Enable AWS VPC Flow Logs

Risk level: Medium (generally tolerable level of risk)

Once enabled, the Flow Logs feature will start collecting network traffic data to and from your Virtual Private Cloud (VPC), data that can be useful to detect and troubleshoot security issues and make sure that the network access rules are not overly permissive.

Enabling VPC Flow Logs will help you detect security and access issues like overly permissive security groups and network ACLs and alert abnormal activities triggered within your Virtual Private Cloud network such as rejected connection requests or unusual levels of data transfer. *Notes: Availability: this feature is not available yet in the following AWS regions: Asia Pacific (Seoul) and South America (Sao Paulo).*
Pricing: since the Flow Log records are made available through AWS CloudWatch, the standard CloudWatch Logs pricing is applied ($0.50 per GB ingested and $0.03 per GB archived / month).

Audit

To determine if your VPC network has Flow Logs enabled, perform the following:

Console

01 Sign in to the AWS Management Console.

02 Navigate to VPC dashboard at https://console.aws.amazon.com/vp

03 In the left navigation panel, select **Your VPCs**.

04 Select the VPC that you need to check.

05 Select the **Flow Logs** tab from the bottom panel.

06 And search for any Flow Logs entries available for the selected VPC.

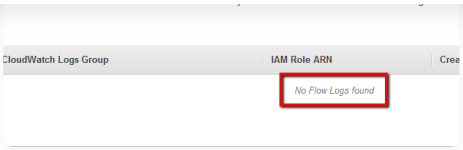
07 If there are no Flow Logs created, the

01 Run **describe-vpcs** command (OSX/Linux/UNIX) to list the VPC networks available in the current AWS region:

```
1  aws ec2 describe-vp
```

02 The command output should expose each VPC ID and its metadata:

```
1  {
2      "Vpcs": [
3          {
4              "VpcId"
5              "Instar
6              "Tags"
7                  {
8
9
```




```
13                "DhcpOp
14                "CidrBl
15                "IsDefa
16            }
17        ]
18    }
```

03 Run **describe-flow-logs** command (OSX/Linux/UNIX) using the VPC ID to determine if the selected virtual network has the Flow Logs feature enabled:

```
1    aws ec2 describe-fl
2      --filter "Name=re
```

04 If there are no Flow Logs created for the selected VPC, the command output will return an empty list **[]**:

```
1    {
2        "FlowLogs": []
```

Remediation / Resolution

To enable Flow Logs for your VPC, you need to create first an IAM role that will grant permissions to publish flow log streams to the specified log group in CloudWatch Logs

Step 1: create the IAM role.

Using AWS Console

Using AWS CLI

02 Navigate to IAM dashboard at https://console.aws.amazon.com/iam/.

03 In the left navigation panel, click **Policies**.

04 Click **Create Policy** button from the IAM dashboard top menu.

05 Select **Create Your Own Policy** and type a name and a description (optional) for the policy.

06 In the **Policy Document** field, paste the following custom IAM policy:

```
{
  "Version": "2012-
    "Statement": [
        {
          "Effect"
          "Action"
            "logs:C
            "logs:C
            "logs:D
```

create the IAM role required for publishing the flow logs:

```
aws iam create-role
  --role-name VPC-F
  --assume-role-pol
```

02 Run **get-role** command (OSX/Linux/UNIX) using the role name to make sure the IAM role has been successfully created:

```
aws iam get-role
  --role-name VPC-F
```

03 The command output should return a JSON object (https://en.wikipedia.org/wiki/JSON) containing the IAM role metadata:

```
{
    "Role": {
```

```
13
14              "Resource
15                "arn:aw
16            ]
17             }
18        ]
19    }
20
21
22
23
24
```

```
6                   {
7
8
9
10
11
12                  }
13              ]
14          },
15          "RoleId": "
16          "CreateDate
17          "RoleName"
18          "Path": "/"
19          "Arn": "arn
20      }
21  }
```

