**Task 1. CPU Utilization**

CloudWatch monitors the AWS instance for CPU utilization. If the utilization exceeds the set threshold value for some period, then a cloud watch alarm is triggered. The alarm triggers a lambda function which creates a service now incident.

**Alarm Name: Linux\_**[**CPU\_Utilization\_Alert**](https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:alarm/CPU_Utilization_Alert)

**Lambda Function:** [**vigil\_cpu\_utilization**](https://us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/vigil_cpu_utilization)

**Threshold value: 70**

**Short Description: CloudWatch Alarm - CPU Utilization {currentValue} exceeded the threshold value {threshold} for instance {instanceId} in region {region}"**

**Instance Name: vigil-linux-01**

**Task 2. Memory Utilization**

CloudWatch monitors the AWS instance for memory utilization. If the memory exceeds the set threshold value for some period, then a cloud watch alarm is triggered. The alarm triggers a lambda function which creates a service now incident.

**Alarm Name: Linux\_Memory\_Utilization**

**Lambda Function: linux\_memory\_utilization**

**Threshold value: 70**

**Short Description: CloudWatch Alarm - Memory Utilization {currentValue} exceeded the threshold value {threshold} for instance {instanceId} in region {region}"**

**Instance Name: vigil-linux-03**

**Instance ID: i-06ed437a4b8df4885**

**Task 3. EC2 Instance Network Failure / AWS EC2 Security Group Update**

CloudWatch monitors the AWS instance to monitor the inbound rules defined in the security group. If inbound rules are not listed there and user is unable to take RDP session, and a cloud watch alarm is triggered. The alarm triggers a lambda function which creates a service now incident.

**Alarm Name:** [**Inbound\_Network\_Alert**](https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:alarm/Inbound_Network_Alert)

**Lambda Function:** [**Inbound\_Network\_Alert**](https://us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Inbound_Network_Alert)

**Threshold value: 0.99**

**Short Description: CloudWatch Alarm - Inbound traffic from CIDR 10.0.0.0/16 blocked by EC2 security group for instance {instanceId} in region {region}."**

**Instance Name: vigil-win-04**

**Task 4. AWS EC2 Route Table Disruption**

CloudWatch monitors if the internet gateway entry is present in the route table. If the entry is absent/deleted, it triggers an alarm which in turn triggers the lambda function which creates a service now incident.

**Alarm Name: Internet-Gateway-Error**

**Lambda Function:** [**Internet-Gateway-Error**](https://us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/Internet-Gateway-Error)

**Threshold value: 1**

**Short Description: Cloud Alert: Internet Gateway missing for EC2 instance associated with route table {internetGatewayId} in {region}.**

**Route Table Name: agentic-public-rt**

**Route Table ID: rtb-0e6f92c88351a14fe**

**Task 5.** **AWS Network ACL(NACL) Inbound Rule Update**

CloudWatch monitors if the inbound rule number 100 entry in network ACL is absent/deleted, it triggers an alarm which in turn triggers the lambda function which creates a service now incident.

**Alarm Name:** [**NetworkACL\_Alert**](https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:alarm/NetworkACL_Alert)

**Lambda Function:** [**NetworkACL\_Alert**](https://us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/NetworkACL_Alert)

**Threshold value: 1**

**Short Description: CloudWatch Alarm - Inbound rule number 100 is missing from the Network ACL {naclId} in region {region}.**

**Network ACL ID: acl-04693d8452e77de5a**