SOE - Availability Monitoring

Operational Playbook

Table of Contents

1. SOE Availability Monitoring Overview

The SOE monitoring solution will provide an automated process to create Real-time monitoring of critical metrics & KPIs via elegant CloudWatch dashboard and associated alarms to capture the metrics for AWS resources as outlined in the requirements in section “4. Monitoring Requirements” below. The monitoring solution will log metrics for EC2, ELB and RDS resources and create a dashboard and alarms per application. It can be implemented in any AWS accounts and environments and its functionality is implemented through a set of CloudFormation (Infrastructure as Code) Templates and Lambda serverless functions.

A. Features

- Define critical and warning thresholds for alarms for EC2, ELB and RDS
- Alerts send alarms to SNS topics which can be subscribed to using the email addresses
- Automatically creates dashboards with widgets and thresholds
- Creates metrics using CloudWatch agent for both Windows and Linux EC2 instances
- Validation of user input of thresholds using regular expressions
- Validation of resources input given in lambda logs
- Alerts given for both ALARM and OK state
- Includes utility function to manually delete alarms

B. Pre-Requisites

- Amazon CloudWatch agent installed on EC2 and Linux instances
- AWS CloudTrail on all accounts
- Application owners have the inventory of EC2, ELB and RDS inventory for the application

C. Down Stream Dependents

- Notification stakeholders identified
- Any changes to the Dashboard and Alarms to be made only by running the scripts as below. No manual changes done to the dashboard

2. Monitoring Requirements

Monitoring Category	Metric	Monitor/Alert	Warning Threshold	Critical Threshold
System	System status check	Alert		Passed/Failed
	Instance status check	Alert		Passed/Failed
CPU	CPU Utilization	Alert	70%, 5 min	90%, 5 min
Memory (Lin)	Memory Utilization	Alert	70%, 5 min	80%, 5 min
Memory (Win)	Memory Utilization	Alert	Custom	Custom
Disk	Disk Utilization	Alert	70%	90%
Network	Network In/ Out	Monitor		
Direct Connect	Connection State	Alert		Up/Down
	Utilization	Alert	50%	75%
S3	Public vs. Private	Alert		Public/Private
ELB	Unhealthy host account	Alert	>=1	
	Healthy host account	Monitor		
	Request Count	Monitor		
	New Connection Count	Monitor		
	Backend connections	Alert	>=1	
	Latency	Alert	>50 ms	
	Tatget 4xx, 5xx error count	Alert	>=1	
	ELB 3xx,4xx,5xx error count	Monitor		
RDS	CPU Utilization	Alert	70%, 5 min	90%, 5 min
	Free Storage	Alert	Custom	Custom
	Freeable memory	Alert	Custom	Custom
	ReadThroughput	Monitor		
	WriteThroughput	Monitor		
	ReadIOPS	Monitor		
	WriteIOPS	Monitor		

3. Solution Deployment

The section includes the detailed steps to deploy the solution **for each application**.

Note about CloudWatch agent:

- The installation of Cloudwatch agent is a prerequisite for those instances for which disk and memory metrics needs to be monitored. Usually, the new AMI's must come with the agent preconfigured. If the agent is not installed, the corresponding metrics on the dashboard will show as empty for these instances. However, the remaining metrics will function as expected. The installation instructions will be present in the CodeCommit repository (It's not part of SOE Availability Monitoring)

Note about SSM agent:
EC2 instances must be setup per the playbook to be available in System Manager – Inventory.

Note about Thresholds:

- If the application does not have a particular resource (ec2,elb and/or rds) and you are required to fill the threshold which is empty (Windows CPU utilization and RDS metric for storage and memory), please input 0 for those thresholds.
- The thresholds in GB values can be decimal integers
- All other thresholds including percentages must be Whole number

1. Follow the instructions provided in the file *Installation_Instructions_CWAgent_V01.pdf*

a. This installs CW Agent which allows Disk and Memory Utilization metrics to be monitored on the applicable EC2 instances

2. Go to CloudFormation and create Stack (first stack)
    a. Under the Choose a template section select “Upload to S3” and upload the file “1_coma_CreateBucket.json” where prompted
    b. Provide stack name of choosing (recommended to name after the parameter in the following section following convention <*applicationname*>*-codebucket*)
    c. Take note of the bucket name
    d. Under the Parameters section
        i. Bucket name
            1. Enter the name of the S3 bucket created by the stack
            2. Click next
    e. Go to the Advanced drop down section and set the Timeout to 5 minutes (LEAVE ALL OTHER SECTIONS AS DEFAULT) and click next
    f. Review the detail section to confirm the parameters
    g. Under the Capabilities section check the box for “I acknowledge that AWS CloudFormation might create IAM resources with custom names.” and click create
    h. Wait for stack status to display “Create_Complete”
3. Go to AWS Console and select S3
    a. In the “Search for buckets” search bar type the name of the bucket created in the previous section
    b. Select the bucket
    c. Upload all provided files in the SOEGuardDutyMacie” folder (13 files to be uploaded in total) to S3 by clicking the “Upload” button
        i. *1_coma_CreateBucket.json*
        ii. *2_coma_CrateIAMRole.json*
        iii. *3_coma_Monitoring_v1.json*
        iv. *Installing_Instructions_CWAgent_V01.zip*
        v. *SOE – Monitoring Playbook 1.4.pdf*
        vi. *coma_Monitoring_lambda_v1.zip*
        vii. *coma_applicationelb_alarm_lambda.zip*
        viii. *coma_create_sns_topic_lambda.zip*
        ix. *coma_ec2_alarm_lambda.zip*
        x. *coma_ec2_cloudwatchagent_alarm_lambda.zip*
        xi. *coma_rds_alarma_lambda.zip*
        xii. *coma_utility_deleteAlarm.py*
        xiii. *input.csv*
            1. Before uploading this particular file – make sure to update the contents to reflect the resources (such as the private EC2 DNS, ELB DNS name, and RDS Endpoint) in the application – refer to the next section “B. Input file “input.csv” format” for formatting instructions
    d. Once the upload is complete take note of the object URLs below:
        i. *2_coma_CrateIAMRole.json*
        ii. *3_coma_Monitoring_v1.json*

