

Chapter 5 : Cloudwatch (Send Application Logs To Cloudwatch)

=====

Amazon Web services has a centralized Log mangement systems known as Cloudwatch, Using which you can ship the server and application logs to cloudwatch and setup an alerting based on the error or log level.

This article guides you through the process of setting up **CLOUDWATCH AGENT** on the servers to collect and ship the logs to cloudwatch Log group.

Services Used:

EC2 INSTANCES : *Instance With The Server And Application Logs.*

IAM : *Required Permission For EC2 Instance To Ship Logs To Cloudwatch.*

Pre-Requisites:

- *An IAM role with cloudwatch access policy should be created and attached to the EC2 Instances.*

Configuring IAM Role:

Login to **IAM console**,

<https://console.aws.amazon.com/iam/home?region=ap-southeast-1#/home>

Before creating an IAM role , We should create a custom policy.

Choose **Policies** in the left pane , Click **Create policy**

You will see the following page , remove the existing code and add the below configuration.

Chapter 5 : Cloudwatch (Send Application Logs To Cloudwatch)

=====

Create policy

1

2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

[Import managed policy](#)

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": []  
4 }
```

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "logs:CreateLogGroup",  
        "logs:CreateLogStream",  
        "logs:PutLogEvents",  
        "logs:DescribeLogStreams"  
      ],  
      "Resource": [  
        "arn:aws:logs:*:*:*"  
      ]  
    }  
  ]  
}
```

Click **Review policy** , Give a unique name to the policy

And then click **Create policy**.





Now We have to create an IAM role with the custom policy we have created.

To create Role , Click **Roles** in the left pane of the IAM home page,

Chapter 5 : Cloudwatch (Send Application Logs To Cloudwatch)

Click **Create role**,

Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

Choose **EC2** and **Next: permissions**

Search for the policy name which you have created , Select it

Filter policies		Q cloudwatch	Showing 23 results
	Policy name	Used as	
<input type="checkbox"/>	AmazonDMSCloudWatchLogsRole	None	
<input type="checkbox"/>	AWSAppSyncPushToCloudWatchLogs	None	
<input type="checkbox"/>	AWSOpsWorksCloudWatchLogs	None	
<input checked="" type="checkbox"/>	cloudwatch	None	
<input type="checkbox"/>	CloudWatch-CrossAccountAccess	None	
<input type="checkbox"/>	CloudWatchActionsEC2Access	None	

Add a tag if required , Click **Review**

Give a name to the Role and Click **Create role**

Chapter 5 : Cloudwatch (Send Application Logs To Cloudwatch)

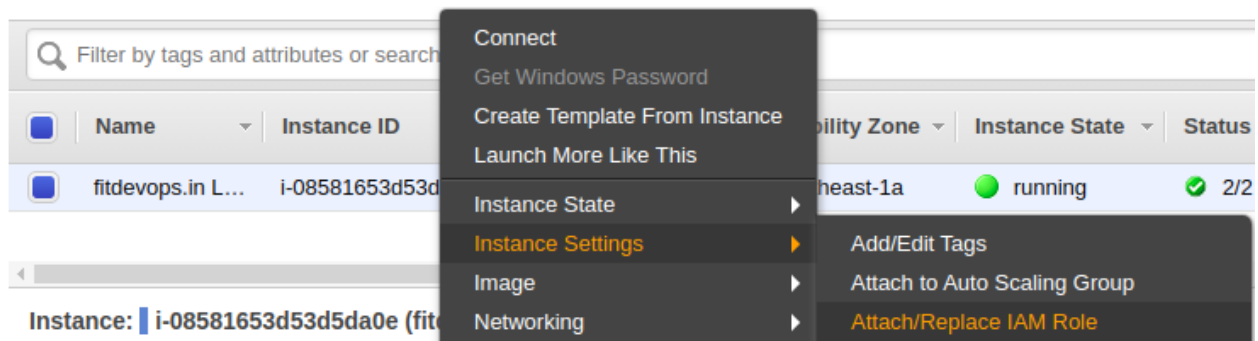
Adding IAM Role To EC2 Instance:

Now We have to attach the IAM role with the EC2 Instance so that EC2 instance will be able to communicate with the Cloudwatch services , Create Log groups and Log streams.