07 Click **Create Policy**.

08 In the left navigation panel, click **Roles**.

09 Click the **Create New Role** button from the IAM dashboard top menu and follow the wizard:

A. Enter a name for the IAM role.

C. Search for the policy name created earlier and select it:

D. Click **Next Step**.

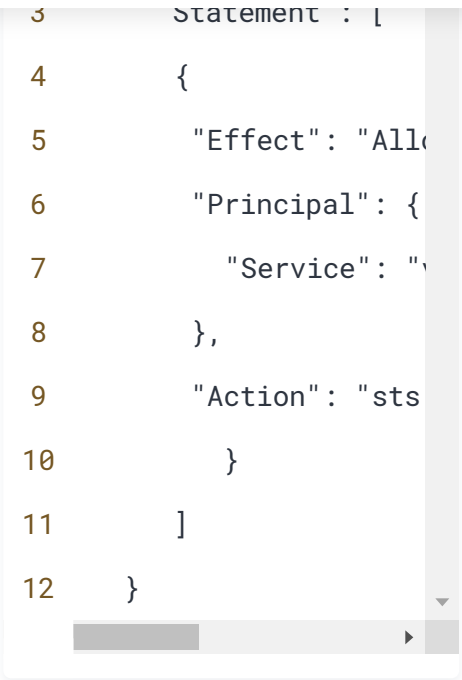
E. Review the IAM role information and click **Create Role**.

10 In the left navigation panel, click **Roles**.

11 Select the newly created IAM role.

12 Select **Trust Relationships** tab from the bottom panel and click **Edit Trust Relationship**.

13 Paste the following access control policy document and click **Update Trust Policy**:



Step 2: enable VPC Flow Logs

Using AWS Console

Using AWS CLI

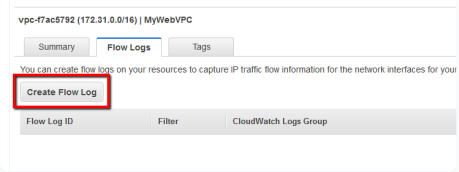
01 Sign in to the AWS Management Console.

02 Navigate to VPC dashboard at https://console.aws.amazon.com/vpc/.

03 In the left navigation panel, select **Your VPCs**.

04 Select the VPC that you need to check.

05 Select the **Flow Logs** tab from the bottom panel and click **Create Flow Log**:



06 In the **Create Flow Log** dialog box, enter the following details:

01 Run **create-flow-logs** command (OSX/Linux/UNIX) to create a flow log for the selected VPC, in the current AWS region. The following example creates a flow log that captures all traffic for the VPC network with the ID vpc-f7ac5792. The flow logs are delivered to a log group called MyFlowLogs, using an IAM role named VPC-Flow-Logs-Role:

```
1  aws ec2 create-flo
2    --resource-type
3    --resource-ids vp
4    --traffic-type AL
5    --log-group-name
6    --deliver-logs-pe
```

02 The command output should return the new flow log ID:

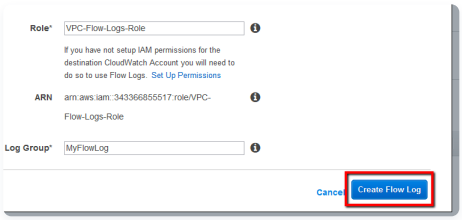
```
3       "FlowLogIds":
4           "fl-272ec84
5       ],
6       "ClientToken":
7   }
```

be logged – accepted, rejected, or all.

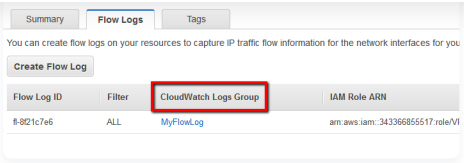
B. **Role**: enter the name of the IAM role that will allow permissions to publish to the CloudWatch Logs log group.

C. **Destination Log Group**: enter a name for the new CloudWatch Logs log group, where the flow logs will be published.

07 Review the flow log configuration and click **Create Flow Log**:



The log group will be available in approximately 10 minutes after you create the flow log. To access it, just click on the log



or open the CloudWatch Logs dashboard at https://console.aws.amazon.com/cloudwatch/home#logs:

References

AWS Documentation

Security in Your VPC

VPC Flow Logs

Creating IAM Roles

Creating a Role to Delegate Permissions to an AWS Service

Overview of IAM Policies

Install and Configure the CloudWatch Logs Agent on an Existing EC2 Instance

AWS Command Line Interface (CLI) Documentation

describe-vpcs

create-role

get-role

describe-flow-logs

create-flow-logs

AWS Blog(s)

VPC Flow Logs – Log and View Network Traffic Flows

Publication date Apr 8, 2016

Create Route Table for Private Subnets (Security)

Create NAT Gateways in at Least Two Availability Zones (Security)

Ineffective Network ACL DENY Rules (Security)

Create Route Table for Public Subnets (Security)

Advanced
Technology
Partner

Security Competency

Cloud Management
Tools Competency

Features
Pricing
Auto-Remediation
API Documentation
Help

Careers
Knowledge base
FAQ
Contact
Blog

Terms and Conditions — Privacy Policy
SaaS Agreement