**Domain: Networking and Content Delivery**

**Topic: VPC Flow Logs**

**Task: Publishing flow logs to CloudWatch Logs**

**Problem to Be Solved**

*In this task we’re going to configure VPC Flow logs to publish flow log data directly to Amazon CloudWatch.*

## Explanation of the Solution

*When publishing to CloudWatch Logs, flow log data is published to a log group, and each network interface has a unique log stream in the log group. Log streams contain flow log records.*

* *Flow Logs can be created for VPC, Network Interfaces or Subnets.*
* *If the Flow Logs are configured for a VPC , All the subnets and the network interfaces within that VPC will be monitored.*
* *If the Flow Logs are enabled on the subnet level , Then the network interfaces within that subnet will be monitored.*
* *The Flow Logs data which are collected from network interfaces, subnets or VPC is referred to as Flow Log records.*

## Implementation Details

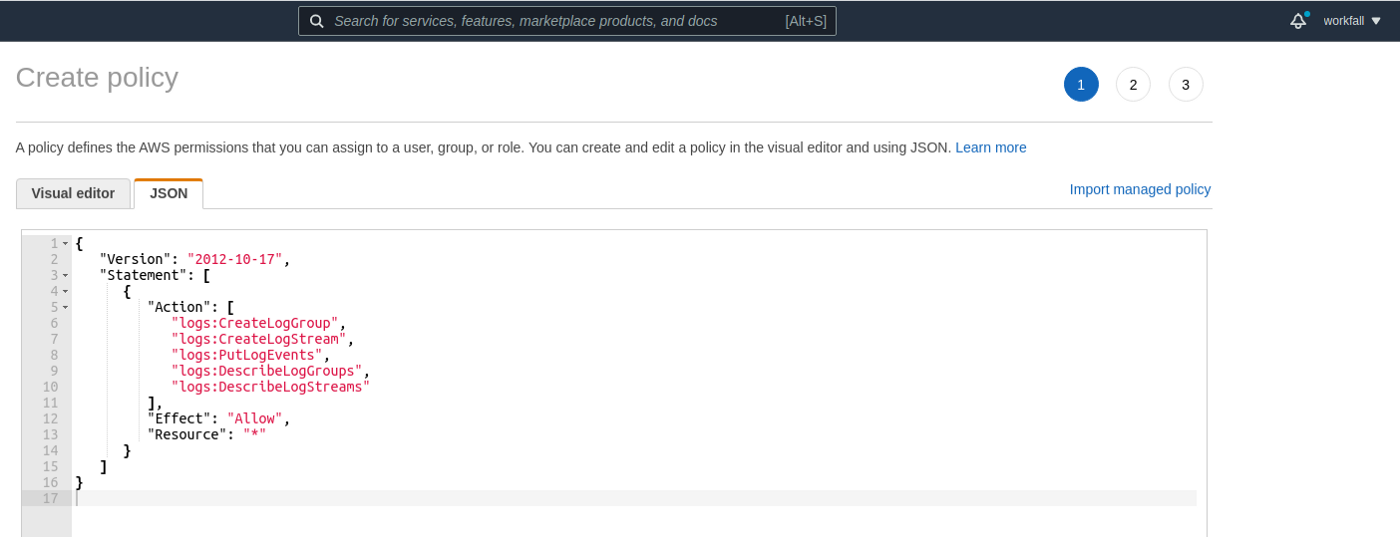
## **Configure Permissions**

*Before creating Flow Logs , we need to grant permission for the Flow Logs to publish logs to Cloudwatch Log group.*

* **Creating IAM Policy**

*First create an IAM Role for the Flow Logs to send data to Cloudwatch Log group.*

*The minimum permission required for the Flow Logs are CreateLogGroup , DescribeLogGroups , CreateLogStream , DescribeLogStreams , PutLogEvents.*