To attach the Role , Go to EC2 Console,

<https://ap-southeast-1.console.aws.amazon.com/ec2/v2/home>

Select the EC2 instance , Under **Actions** , Select **Instance Settings** , **Attach / Replace IAM Role**,



Attach/Replace IAM Role

Select an IAM role to attach to your instance. If you don't have any IAM roles, choose Create new IAM role to create a role in the IAM console. If an IAM role is already attached to your instance, the IAM role you choose will replace the existing role.

Instance ID i-08581653d53d5da0e (fitdevops.in Latest) ⓘ

IAM role* No Role ▼

🔄 Create new IAM role ⓘ

Under IAM Role , Select the Role you have created and click **Apply**.

In the Description of the instance , You should see the IAM Role attached.

Chapter 5 : Cloudwatch (Send Application Logs To Cloudwatch)

=====

```
Platform -
IAM role  EC2forSSM
```

Setup Cloudwatch Agent:

SSH into the EC2 Instance , Let's download the agent setup ,

```
curl https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/awslogs-agent-setup.py -O
```

When running the python file , You have to explicitly mention the region of your EC2 instances.

```
sudo python ./awslogs-agent-setup.py --region ap-southeast-1
```

In the next setup , It will ask you for Access Key Id and Secret Access key.
Provide them and make sure that the Keys have required permissions to perform this operation.

Provide the log file location and the **Log group** name ,

```
Step 4 of 5: Configuring the CloudWatch Logs Agent ...
Path of log file to upload [/var/log/syslog]: /var/log/nginx/access.log
Destination Log Group name [/var/log/nginx/access.log]: Nginx-logs
```

You should also provide a **Log stream** name ,

```
Choose Log Stream name:
 1. Use EC2 instance id.
 2. Use hostname.
 3. Custom.
Enter choice [1]: 2
```

And let the cloudwatch to store the logs in the following timestamps,

Chapter 5 : Cloudwatch (Send Application Logs To Cloudwatch)

```
Choose Log Event timestamp format:
 1. %b %d %H:%M:%S      (Dec 31 23:59:59)
 2. %d/%b/%Y:%H:%M:%S  (10/Oct/2000:13:55:36)
 3. %Y-%m-%d %H:%M:%S  (2008-09-08 11:52:54)
 4. Custom
Enter choice [1]: 3
```

And finally , let the cloudwatch agent to send all the logs in the log file, As we might be having some data already present in the log file.

```
Choose initial position of upload:
 1. From start of file.
 2. From end of file.
Enter choice [1]: 1
More log files to configure? [Y]: n

Step 5 of 5: Setting up agent as a daemon ...DONE
```

Now We have configured Cloudwatch agent successfully.

And you can manage the cloudwatch agent using the below commands,

```
service awslogs start
service awslogs status
```

```
root@ELK-UAT:~# service awslogs status
● awslogs.service - LSB: Daemon for AWSLogs agent.
   Loaded: loaded (/etc/init.d/awslogs; generated)
   Active: active (running) since Sat 2020-01-18 18:53:58 IST; 5min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 28693 ExecStart=/etc/init.d/awslogs start (code=exited, status=0/SUCCESS)
    Tasks: 6 (limit: 4915)
   CGroup: /system.slice/awslogs.service
           └─28719 /bin/sh /var/awslogs/bin/awslogs-agent-launcher.sh
           └─28721 /var/awslogs/bin/python /var/awslogs/bin/aws logs push --config-file /var/awslogs/etc/awslogs.conf --additional-configs-dir

Jan 18 18:53:57 ELK-UAT systemd[1]: Starting LSB: Daemon for AWSLogs agent....
Jan 18 18:53:58 ELK-UAT awslogs[28693]: Starting system awslogs daemon
Jan 18 18:53:58 ELK-UAT awslogs[28693]: * /var/awslogs/bin/awslogs-agent-launcher.sh is running
Jan 18 18:53:58 ELK-UAT systemd[1]: Started LSB: Daemon for AWSLogs agent..
```

Now the service is UP and running and You will find the cloudwatch agent file locations.

