EC2 use cases

Amazon EC2 (Elastic Compute Cloud) provides scalable computing capacity in the cloud. When using a service like this, it is highly desirable to monitor for attacks or other unauthorized actions being performed against your cloud assets. With CloudTrail and Wazuh's EC2 event analysis capabilities, this is very possible.

Following are some use cases for Wazuh rules built in for EC2.

Run a new instance in EC2

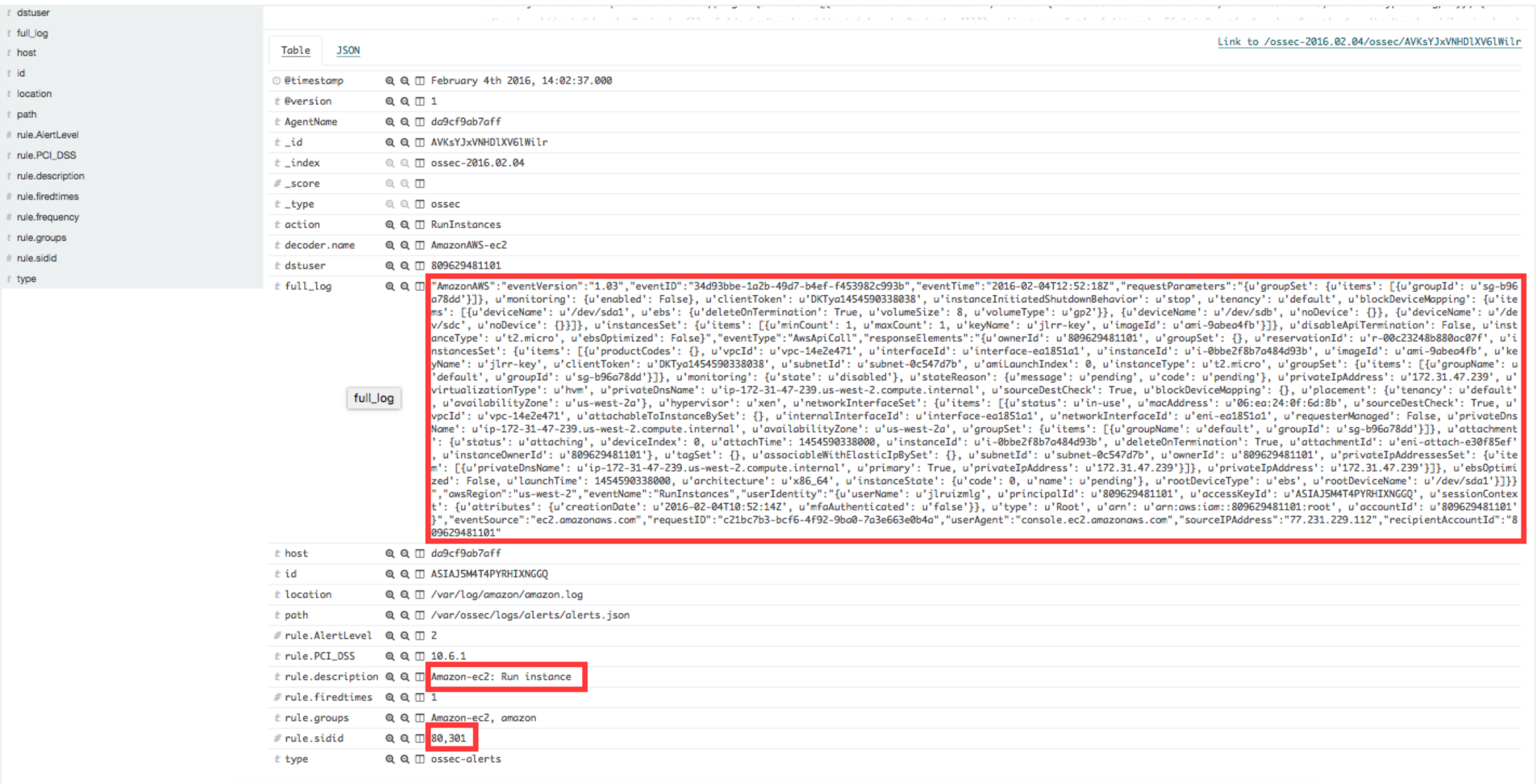
When a user runs a new instance in EC2, an AWS event is generated. As previously illustrated, the log message flows to the Wazuh agent which passes it on to Wazuh manager. The latter analyzes the log event and finds that it matches rule `80301`, which results in an alert being generated, as can be seen in Kibana.

Definition of rule 80301

Copied to clipboard

```
<rule id="80301" level="2">
    <if_sid>80300</if_sid>
    <action>RunInstances</action>
    <description>Amazon-ec2: Run instance</description>
    <group>amazon,pci_dss_10.6.1,</group>
</rule>
```