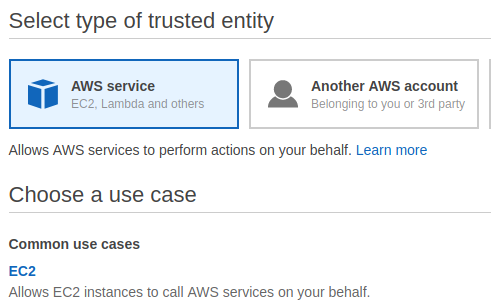
*Once the policy is created , We need to create an IAM role and attach the policy with it.*

*The role will be used later while creating Flow Logs.*

* **Creating IAM Role**

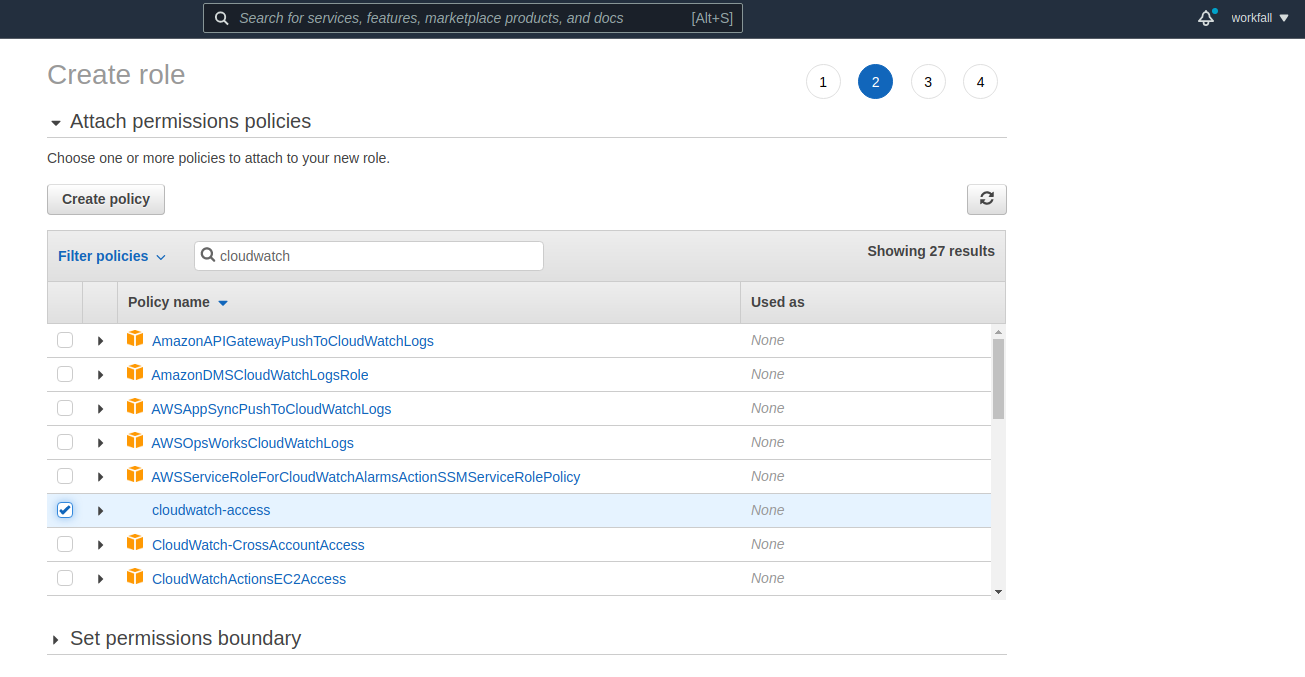
*To Create an IAM Role , Choose* ***Roles*** *and click* ***Create Role***