4. If the IAM role “soe-monitoring-role” is NOT present in the account (navigate to IAM in the AWS Console to check) go to CloudFormation and create Stack (second stack)
    a. Under the Choose a template section select “Specify an Amazon S3 template URL” and input the S3 URL of the CloudFormation stack file uploaded in the previous step and click next (*2_coma_CrateIAMRole.json*)
    b. Provide stack name of choosing (recommended to name following convention <secretariat>-create-IAM-lambda-alarm)
    c. Click next
    d. Go to the Advanced drop down section and set the Timeout to 5 minutes (LEAVE ALL OTHER SECTIONS AS DEFAULT) and click next
    e. Review the detail section to confirm the parameters
    f. Under the Capabilities section check the box for “I acknowledge that AWS CloudFormation might create IAM resources with custom names.” and click create
    g. Wait for stack status to display “Create_Complete”
5. Go to CloudFormation and create Stack (third stack)
    a. Under the Choose a template section select “Specify an Amazon S3 template URL” and input the S3 URL of the CloudFormation stack file uploaded in the previous step and click next (*3_coma_Monitoring_v1.json*)
    b. Provide stack name of choosing (recommended to name following convention <secretariat>-create-dashboard-alarm-<dashboardName>)
    c. Under the Parameters section:
        i. Dashboard Details
            1. Enter name of the S3 bucket created in the first stack
            2. Enter name of the dashboard (recommended to use application name as the dashboard name)
            3. Enter a comma separate list of email addresses to send alarm notifications to
                a. Select drop down for create alarm and set to “YES”
        ii. EC2 thresholds
            1. Enter the desired metric threshold (read the descriptions to the right of the input box for more details)
        iii. ELB thresholds
            1. Enter the desired metric threshold (read the descriptions to the right of the input box for more details)
        iv. RDS thresholds
            1. Enter the desired metric threshold (read the descriptions to the right of the input box for more details)
    d. Click next
    e. Go to the Advanced drop down section and set the Timeout to 20 minutes (LEAVE ALL OTHER SECTIONS AS DEFAULT) and click next
    f. Review the detail section to confirm the parameters
    g. Under the Capabilities section check the box for “I acknowledge that AWS CloudFormation might create IAM resources with custom names.” and click create

h. Wait for stack status to display “Create_Complete”

CloudFormation Stack Created Resources in AWS Environment

Resource Type	Resource Name
CloudWatch Dashboard	[user determined]
CloudWacth Alarm	CPU_UTILIZATION_CRITICAL
CloudWacth Alarm	CPU_UTILIZATION_WARNING
CloudWacth Alarm	STATUS_CHECK
CloudWacth Alarm	MEMORY_UTILIZATION_CRITCAL(LIN)
CloudWacth Alarm	MEMORY_UTILIZATION_WARNING(LIN)
CloudWacth Alarm	MEMORY_UTILIZATION_CRITCAL(WIN)
CloudWacth Alarm	MEMORY_UTILIZATION_WARNINGL(WIN)
CloudWacth Alarm	DISK_UTILIZATION_CRITCAL
CloudWacth Alarm	DISK_UTILIZATION_WARNING
CloudWacth Alarm	UNHEALTHY_HOST_WARNING
CloudWacth Alarm	TARGET_CONNECTION_ERROR
CloudWacth Alarm	TARGET_RESPONSE_TIME
CloudWacth Alarm	HTTP_TARGET_4XX_RESPONSE
CloudWacth Alarm	HTTP_TARGET_5XX_RESPONSE
CloudWacth Alarm	RDS_CPU_UTILIZATION_CRITICAL
CloudWacth Alarm	RDS_CPU_UTILIZATION_WARNING
CloudWacth Alarm	RDS_FREEABLEMEM_CRITICAL
CloudWacth Alarm	RDS_FREESTORAGESPACE_CRITICAL
CloudWacth Alarm	RDS_FREESTORAGESPACE_WARNING

B. Input file “input.csv” format

The input file must be in the following format exactly. A sample is provided in the code ZIP file.

	A	B	C
1	Hostname	Type	
2	<Ec2 private DNS >	Ec2	
3	<Application ELB DNS name >	Elb	
4	<RDS endpoint>	Rds	
5			
6			
7			

4. Post Deployment Process

- Bucket created per application must preferably not be deleted. This minimizes the efforts in inventorying the application in the event that the dashboard needs to be created again (to add new resources for example)
- Adding new resources in Application:
    a. Any new resources added to the application inventory must be added along with the existing resources to the input.csv and the Solution Deployment step #6 needs to be re-run
- Adding new users for notification:
    a. Any new users can be added by adding to the subscribers of the topic. Please make sure that these new users are carried forward in the event the dashboard is recreated (i.e. when step 6 is re-run)