  |  [SAMPLE] Backdoor:EC2/DenialOfService.Udp | | Instance: i-99999999 | | a minute ago | 1 |
|  |  |  [SAMPLE] UnauthorizedAccess:EC2/RDPBruteForce | | Instance: i-99999999 | | a minute ago | 1 |
|  |  |  [SAMPLE] Backdoor:EC2/DenialOfService.UdpOnTcpPorts | | Instance: i-99999999 | | a minute ago | 1 |
|  |  |  [SAMPLE] Recon:EC2/PortProbeUnprotectedPort | | Instance: i-99999999 | | a minute ago | 1 |
|  |  |  [SAMPLE] UnauthorizedAccess:EC2/TorClient | | Instance: i-99999999 | | a minute ago | 1 |
|  |  |  [SAMPLE] Recon:EC2/PortProbeEMRUnprotectedPort | | Instance: i-99999999 | | a minute ago | 1 |
|  |  |  [SAMPLE] UnauthorizedAccess:EC2/TorRelay | | Instance: i-99999999 | | a minute ago | 1 |

5. On the Top-right corner, you can see numbers with colors.

6. Color Indications:

- The **Blue** indicates **Low severity**
- **Orange** indicates **Medium severity**
- **Red** indicates **High severity**

7. You can use filter criteria to filter your findings.

Findings

Showing 56 of 56

93017

Actions

Suppress Findings

Saved rulesNo saved rules

Current

Add filter criteria

| | | Resource | Last seen | Count |
|--------------------------|-------------------------|-----------------------|---------------|-------|
| <input type="checkbox"/> | Access Key ID | | | |
| <input type="checkbox"/> | Account ID | | | |
| <input type="checkbox"/> | Action type | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | API call service name | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | API called | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | API caller ASN ID | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | API caller ASN name | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | API caller city | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | API caller country | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | API caller IPv4 address | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | API caller type | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | DNS request domain | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | Finding ID | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | Finding type | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | IAM instance profile ID | Instance: i-999999999 | 5 minutes ago | 1 |
| <input type="checkbox"/> | Instance ID | Instance: i-999999999 | 5 minutes ago | 1 |

8. Click on one of the sample findings.

9. You can see various parameters like **severity, region, Account ID, Resource ID, Resource Affected, Target, etc.**

The screenshot shows the Amazon GuardDuty Findings console. The main panel displays a list of findings with columns for Finding type, Resource, and Count. The finding '[SAMPLE] Recon:EC2/Portscan' is highlighted. The right panel provides details for this finding, including its severity (MEDIUM), region (us-east-1), account ID, resource ID (i-99999999), and the resource affected (EC2 instance i-99999999).

| Finding type | Resource | Count |
|---|-----------------------|-------|
| [SAMPLE] UnauthorizedAccess:EC2/TorIPCal... | Instance: i-999999999 | 1 |
| [SAMPLE] Trojan:EC2/BlackholeTraffic | Instance: i-999999999 | 1 |
| [SAMPLE] Recon:EC2/Portscan | Instance: i-999999999 | 1 |
| [SAMPLE] Backdoor:EC2/DenialOfService.Tcp | Instance: i-999999999 | 1 |
| [SAMPLE] Backdoor:EC2/DenialOfService.Udp | Instance: i-999999999 | 1 |
| [SAMPLE] UnauthorizedAccess:EC2/RDPBrut... | Instance: i-999999999 | 1 |
| [SAMPLE] Backdoor:EC2/DenialOfService.U... | Instance: i-999999999 | 1 |
| [SAMPLE] Recon:EC2/PortProbeUnprotecte... | Instance: i-999999999 | 1 |
| [SAMPLE] UnauthorizedAccess:EC2/TorClient | Instance: i-999999999 | 1 |
| [SAMPLE] Recon:EC2/PortProbeEMRUnprot... | Instance: i-999999999 | 1 |
| [SAMPLE] UnauthorizedAccess:EC2/TorRelay | Instance: i-999999999 | 1 |

Recon:EC2/Portscan
Finding ID: 90b802ca9769f8d742bc25edca1afa9a

Severity: MEDIUM
Region: us-east-1
Count: 1
Account ID: [Redacted]
Resource ID: i-99999999
Created at: 02-02-2020 16:37:07 (...)
Updated at: 02-02-2020 16:37:07 (...)