*Then Choose* ***EC2*** *as a Service to create a Role.*

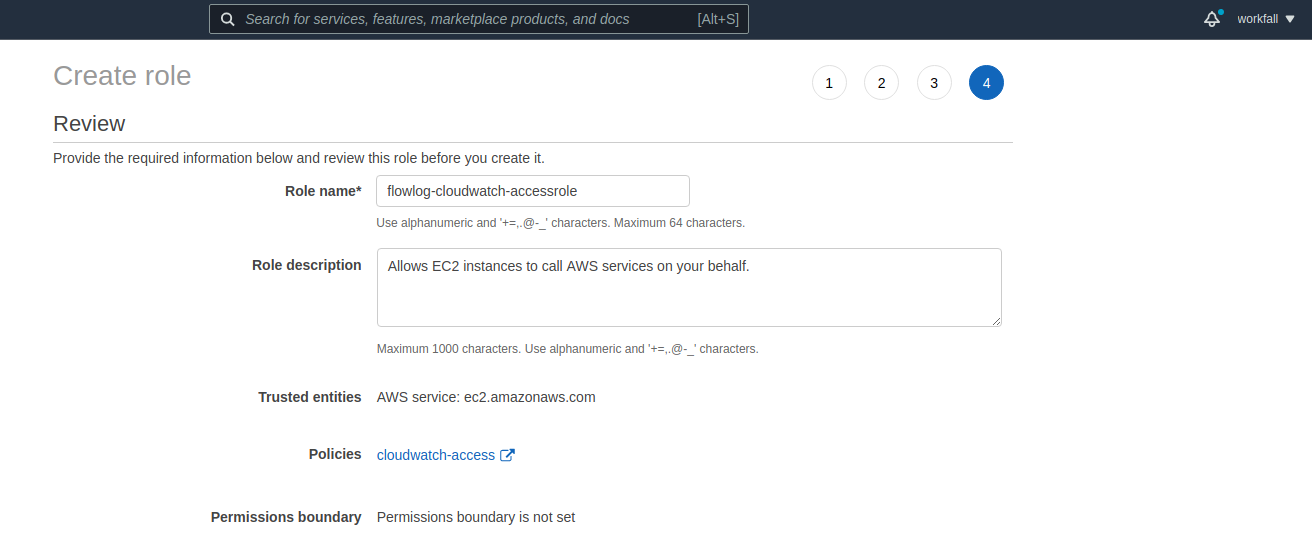


*and click* ***Next: Permissions***

*Search for the policy name which we have created.Select it.*



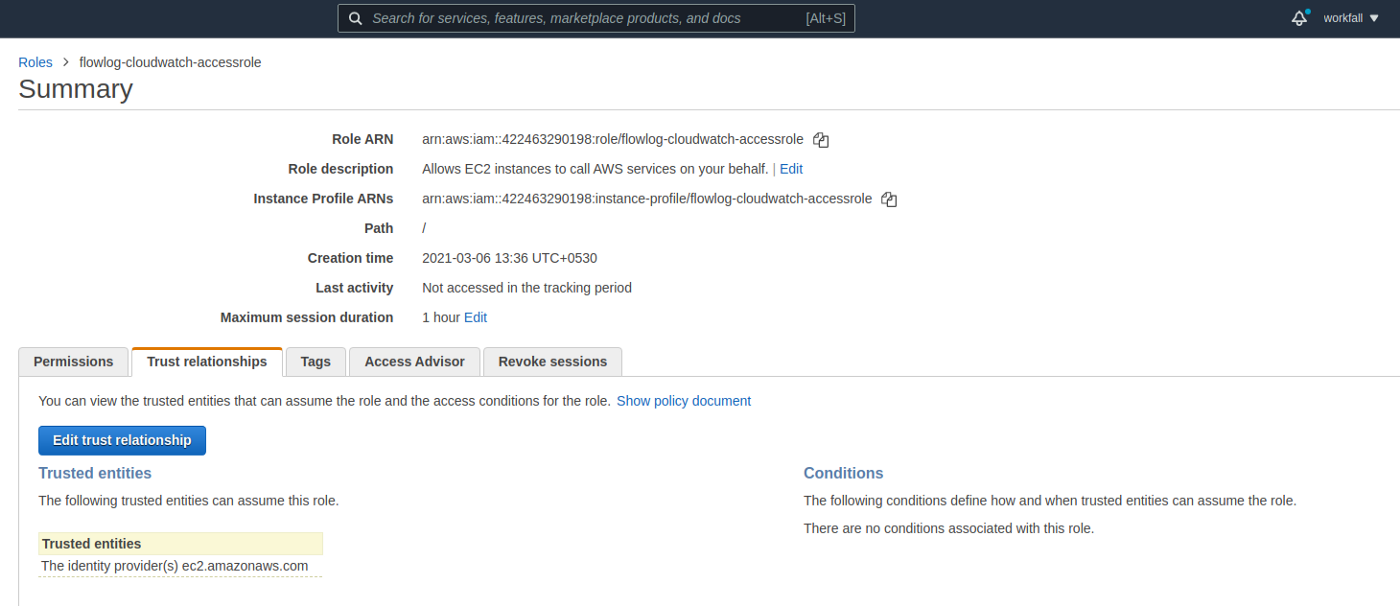
*And finally provide a name for the role and then click* ***Create Role****.*



