Work with AWS VPC Flow Logs for Network Monitoring

01:32:37 Exit Lab Complete Lab

Guided Mode 1 hour 45 minutes duration Professional Rate this lab

Videos Guide

Introduction

Monitoring network traffic is a critical component of security best practices to meet compliance requirements, investigate security incidents, track key metrics, and configure automated notifications. AWS VPC Flow Logs captures information about the IP traffic going to and from network interfaces in your VPC. In this hands-on lab, we will set up and use VPC Flow Logs published to Amazon CloudWatch, create custom metrics and alerts based on the CloudWatch logs to understand trends and receive notifications for potential security issues, and use Amazon Athena to query and analyze VPC flow logs stored in S3.

Solution

Log in to the live AWS environment using the credentials provided. Make sure you are using `us-east-1` (N. Virginia) as the selected Region.

Create a CloudWatch Log Group and VPC Flow Logs to CloudWatch

Create a VPC Flow Log to S3

1. Navigate to **VPC**.
2. In the VPC dashboard, select the **VPCs** card.

   You should see an **A Cloud Guru** VPC pre-provisioned for the lab.
3. Check the checkbox next to the **A Cloud Guru** VPC.
4. Toward the bottom of the screen, select the **Flow logs** tab.
5. On the right, click **Create flow log**.
6. Fill in the flow log details:
   - **Name**: You can leave this field blank.
   - **Filter**: Ensure that **All** is selected.
   - **Maximum aggregation interval**: Select **1 minute**.
   - **Destination**: Select **Send to an Amazon S3 bucket**.
7. Get the S3 bucket ARN:
   - In a new browser tab, navigate to **S3**.
   - Select the radio button next to the provided bucket.
   - Click **Copy ARN**.
8. Navigate back to the **VPC Management Console** tab and fill in the rest of the flow log details:
   - **S3 bucket ARN**: In the text field, paste your copied S3 bucket ARN.
   - **Log record format**: Ensure that **AWS default format** is selected.
9. Leave the other fields as the default settings and click **Create flow log**.

   Your flow log is created.
10. From the **Your VPCs** page, select the **Flow logs** tab.
11. Review the flow log details and verify that it shows an **Active** status.
12. Navigate back to the **S3 Management Console** tab.
13. Select your bucket name, and then select the **Permissions** tab.

14. Review the bucket policy and note that it is modified automatically by AWS when you create flow logs so that the flow logs can write to the bucket.

> **Note**: It can take between 5–15 minutes for flow logs to appear. You can continue working through the other lab objectives while you wait for the flow logs to populate.

Create the CloudWatch Log Group and VPC Flow Log

1. In a new browser tab, navigate to **CloudWatch**.
2. In the CloudWatch sidebar menu, navigate to **Logs** and select **Log groups**.
3. Click **Create log group**.
4. In the **Log group name** field, enter *VPCFlowLogs*.
5. Click **Create**.
6. Navigate back to the **VPC Management Console** tab and ensure the **Flow logs** tab is still selected.
7. On the right, click **Create flow log**.
8. Fill in the flow log details:
    - **Name**: You can leave this field blank.
    - **Filter**: Ensure that **All** is selected.
    - **Maximum aggregation interval**: Select **1 minute**.
    - **Destination**: Ensure that **Send to CloudWatch Logs** is selected.
    - **Destination log group**: Click into the field and select your **VPCFlowLogs** log group.
    - **IAM role**: Use the dropdown to select the **DeliverVPCFlowLogsRole** role.
    - **Log record format**: Ensure that **AWS default format** is selected.
9. Click **Create flow log**.

    Your flow log is created.
10. From the **Your VPCs** page, ensure the **Flow logs** tab is selected.
11. Review the flow log details and verify that the new flow log shows an **Active** state.
12. Navigate back to the **CloudWatch Management Console** tab.
13. Select the **VPCFlowLogs** log group name.

    You should see there are currently no log streams. Remember, it may take some time before the flow logs start populating data.

Generate Network Traffic

1. In a new browser tab, navigate to **EC2**.
2. In the **Resources** section of the EC2 dashboard, select **Instances (running)**.

