**Activating a GuardDuty Threat List**

### Introduction

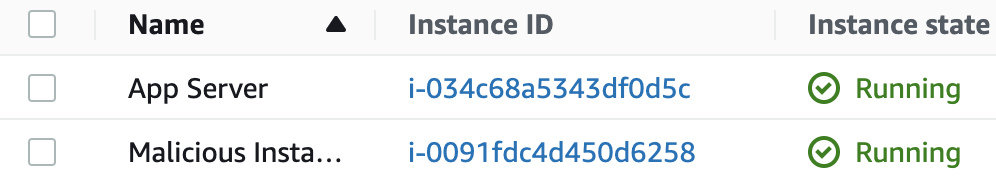
Amazon GuardDuty analyzes its data sources to find potential security threats. You can influence the security findings that GuardDuty reports through trusted IP lists and threat lists. Trusted IP lists whitelist IP addresses from being included in GuardDuty's findings to reduce false positives. Threat lists include known malicious IP addresses. GuardDuty reports additional findings for IP addresses in threat lists.

You will activate a threat list that includes the IP address of an EC2 instance that is part of the Cloud Academy Lab environment. The environment consists of two EC2 instances in different VPCs. The instances are configured to communicate with each other. You will see the findings GuardDuty discovers regarding communicating with malicious instances in a later lab step.

### Instructions

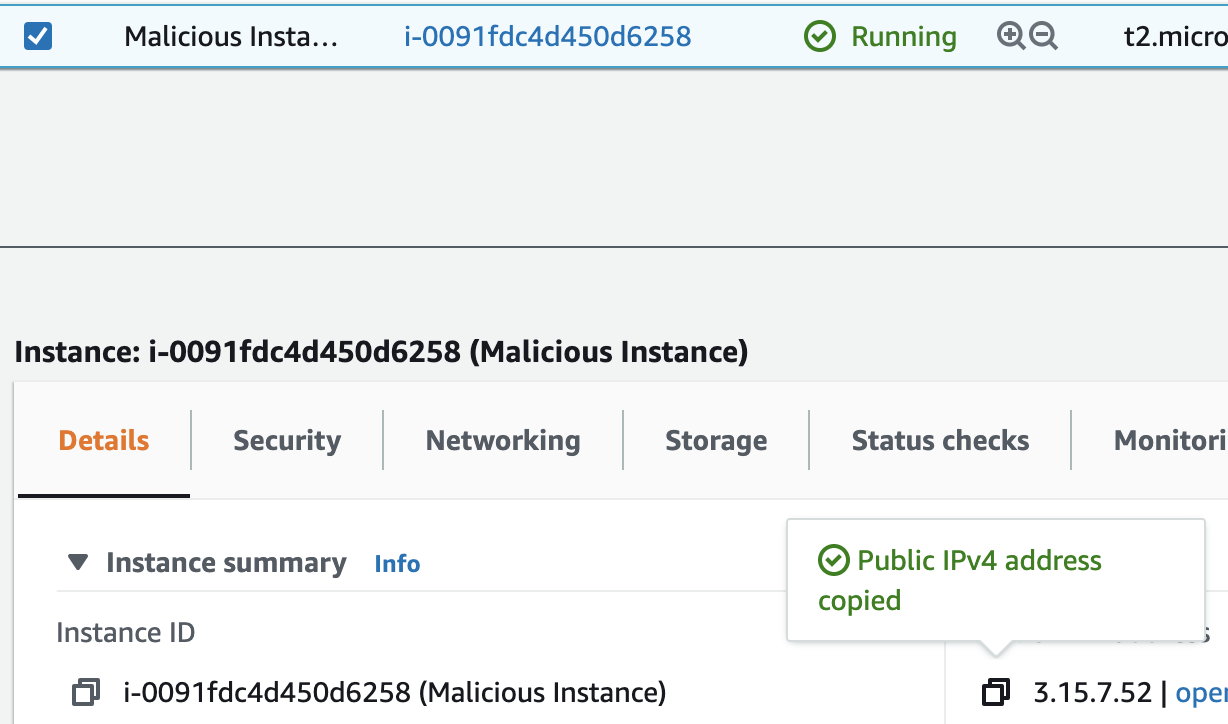
1. [Open the EC2 console](https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#Instances:sort=instanceId) to view the instances in the Lab environment.