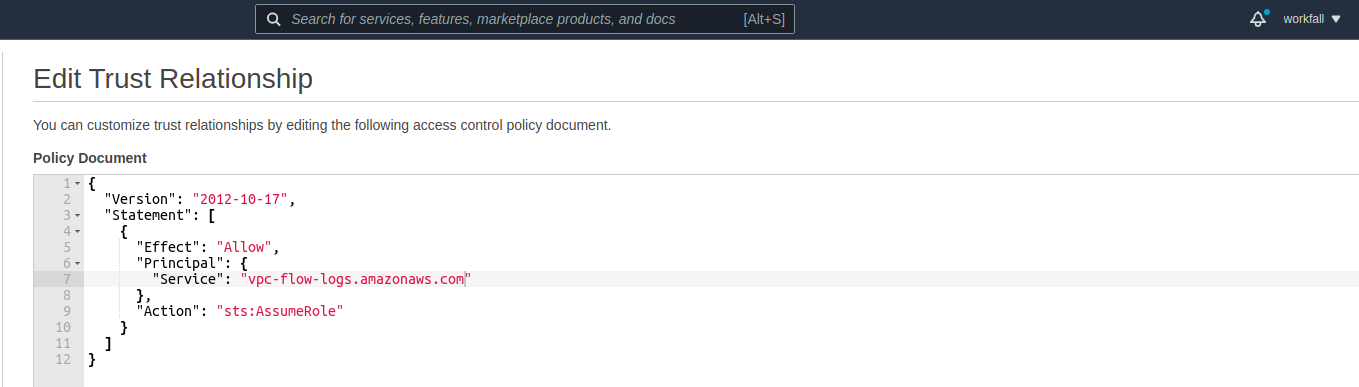
*Also we should make sure that the role has a trusted relationship that allows Flow Logs service to assume the role.*

*For that , Choose the Role that we have created , Select* ***Trust Relationships***

*and click* ***Edit trust relationship***



*In the place of* ***ec2.amazonaws.com*** *, Replace it with* ***vpc-flow-logs.amazonaws.com*** *and then click* ***Update trust policy***



*Now that we have successfully created the minimum permissions required for the Flow Logs service to publish Flow Logs data to Cloudwatch Log group.*

*Note the* ***ARN of the Role*** *(Role ARN) which will be used while creating Flow Logs.*

## **Create a Log Group in CloudWatch Logs**

*Create a log group directly in the CloudWatch console.*

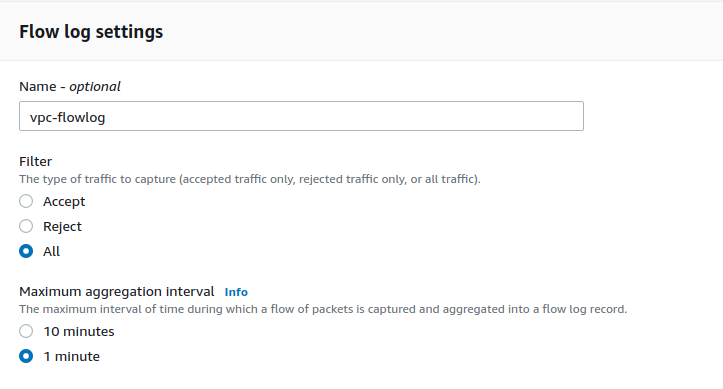
*To create a log group:*

* *Open the CloudWatch console at* [*https://console.aws.amazon.com/cloudwatch/*](https://console.aws.amazon.com/cloudwatch/)*.*
* *In the navigation pane, choose* ***Log groups****.*
* *Choose* ***Actions****, and then choose* ***Create log group****.*
* *Enter* ***vpc-flowlog*** *as a name for the log group, and then choose* ***Create log group****.*