    You should see a **Web Server** instance that was pre-provisioned for the lab.
3. Check the checkbox next to the **Web Server** instance.
4. In the instance's **Details** tab, copy the **Public IPv4 address**.
5. Open a terminal session and log in to the EC2 instance using the credentials provided for the lab:

    ```
    ssh cloud_user@<PUBLIC-IP-ADDRESS>
    ```
    Now that you have connected to the terminal successfully, the VPC flow logs will record for this connection.
6. Exit the terminal:

    ```
    logout
    ```
7. Navigate back to the **EC2 Management Console** tab.
8. Update the EC2 instance security group:

- Check the checkbox next to the **Web Server** instance, and then use the **Actions** dropdown to select **Security** > **Change security groups**.
- In the **Associated security groups** section, click **Remove** to the right of the security group details to remove the **SecurityGroupHTTPAndSSH** group.
- Use the search bar in the **Associated security groups** section to select the **SecurityGroupHTTPOnly** security group.
- Click **Add security group**, and then click **Save**.

9. Navigate back to your terminal session and reconnect to the EC2 instance using the credentials provided for the lab:

   ```
   cloud_user@<PUBLIC-IP-ADDRESS>
   ```

   This time, your connection should time out because you removed SSH access with the security group change. This will be recorded in VPC Flow Logs as a reject record.

10. Press **Ctrl+C** to cancel the SSH command.
11. Navigate back to the **EC2 Management Console** tab.
12. Revert the EC2 instance security group back to **SecurityGroupHTTPAndSSH**:
    - Ensure the **Web Server** instance is selected, and then use the **Actions** dropdown to select **Security** > **Change security groups**.
    - In the **Associated security groups** section, click **Remove** to the right of the security group details to remove the **SecurityGroupHTTPOnly** group.
    - Use the search bar in the **Associated security groups** section to select the **SecurityGroupHTTPAndSSH** security group.
    - Click **Add security group**, and then click **Save**.
13. Navigate back to your terminal session and reconnect to the EC2 instance using the credentials provided for the lab:

    ```
    ssh cloud_user@<PUBLIC-IP-ADDRESS>
    ```

    This time, the connection should be accepted.

Create CloudWatch Filters and Alerts

Create a CloudWatch Log Metric Filter

1. Navigate back to the **CloudWatch Management Console** tab.
2. In the CloudWatch sidebar menu, navigate to **Logs** and select **Log groups**.
3. Select the **VPCFlowLogs** log group name.

   You should now see a log stream. If you don't see a log stream listed yet, wait a few more minutes and refresh the page until the data appears.

4. Select the listed log stream name and review the data.
5. Use the breadcrumb along the top of the page to select **VPCFlowLogs**.
6. Select the **Metric filters** tab and then click **Create metric filter**.
7. In the **Filter pattern** field, enter the following pattern to track failed SSH attempts on port 22:

   ```
   [version, account, eni, source, destination, srcport, destport="22", protocol="6", packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]
   ```

8. Use the **Select log data to test** dropdown to select **Custom log data**.
9. In the **Log event messages** field, replace the existing log data with the following:

   ```
   2 086112738802 eni-0d5d75b41f9befe9e 61.177.172.128 172.31.83.158 39611 22 6 1 40 1563108188 1563108227 REJECT OK
   2 086112738802 eni-0d5d75b41f9befe9e 182.68.238.8 172.31.83.158 42227 22 6 1 44 1563109030 1563109067 REJECT OK
   2 086112738802 eni-0d5d75b41f9befe9e 42.171.23.181 172.31.83.158 52417 22 6 24 4065 1563191069 1563191121 ACCEPT OK
   2 086112738802 eni-0d5d75b41f9befe9e 61.177.172.128 172.31.83.158 39611 80 6 1 40 1563108188 1563108227 REJECT OK
   ```

10. Click **Test pattern** and then review the results.
11. Click **Next**.
12. Fill in the metric details:
    - **Filter name**: In the text field, enter *dest-port-22-reject*.
    - **Metric namespace**: In the text field, enter a name (e.g., *vpcflowlogs*).
    - **Metric name**: In the text field, enter **SSH Rejects**.

- **Metric value**: In the text field, enter **1**.

13. Leave the other fields blank and click **Next**.
14. Review the metric details and then click **Create metric filter**.

Create an Alarm Based on the Metric Filter

1. After the metric filter is created, ensure that the **Metric filters** tab is selected.
2. In the **Metric filter** details, check the checkbox to the right of the **dest-port-22-reject** filter.
3. On the right, click **Create alarm**.

   The **Alarms** page opens in a new browser tab automatically.
4. Specify the metric conditions:
   - **Period**: Use the dropdown to select **1 minute**.
   - **Threshold type**: Ensure that **Static** is selected.
   - **Whenever SSH Rejects is...**: Select **Greater/Equal**.
   - **than...**: In the text field, enter *1*.

