Install and Configure the CloudWatch Logs Agent on a New EC2 Instance

You can use Amazon EC2 user data, a feature of Amazon EC2 that allows parametric information to be passed to the instance on launch, to install and configure the CloudWatch Logs agent on that instance. To pass the CloudWatch Logs agent installation and configuration information to Amazon EC2, you can provide the configuration file in a network location such as an Amazon S3 bucket. You can launch a new Amazon EC2 instance and enable logs by performing the following steps:

To launch a new instance and enable CloudWatch Logs

1. Create an agent configuration file that describes all your log groups and log streams:

   Sample agent configuration file for Amazon Linux

   ```
   [general]
   state_file = /var/awslogs/state/agent-state

   [/var/log/messages]
   file = /var/log/messages
   log_group_name = /var/log/messages
   log_stream_name = {instance_id}
   datetime_format = %b %d %H:%M:%S
   ```

   Sample agent configuration file for Ubuntu

   ```
   [general]
   state_file = /var/awslogs/state/agent-state

   [/var/log/syslog]
   file = /var/log/syslog
   log_group_name = /var/log/syslog
   log_stream_name = {instance_id}
   datetime_format = %b %d %H:%M:%S
   ```

   The agent configuration file describes the log files to monitor and the target log groups and log streams to upload it to. The agent consumes this configuration file and starts monitoring/uploading all the log files described in it..

Save it as a text file (for example, awslogs.cfg) either on the AMI's filesystem, in a publicly accessible http/https location, or an Amazon S3 location (for example, s3://myawsbucket/my-config-file).

2. Open the IAM console at https://console.aws.amazon.com/iam/.
3. In the navigation pane, click **Policies**, and then in the contents pane, click **Create Policy**.
4. On the **Create Policy** page, under **Create Your Own Policy**, click **Select**. For more information about creating custom policies, see IAM Policies for Amazon EC2 in the *Amazon EC2 User Guide for Linux Instances*.
5. On the **Review Policy** page, in the **Policy Name** field, type a name for the policy.
6. In the **Policy Document** field, paste in the following policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": [
                "arn:aws:logs:*:*:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::myawsbucket/*"
            ]
        }
    ]
```

    - }

7. Click **Create Policy**.

8. In the navigation pane, click **Roles**, and then in the contents pane, click **Create New Role**.
9. On the **Set Role Name** page, enter a name for the role and click **Next Step**.
10. On the **Select Role Type** page, click **Select** next to **Amazon EC2**.
11. On the **Attach Policy** page, in the table header (next to **Filter** and the **Search** box), click the **Policy Type**drop-down list, and select **Customer Managed Policies**.
12. In the list of **Customer Managed Policies**, select the IAM policy that you created above, and then click **Next Step**.
13. If you're satisfied with the role, click **Create Role**.
14. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
15. If necessary, change the region. From the navigation bar, select the region that meets your needs. For more information, see Regions and Endpoints in the *Amazon Web Services General Reference*.
16. On the Amazon EC2 console dashboard, click **Launch Instance**.

    For more information about how to launch an instance, see Launching an Instance in *Amazon EC2 User Guide for Linux Instances*.

17. On the **Step 1: Choose an Amazon Machine Image (AMI)** page, select the Linux instance type you want to launch, and then on the **Step 2: Choose an Instance Type** page, click **Next: Configure Instance Details**.
18. On the **Step 3: Configure Instance Details** page, In the **IAM role** field, select the IAM role that you created above.
19. Under **Advanced Details**, in the **User data** field, paste in the script and update the **-c** option with the location of the configuration file:

```
#!/bin/bash
curl https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/awslogs-agent-setup.py -O
chmod +x ./awslogs-agent-setup.py
```

```
./awslogs-agent-setup.py -n -r us-east-1 -c s3://myawsbucket/my-config-file
```

23. Make any other changes to the instance that you want, review your launch settings, and then click **Launch**.
24. You should see the newly created log group and log stream in the CloudWatch console after the agent has been running for a few moments.