Chapter 5 : Cloudwatch (Send Application Logs To Cloudwatch)

=====

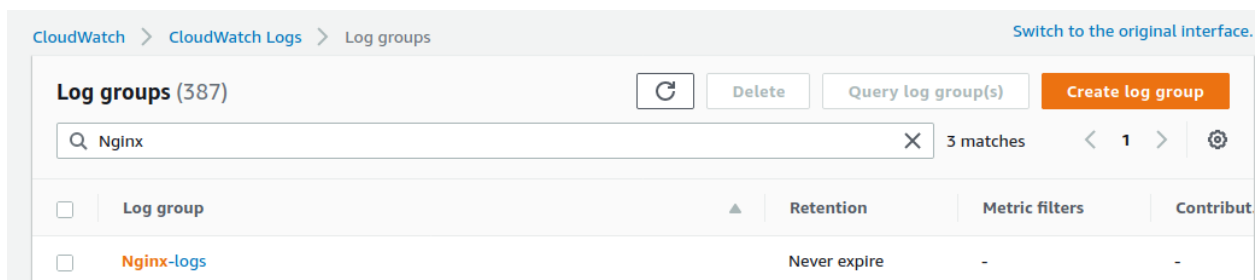
All the configuration files and start up scripts are stored under **/var/awslogs/** folder.

You can edit the logs configuration in **/var/awslogs/etc/awslogs.conf**

```
[/var/log/nginx/access.log]
datetime_format = %Y-%m-%d %H:%M:%S
file = /var/log/nginx/access.log
buffer_duration = 5000
log_stream_name = {hostname}
initial_position = start_of_file
log_group_name = Nginx-logs
```

Once the setup is configured properly , You should be able to see the logs in **Cloudwatch Management Console**.

Under Logs , Select Log groups , search for the log group name you have provided while configuring cloudwatch agent.



Click the Log group and You should be able to see the log streams which holds all the logs of the server and the applications , Based on your configuration.

Chapter 5 : Cloudwatch (Send Application Logs To Cloudwatch)

Log streams | Metric filters | Contributor Insights

Log streams (1)

Filter log streams

< 1 > ⚙

☐

Log stream

▼

Last event time

▼

☐

ELK-UAT

1/18/2020, 6:59:49 PM

You can find all the log events here,

Log events ☐ Format code

Export results ▼

Query log group

Filter events

30s 1m 30m 1h 12h custom ⚙

Timestamp	Message
🔍 2020-01-18T18:53:58.528+05:30	139.162.113.204 - - [18/Jan/2020:06:33:46 +0530] "GET / HTTP/1.1" 401 204 "-" "HTTP Banner Detection (..."
🔍 2020-01-18T18:53:58.528+05:30	44.224.22.196 - - [18/Jan/2020:06:41:46 +0530] "GET http://example.com/ HTTP/1.1" 400 280 "-" "AWS Se..."
🔍 2020-01-18T18:53:58.528+05:30	44.224.22.196 - - [18/Jan/2020:06:41:46 +0530] "GET http://169.254.169.254/ HTTP/1.1" 400 280 "-" "AW..."
🔍 2020-01-18T18:53:58.528+05:30	44.224.22.196 - - [18/Jan/2020:06:41:46 +0530] "GET http://[::ffff:a9fe:a9fe]/ HTTP/1.1" 400 280 "-" "AWS ..."
🔍 2020-01-18T18:53:58.528+05:30	44.224.22.196 - - [18/Jan/2020:06:41:47 +0530] "GET http://169.254.169.254/latest/dynamic/Instance-Id..."

Hope this article helped you to manage the logs in the Centralized Log management console.