   The metric will trigger an alarm whenever there is one or more reject messages within a one-minute period.
5. Click **Next**.
6. Configure the alarm actions:
   - **Alarm state trigger**: Ensure that **In alarm** is selected.
   - **Send a notification to the following SNS topic**: Select **Create a new topic**.
   - **Create a new topic...**: Leave the default topic name.
   - **Email endpoints that will receive the notification...**: In the text field, enter an email address (this can be your real email address or a sample address like ***user@example.com***), and then click **Create topic**.

> **Note**: If you entered your real email address, open your email inbox and click the **Confirm Subscription** link you received in the SNS email.

7. Click **Next**.
8. In the **Alarm name** field, enter *SSH rejects*.
9. Click **Next**.
10. Review the alarm details and then click **Create alarm**.

    The alarm is created but will take some time to start populating data.

Generate Traffic for Alerts

1. Navigate back to the terminal session and reconnect to the EC2 instance using the credentials provided for the lab:

   ```
   ssh cloud_user@<PUBLIC-IP-ADDRESS>
   ```
2. Exit the terminal:

   ```
   logout
   ```
3. Navigate back to the **EC2 Management Console** tab.
4. Update the EC2 instance security group:
   - Check the checkbox next to the **Web Server** instance, and then use the **Actions** dropdown to select **Security** > **Change security groups**.
   - In the **Associated security groups** section, click **Remove** to the right of the security group details to remove the **SecurityGroupHTTPAndSSH** group.
   - Use the search bar in the **Associated security groups** section to select the **SecurityGroupHTTPOnly** security group.
   - Click **Add security group**, and then click **Save**.
5. Navigate back to your terminal session and reconnect to the EC2 instance using the credentials provided for the lab:

   ```
   ssh cloud_user@<PUBLIC-IP-ADDRESS>
   ```

Again, this will be recorded as a reject record, since you no longer have SSH access.

6. Press **Ctrl+C** to cancel the SSH command.
7. Navigate back to the **EC2 Management Console** tab.
8. Revert the EC2 instance security group back to **SecurityGroupHTTPAndSSH**:
   - Ensure the **Web Server** instance is selected, and then use the **Actions** dropdown to select **Security** > **Change security groups**.
   - In the **Associated security groups** section, click **Remove** to the right of the security group details to remove the **SecurityGroupHTTPOnly** group.
   - Use the search bar in the **Associated security groups** section to select the **SecurityGroupHTTPAndSSH** security group.
   - Click **Add security group**, and then click **Save**.
9. Navigate back to the **CloudWatch Alarms** tab and refresh the alarms details.

   You should see that the alarm state is now **In alarm**. If you attached the alarm to your email address, you should receive a notification about this alarm.

> **Note**: If the alarm state still shows **Insufficient data**, wait another moment or two and then refresh the alarms details again.

Use CloudWatch Logs Insights

1. In the CloudWatch sidebar menu, navigate to **Logs** and select **Logs Insights**.
2. Use the **Select log group(s)** search bar to select **VPCFlowLogs**.
3. In the right-hand pane, select **Queries**.
4. In the **Sample queries** section, expand **VPC Flow Logs** and then expand **Top 20 source IP addresses with highest number of rejected requests**.
5. Click **Apply** and note the changes applied in the query editor.
6. Click **Run query**.

   After a few moments, you'll see some data start to populate.

Analyze VPC Flow Logs Data in Athena

Create the Athena Table

1. Navigate back to the **S3** browser tab and then navigate to your **Buckets**.
2. Select the provisioned bucket name to open it.
3. Select the **AWSLogs/** folder, and then continue opening the subfolders until you reach the **<DAY>** folder containing the logs.
4. In the top right, click **Copy S3 URI**.
5. Paste the URI into a text file, as you'll need it shortly.
6. In a new browser tab, navigate to **Athena**.
7. On the right, click **Launch query editor**.
8. Select the **Settings** tab and then click **Manage**.
9. In the **Location of query result** field, paste your copied S3 URI.
10. Click **Save**.

Create Partitions and Analyze the Data

1. Select the query editor's **Editor** tab.
2. In the **Query 1** editor, paste the following query, replacing `{your_log_bucket}` and `{account_id}` with your log bucket and account ID details (you can pull these from the S3 URI path you copied):

```
CREATE EXTERNAL TABLE IF NOT EXISTS default.vpc_flow_logs (
  version int,
  account string,
  interfaceid string,
```

```
  sourceaddress string,
  destinationaddress string,
  sourceport int,
  destinationport int,
  protocol int,
  numpackets int,
  numbytes bigint,
  starttime int,
  endtime int,
  action string,
  logstatus string
)
PARTITIONED BY (dt string)
ROW FORMAT DELIMITED
FIELDS TERMINATED BY ' '
LOCATION 's3://{your_log_bucket}/AWSLogs/{account_id}/vpcflowlogs/us-east-1/'
TBLPROPERTIES ("skip.header.line.count"="1");
```

3. Click **Run**.

   You should see a message indicating that the query was successful.

