# Configuring logs for Running EC2 Instances Step 1: Configure your IAM role or user for CloudWatch Logs

The CloudWatch Logs agent supports IAM roles and users. If your instance already has an IAM role associated with it, make sure that you include the IAM policy below. If you don't already have an IAM role assigned to your instance, you'll need to use your IAM credentials for the next steps because you cannot assign an IAM role to an existing instance; you can only specify a role when you launch a new instance..

**To configure your IAM role or user for CloudWatch Logs**

1. Open the IAM console at [https://console.aws.amazon.com/iam/.](https://console.aws.amazon.com/iam/)
2. In the navigation pane, click **Roles**, and then in the **Role Name** column, click an IAM role.
3. On the **Permissions** tab, under **Inline Policies**, click **Create Role Policy**.
4. On the **Set Permissions** page, click **Custom Policy**, and then click **Select**.
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:

|  |  |
| --- | --- |
| 1. { 2. "Version": "2012-10-17", 3. "Statement": [ 4. { 5. "Effect": "Allow", 6. "Action": [ 7. "logs:CreateLogGroup", 8. "logs:CreateLogStream", 9. "logs:PutLogEvents", 10. "logs:DescribeLogStreams" 11. ], 12. "Resource": [ 13. "arn:aws:logs:\*:\*:\*" 14. ] 15. } 16. ] | |
|  | } |

23. Click **Apply Policy**.

# Step 2: Install and configure CloudWatch Logs on an existing Amazon EC2 instance

The process for installing the CloudWatch Logs agent differs depending on whether your Amazon EC2 instance is running Amazon Linux, Ubuntu, CentOS, or Red Hat. Use the steps appropriate for the version of Linux on your instance.

**To install and configure CloudWatch Logs on an existing Amazon Linux instance**

Starting with Amazon Linux AMI 2014.09, the CloudWatch Logs agent is available as an RPM installation with the awslogs package. Earlier versions of Amazon Linux can access the awslogs package by updating their instance with the sudo yum update y command. By installing the awslogs package as an RPM instead of the using the CloudWatch Logs installer, your instance will receive regular package updates and patches from Amazon without having to manually reinstall the CloudWatch Logs agent.

1. Connect to your Amazon Linux instance. For more information, see [Connect to](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-connect-to-instance-linux.html)

[Your Instance](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-connect-to-instance-linux.html) in the *Amazon EC2 User Guide for Linux Instances*.

1. Update your Amazon Linux instance to pick up the latest changes in the package repositories.

[ec2-user ~]$ **sudo yum update -y**

1. Install the awslogs package.

[ec2-user ~]$ **sudo yum install -y awslogs**

1. Edit the /etc/awslogs/awscli.conf file and in the [default] section, specify the region where you want to view log data and add your credentials.

|  |  |
| --- | --- |
| 1. region = *<us-east-1, us-west-1, us-west-2, eu-west-1, eu-central-1, apsoutheast-1,* 2. *ap-southeast-2, or ap-northeast-1>* 3. aws\_access\_key\_id = *<YOUR ACCESS KEY>* | |
|  | aws\_secret\_access\_key = *<YOUR SECRET KEY>* |

1. Edit the /etc/awslogs/awslogs.conf file to configure the logs you would like to track.
2. Start the awslogs service.

|  |  |
| --- | --- |
| 10. [ec2-user ~]$ **sudo service awslogs start** | |
|  | Starting awslogs: [ OK ] |

1. (Optional) Check the /var/log/awslogs.log file for errors logged when starting the service.
2. (Optional) Run the following command to start the awslogs service at each system boot.

[ec2-user ~]$ **sudo chkconfig awslogs on**

1. 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.