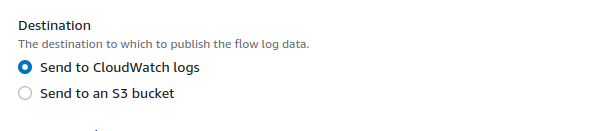
**Creating Flow Log for a VPC**

*To create Flow Log for a VPC , Login to VPC Console.*

* *In the navigation pane ,Choose* ***Your VPCs***
* *Select the VPC for which you want to create vpc Flow Log*
* *Under* ***Actions*** *, Click* ***Create Flow Log***
* *Under Flow Log setting , Provide a name for the Flow Log*
* *For* ***Filter*** *, It will ask for the type of traffic that needs to be recorded.*
* *Choose* ***All*** *to log rejected and accepted traffics.*
* *For* ***Maximum aggregation interval*** *, Choose the maximum period of time during which a Flow Log is captured and aggregated into one Flow Logs record.*



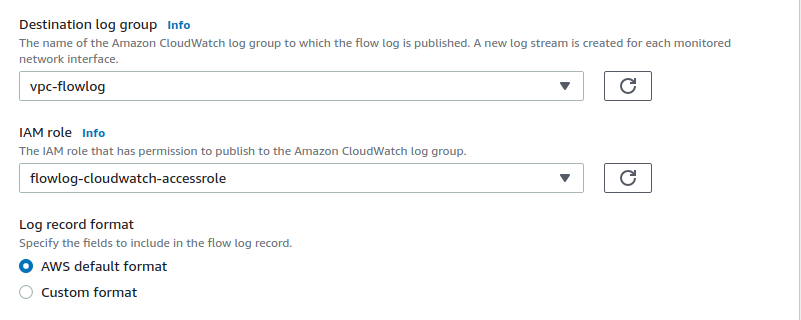
*For* ***Destination*** *, Choose* ***Send to Cloudwatch logs***



*For the* ***Destination log group*** *, Choose the cloudwatch log group which we have already created.*

*For the* ***IAM role*** *, Choose the role that was already created.*

*For the Log record format , We can choose either the default format or we can configure a custom format if required.*



*Add a tag for the Flow Log and click* ***Create Flow Log****.*

## **Launch EC2 Instance**

## *Launch an EC2 instance in one of the subnets which belong to VPC you have just enabled a VPC Flog Log for. Make sure to allow an SSH access to your instance.*

## *Once the instance is up and running connect to it via SSH.*

## **Viewing flow log records**

* *Open the CloudWatch console at* [*https://console.aws.amazon.com/cloudwatch/*](https://console.aws.amazon.com/cloudwatch/)*.*
* *In the navigation pane, choose* ***Logs****, and select the log group that contains your flow log. A list of log streams for each network interface is displayed.*
* *Select the log stream that contains the ID of the network interface for which to view the flow log records.*

## Benefits / Outcomes / Pros and Cons / Summary

*We have implemented Flow Logs for a VPC to analyze the traffic that are coming in and out of the AWS network.*

## Pricing

*Data ingestion and archival charges for vended logs apply when you publish flow logs to CloudWatch Logs or to Amazon S3. For more information and examples, see* [*Amazon CloudWatch Pricing*](https://aws.amazon.com/cloudwatch/pricing)*.*

## Tearing down

*Once you have finished you can destroy the environment:*

* *Destroy EC2 instance*
* *Disable VPC Flow Log for VPC*
* *Delete Cloudwatch Log Group*