4. On the right, click the **+** icon to open a new query editor.

5. In the editor, paste the following query, replacing `YYYY-MM-DD` with the current date, and replacing the existing location with your copied S3 URI:

```
ALTER TABLE default.vpc_flow_logs
    ADD PARTITION (dt='YYYY-MM-DD')
    location 's3://{your_log_bucket}/AWSLogs/{account_id}/vpcflowlogs/us-east-1/YYYY/MM/DD/';
```

6. Click **Run**.

   You should see a message indicating that the query was successful.

7. On the right, click the **+** icon to open a new query editor.

8. In the editor, paste the following query:

```
SELECT day_of_week(from_iso8601_timestamp(dt)) AS
     day,
     dt,
     interfaceid,
     sourceaddress,
     destinationport,
     action,
     protocol
   FROM vpc_flow_logs
   WHERE action = 'REJECT' AND protocol = 6
   order by sourceaddress
   LIMIT 100;
```

9. Click **Run**.

   Your partitioned data should display in the query results.

Conclusion

Congratulations on successfully completing this hands-on lab!

Tools

Lab Diagram Instant Terminal

Credentials

How do I connect?

AWS Account

Username

cloud_user

Password

71![5tGmjF!L[cOAc4Yr

Open Link in Incognito Window

Cloud Server EC2 instance

Username

cloud_user

Password

V-kw&2Ye

Public IP address of EC2 instance

3.228.13.107

Launch Instant Terminal

Additional Resources

Log in to the live AWS environment using the credentials provided. Make sure you are using `us-east-1` (N. Virginia) as the selected Region.

CloudWatch Log Metric Filter Pattern

```
[version, account, eni, source, destination, srcport, destport="22", protocol="6", packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]
```

Custom Log Data to Test

```
2 086112738802 eni-0d5d75b41f9befe9e 61.177.172.128 172.31.83.158 39611 22 6 1 40 1563108188 1563108227 REJECT OK
2 086112738802 eni-0d5d75b41f9befe9e 182.68.238.8 172.31.83.158 42227 22 6 1 44 1563109030 1563109067 REJECT OK
2 086112738802 eni-0d5d75b41f9befe9e 42.171.23.181 172.31.83.158 52417 22 6 24 4065 1563191069 1563191121 ACCEPT OK
2 086112738802 eni-0d5d75b41f9befe9e 61.177.172.128 172.31.83.158 39611 80 6 1 40 1563108188 1563108227 REJECT OK
```

Create Athena Table

```
CREATE EXTERNAL TABLE IF NOT EXISTS default.vpc_flow_logs (
  version int,
  account string,
  interfaceid string,
  sourceaddress string,
  destinationaddress string,
  sourceport int,
  destinationport int,
```

```
  protocol int,
  numpackets int,
  numbytes bigint,
  starttime int,
  endtime int,
  action string,
  logstatus string
) PARTITIONED BY (
  dt string
) ROW FORMAT DELIMITED FIELDS TERMINATED BY ' ' LOCATION 's3://{your_log_bucket}/AWSLogs/{account_id}/vpcflowlogs/us-east-1/' TBLPROPERTIES ("skip.header.line.count"="1");
```

Create Partitions

```
ALTER TABLE default.vpc_flow_logs
ADD PARTITION (dt='YYYY-MM-DD') location 's3://{your_log_bucket}/AWSLogs/{account_id}/vpcflowlogs/us-east-1/YYYY/MM/DD';
```

Analyze Data

```
SELECT day_of_week(from_iso8601_timestamp(dt)) AS
  day,
  dt,
  interfaceid,
  sourceaddress,
  destinationport,
  action,
  protocol
FROM vpc_flow_logs
WHERE action = 'REJECT' AND protocol = 6
order by sourceaddress
LIMIT 100;
```

Learning Objectives

0 of 4 completed

Optional: Run progress checks to confirm you've completed the objectives

- Create a CloudWatch Log Group and a VPC Flow Log to CloudWatch
- Create CloudWatch Filters and Alerts
- Use CloudWatch Logs Insights
- Analyze VPC Flow Logs Data in Athena