

Use Cases

Our rules focuses on providing the desired visibility within the Amazon Web Services platform.

The following describes some use cases for IAM, EC2 and VPC services. The structure followed is always the same. You will see the definition of the rule that matches with the log message generated by the AWS event. You can check how this log message flows in the diagram at the beginning of this section. Also, on each of the examples, you will see a screenshot of how Kibana shows the corresponding alert. Remember that an alert is triggered when the log message matches a specific rule if its level is high enough.

Contents

- [IAM use cases](#)
 - [Create user account](#)
 - [Create user account without permissions](#)
 - [User login failed](#)
 - [Possible break-in attempt](#)
 - [Login success](#)
- [EC2 use cases](#)
 - [Run a new instance in EC2](#)
 - [Start instances in EC2](#)
 - [Stop instances in EC2](#)
 - [Create Security Groups in EC2](#)
 - [Allocate a new Elastic IP address](#)
 - [Associate a new Elastic IP address](#)
- [VPC Use cases](#)
 - [Create VPC](#)

