**AWS CloudWatch EC2 Application monitoring using SSM, RUN command and Parameter Store.**

*AWS Systems Manager Agent (SSM Agent) is Amazon software that runs on EC2 instances, edge devices, and on-premises servers and virtual machines (VMs). SSM Agent makes it possible for Systems Manager to update, manage, and configure these resources.*

**Create an IAM role for SSM** to be able to install the CloudWatch agent with the help of SSM.

* SSMFullAccess

**Launch an EC2 instance and attach the created roles for SSM and the CloudWatch agent**. Configure the user-data to install, start, and setup the Apache web server.

#!/bin/bash

# Install Apache Web Server

yum install -y httpd

# Turn on Web Server

systemctl enable httpd.service

systemctl start httpd.service

# Setup Web Server

chmod 755 var/www/html

touch var/www/html/index.html

echo "Welcome to my Website :)" > /var/www/html/index.html

*Systems Manager Run Command enables you to manage the configuration of your instances. You specify a Systems Manager document, specify parameters, and execute the command on one or more instances.*

**Download the SSM agent using Run Command**

1. Open the Systems Manager console
2. In the navigation pane, choose **Run Command**.
3. In the **Command document** list, choose **AWS-ConfigureAWSPackage**.
4. In the **Action** list, choose **Install**.
5. In the **Name** box, enter *AmazonCloudWatchAgent*.
6. Keep **Version** set to **latest** to install the latest version of the agent.
7. In the **Targets** area, choose the instance on which to install the CloudWatch agent. If you do not see a specific instance, it might not be configured for Run Command.
8. Choose **Run**.

**In the *Parameter Store*, create a CloudWatch agent configuration file that specifies the metrics and logs that the agent will collect for the machine. (***This information will be sent to CloudWatch.****)***

Name: Monitor-Web-Server

Description: Collect web logs and monitor system metrics

Tier: Standard

Type: String

Data type: text

Value: (JSON document to install CloudWatch configuration)

{

    "logs": {

      "logs\_collected": {

        "files": {

          "collect\_list": [

            {

              "log\_group\_name": "HttpAccessLog",

              "file\_path": "/var/log/httpd/access\_log",

              "log\_stream\_name": "{instance\_id}",

              "timestamp\_format": "%b %d %H:%M:%S"

            },

            {

              "log\_group\_name": "HttpErrorLog",

              "file\_path": "/var/log/httpd/error\_log",

              "log\_stream\_name": "{instance\_id}",

              "timestamp\_format": "%b %d %H:%M:%S"

            }

          ]

        }

      }

    },

    "metrics": {

      "metrics\_collected": {

        "cpu": {

          "measurement": [

            "cpu\_usage\_idle",

            "cpu\_usage\_iowait",

            "cpu\_usage\_user",

            "cpu\_usage\_system"

          ],

          "metrics\_collection\_interval": 10,

          "totalcpu": false

        },

        "disk": {

          "measurement": [

            "used\_percent",

            "inodes\_free"

          ],

          "metrics\_collection\_interval": 10,

          "resources": [

            "\*"

          ]

        },

        "diskio": {

          "measurement": [

            "io\_time"

          ],

          "metrics\_collection\_interval": 10,

          "resources": [

            "\*"

          ]

        },

        "mem": {

          "measurement": [

            "mem\_used\_percent"

          ],

          "metrics\_collection\_interval": 10

        },

        "swap": {

          "measurement": [

            "swap\_used\_percent"

          ],

          "metrics\_collection\_interval": 10

        }

      }

    }

  }

Click on ***Create Parameter***

**Install the CloudWatch agent using Run Command**

1. Open the Systems Manager console
2. In the navigation pane, choose **Run Command**.
3. In the **Command document** list, choose **AmazonCloudWatch-ManageAgent**.
4. In the **Action** list, choose **Configure**.
5. In the **Mode** box, enter *ec2*.
6. In the **Optional Configuration Source** box,enter *ssm.*
7. Inthe **Optional Configuration Location:** Monitor-Web-Server
8. For **Optional Open Telemetry Source**,enter*ssm*
9. In the **Optional Restart** box, enter *yes*.
10. In the **Targets** area, choose the instance on which to install the CloudWatch agent. If you do not see a specific instance, it might not be configured for Run Command.
11. In the **Output options**, enable CloudWatch logs.
12. Choose **Run**.

**Create a CloudWatch alarm to be notified for whenever a request receives a 404 error.**

Open the CloudWatch console and navigate to log groups.

Select HttpAccessLog

Click on the Actions drop down, and select **Create Metric Filter**

**Filter pattern**: [ip, id, user, timestamp, request, status\_code=404, size]

Select the instance of your choice in the **Test pattern box**, then click **Next**.

**Filter Name**: 404Errors

**Metric namespace**: LogMetrics

**Metric name**: 404Errors

**Metric value**: 1

Click ***Next*** >>> ***Create Metric Filter***

Select the created Metric Filter, then click **Create Alarm**

Graphical user interface, application

Description automatically generated

\*\*If you get five 404 errors within 1 minute you’ll receive an alarm\*\*

**Alarm name**: 404 Errors

**Alarm description**: Alert when too many 404s detected on an instance.

Review and ***Create Alarm***