Resource affected

| Resource role | Resource type |
|---------------|---------------|
| ACTOR | Instance |

| Instance ID | Port |
|-------------|-------|
| i-99999999 | 24844 |

| Port name | Instance type |
|-----------|---------------|
| | |

10. Go through the sample to learn more about the different severities.

Task 5: Validation of the Lab

- Once the labs steps are completed, please click on **Validation** button on right side panel.
- This will validate the resources in the AWS account and displays whether you have completed this lab successfully or not.
- Sample Output:

The screenshot shows the WhizLabs interface for the 'Introduction to Amazon GuardDuty' lab. The 'Lab Validation' section is active, displaying a 'Check your Validation' message and a 'Validate My Lab' button. The right panel shows the lab's progress, including a timer (0h 28m 24s left), buttons for 'End Lab', 'Open Console', and 'Validation', and a section for 'Lab Credentials' (User Name, Password, Access Key).

WHIZLABS Lab Library Cloud Sandboxes My Activity

Home / AWS / Guided Lab / Introduction to Amazon GuardDuty

Introduction to Amazon GuardDuty

Level: Fundamental

Amazon Web Services Amazon GuardDuty

Lab Overview Lab Steps Lab Validation

Check your Validation

If any checks fail ✖, you can use the remaining time it the Lab to work on making the checks pass ✔. Click Validate My Lab again to rerun the checks at any time.

Validate My Lab

Login to AWS Management Console

Check whether you have logged in to AWS Management Console

Lab Validation

0h 28m 24s left

End Lab

Open Console

Validation

Lab Credentials

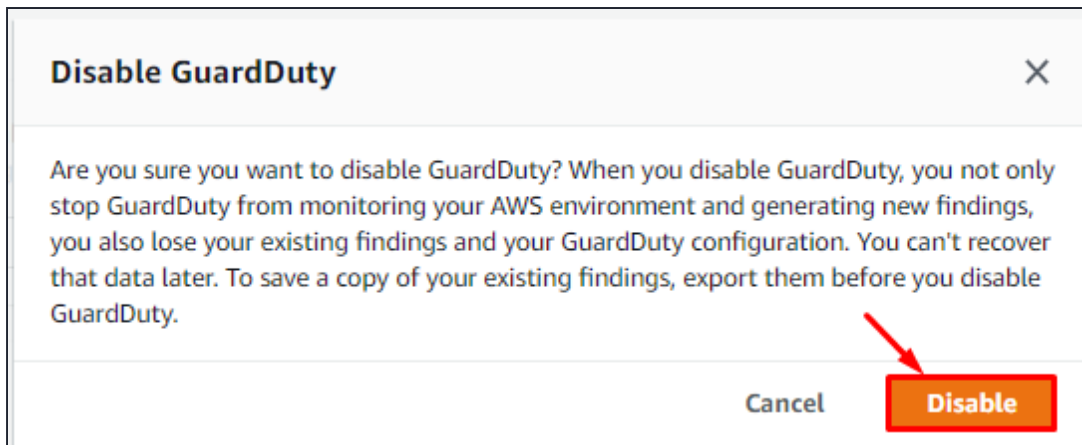
User Name ⓘ
Whiz_User_80706.83741841

Password ⓘ
56806cfc-637e-43a6-b19a-3423379f49x

Access Key ⓘ
AKIAT2HWZBDN5MPPSO6Z

Task 6: Disabling GuardDuty

- Go to the settings and click on **DisableGuardDuty** under suspend GuardDuty to stop it.
- Click on **Disable** to confirm.



3. You have successfully disabled GuardDuty.

Do You Know ?

Amazon GuardDuty analyzes and monitors billions of events across your AWS accounts, including API calls, network traffic, and DNS data, to identify potential security threats and anomalies.

Completion and Conclusion

- You have successfully used the AWS management console to enable Amazon GuardDuty.
- You have successfully explored the options of Amazon GuardDuty Service like Settings, Lists, and Accounts.
- You have generated some sample findings and reviewed them.
- You have successfully disabled Amazon GuardDuty.

End Lab

1. Sign out of AWS Account.
2. You have successfully completed the lab.
3. Once you have completed the steps click on **End Lab** from your whizlabs dashboard.