There are two EC2 instances to focus on for this lab: **Malicious Instance**, and **App Server**:



You may also see another instance but it is not important for this lab step.

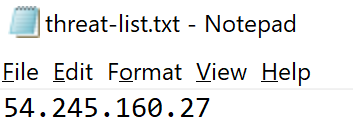
2. Select **Malicious Instance** and copy its IPv4 Public IP:



The Public IP address is what is needed for GuardDuty's threat list. DNS names and private IP addresses are ignored in threat lists.

3. Save the IP address in a plain text file named threat-list.txt.

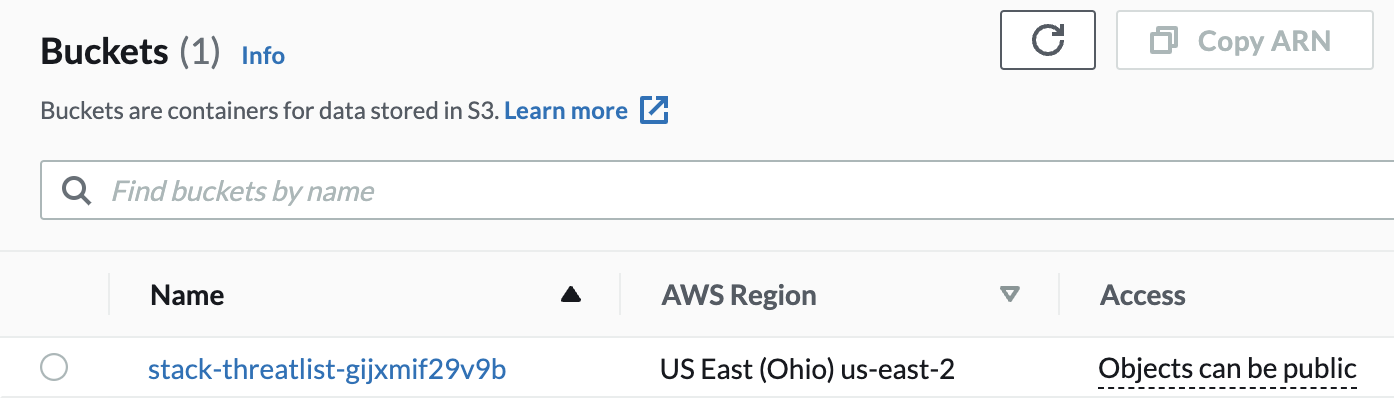
GuardDuty requires a file on Amazon S3 to create a threat list. As an example on Windows, you could use Notepad and the file contents would look similar to the following:



Similarly, you could use TextEdit on macOS.

4. [Open the Amazon S3 console](https://s3.console.aws.amazon.com/s3/home?region=us-east-2).

The Cloud Academy Lab environment has created a bucket for you to upload the threat list:



5. Click on the bucket containing **threatlist** in the name.

6. Click **Upload** to open the S3 upload wizard.

7. Click **Add files** and select the threat-list.txt file you created earlier.

8. Click **Upload**in the lower-right corner to upload the file with the default S3 file configuration.

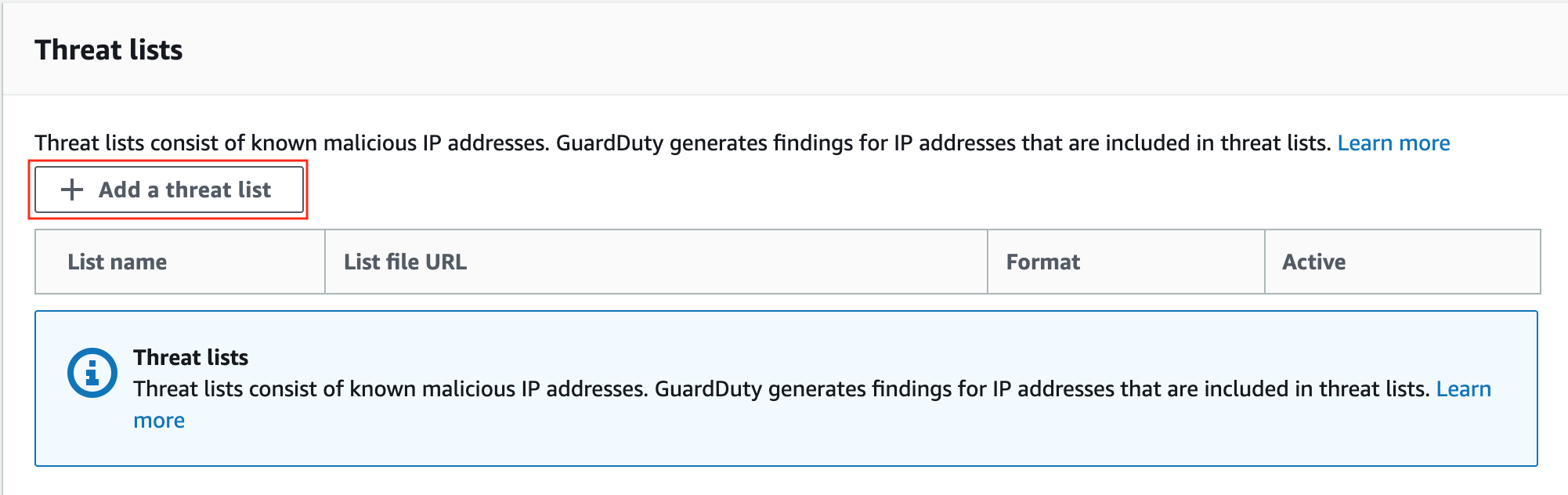
9. Click threat-list.txt to open its details in a new tab, and copy the **Object URL**in the **Object overview** panel:



10. Return to the GuardDuty Console, and select **Lists** in the left sidebar.

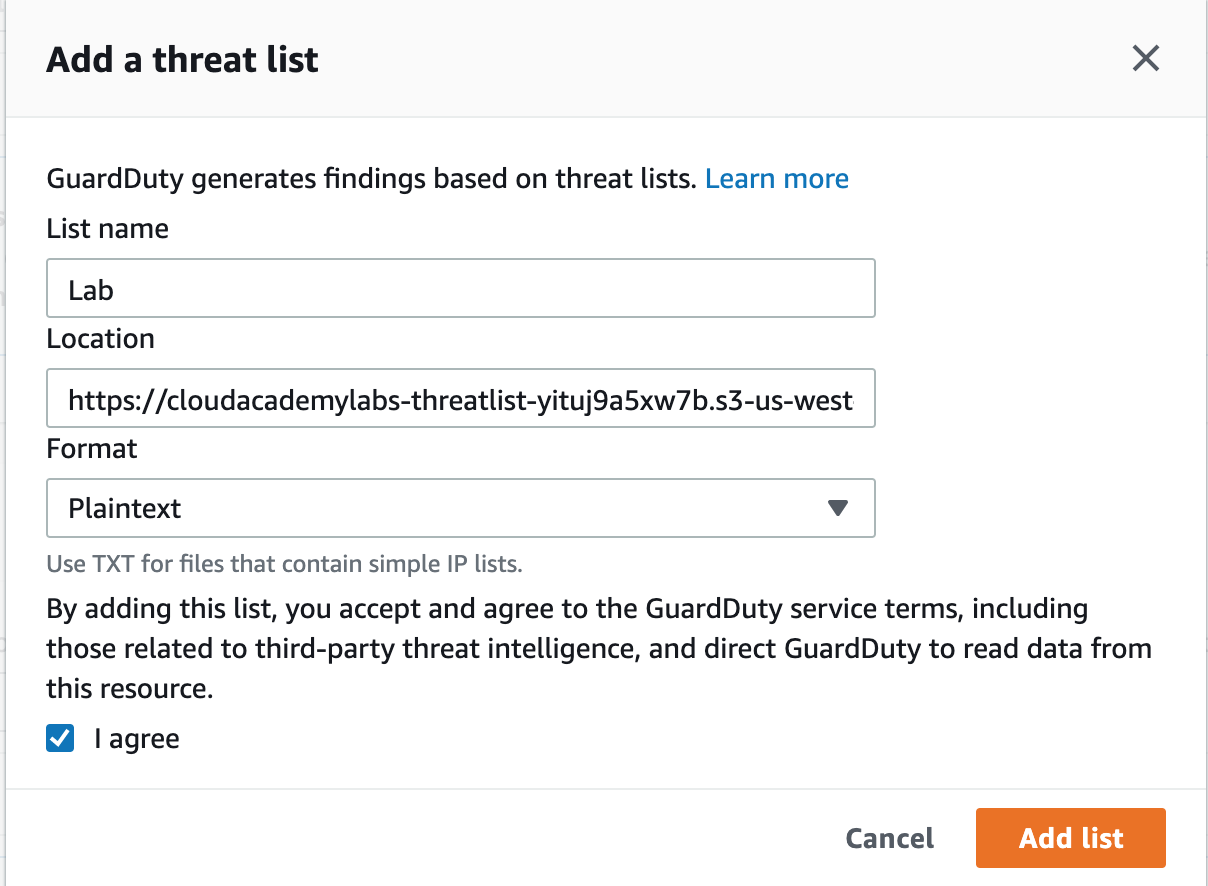
Note: You may already see some **Findings** in the GuardDuty Console. GuardDuty does not require a threat list to make findings. It will only report additional findings for IP addresses in the threat list.

11. Click **Add a threat list** to create a threat list:



12. In the **Add a threat list**form, enter the following values and click **Add list**:

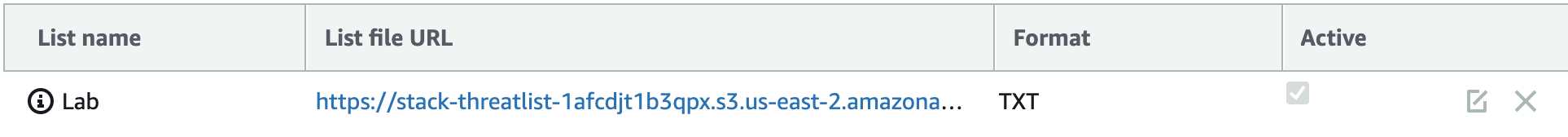
* **List name**: Lab
* **Location**: Paste in the S3 link you copied a few instructions ago
* **Format**: Plaintext (Notice that the drop-down lists other formats that can be used if you have existing threat intelligence services to import threat lists from)
* **I agree**: checked



A success confirmation appears:



13. Check the **Active**checkbox to activate the threat list:



The message warns that it can take up to **5 or more minutes to take effect**. The small threat list you uploaded is active in seconds, but it can take five or more minutes for new GuardDuty to report new findings related to the threat list. You will view sample GuardDuty finding in the next lab step while waiting for the new findings to appear.

### Summary

In this lab step, you have activated a threat list in GuardDuty. You began by listing IP addresses in a file. Then you uploaded the file to S3, and created a threat list in GuardDuty. Lastly, you activated the threat list. No new findings related to the threat list will be made unless the threat list is active.