Kibana will show this alert



Link to /ossec-2016.02.04/ossec/AVKsYJxVNHDlXV6lWilr

```
@timestamp        February 4th 2016, 14:02:37.000
@version          1
AgentName         da9cf9ab7aff
_id               AVKsYJxVNHDlXV6lWilr
_index            ossec-2016.02.04
_score
_type             ossec
action            RunInstances
decoder.name      AmazonAWS-ec2
dstuser           809629481101
full_log          "AmazonAWS":"eventVersion":"1.03","eventID":"34d93bbe-1a2b-49d7-b4ef-f453982c993b","eventTime":"2016-02-04T12:52:18Z","requestParameters":"{u'groupSet': {u'items': [{u'groupId': u'sg-b96
                  a78dd'}]}, u'monitoring': {u'enabled': False}, u'clientToken': u'DKTya1454590338038', u'instanceInitiatedShutdownBehavior': u'stop', u'tenancy': u'default', u'blockDeviceMapping': {u'ite
                  ms': [{u'deviceName': u'/dev/sda1', u'ebs': {u'deleteOnTermination': True, u'volumeSize': 8, u'volumeType': u'gp2'}}, {u'deviceName': u'/dev/sdb', u'noDevice': {}}, {u'deviceName': u'/de
                  v/sdc', u'noDevice': {}}]}, u'instancesSet': {u'items': [{u'minCount': 1, u'maxCount': 1, u'keyName': u'jlrr-key', u'imageId': u'ami-9abea4fb'}]}, u'disableApiTermination': False, u'inst
                  anceType': u't2.micro', u'ebsOptimized': False}","eventType":"AwsApiCall","responseElements":"{u'ownerId': u'809629481101', u'groupSet': {}, u'reservationId': u'r-00c23248b880ac07f', u'i
                  nstancesSet': {u'items': [{u'productCodes': {}, u'vpcId': u'vpc-14e2e471', u'interfaceId': u'interface-ea1851a1', u'instanceId': u'i-0bbe2f8b7a484d93b', u'imageId': u'ami-9abea4fb', u'ke
                  yName': u'jlrr-key', u'clientToken': u'DKTya1454590338038', u'subnetId': u'subnet-0c547d7b', u'amiLaunchIndex': 0, u'instanceType': u't2.micro', u'groupSet': {u'items': [{u'groupName': u
                  'default', u'groupId': u'sg-b96a78dd'}]}, u'monitoring': {u'state': u'disabled'}, u'stateReason': {u'message': u'pending', u'code': u'pending'}, u'privateIpAddress': u'172.31.47.239', u'
                  virtualizationType': u'hvm', u'privateDnsName': u'ip-172-31-47-239.us-west-2.compute.internal', u'sourceDestCheck': True, u'blockDeviceMapping': {}, u'placement': {u'tenancy': u'default'
                  , u'availabilityZone': u'us-west-2a'}, u'hypervisor': u'xen', u'networkInterfaceSet': {u'items': [{u'status': u'in-use', u'macAddress': u'06:ea:24:0f:6d:8b', u'sourceDestCheck': True, u'
                  vpcId': u'vpc-14e2e471', u'attachableToInstanceBySet': {}, u'internalInterfaceId': u'interface-ea1851a1', u'networkInterfaceId': u'eni-ea1851a1', u'requesterManaged': False, u'privateDns
                  Name': u'ip-172-31-47-239.us-west-2.compute.internal', u'availabilityZone': u'us-west-2a', u'groupSet': {u'items': [{u'groupName': u'default', u'groupId': u'sg-b96a78dd'}]}, u'attachment
                  ': {u'status': u'attaching', u'deviceIndex': 0, u'attachTime': 1454590338000, u'instanceId': u'i-0bbe2f8b7a484d93b', u'deleteOnTermination': True, u'attachmentId': u'eni-attach-e30f85ef'
                  , u'instanceOwnerId': u'809629481101'}, u'tagSet': {}, u'associableWithElasticIpBySet': {}, u'subnetId': u'subnet-0c547d7b', u'ownerId': u'809629481101', u'privateIpAddressesSet': {u'ite
                  m': [{u'privateDnsName': u'ip-172-31-47-239.us-west-2.compute.internal', u'primary': True, u'privateIpAddress': u'172.31.47.239'}]}, u'privateIpAddress': u'172.31.47.239'}]}, u'ebsOptimi
                  zed': False, u'launchTime': 1454590338000, u'architecture': u'x86_64', u'instanceState': {u'code': 0, u'name': u'pending'}, u'rootDeviceType': u'ebs', u'rootDeviceName': u'/dev/sda1'}]}}
                  ","awsRegion":"us-west-2","eventName":"RunInstances","userIdentity":"{u'userName': u'jlruizmlg', u'principalId': u'809629481101', u'accessKeyId': u'ASIAJ5M4T4PYRHIXNGGQ', u'sessionContex
                  t': {u'attributes': {u'creationDate': u'2016-02-04T10:52:14Z', u'mfaAuthenticated': u'false'}}, u'type': u'Root', u'arn': u'arn:aws:iam::809629481101:root', u'accountId': u'809629481101'
                  }","eventSource":"ec2.amazonaws.com","requestID":"c21bc7b3-bcf6-4f92-9ba0-7a3e663e0b4a","userAgent":"console.ec2.amazonaws.com","sourceIPAddress":"77.231.229.112","recipientAccountId":"8
                  09629481101"
host              da9cf9ab7aff
id                ASIAJ5M4T4PYRHIXNGGQ
location          /var/log/amazon/amazon.log
path              /var/ossec/logs/alerts/alerts.json
rule.AlertLevel   2
rule.PCI_DSS      10.6.1
rule.description  Amazon-ec2: Run instance
rule.firedtimes   1
rule.groups       Amazon-ec2, amazon
rule.sidid        80,301
type              ossec-alerts
```

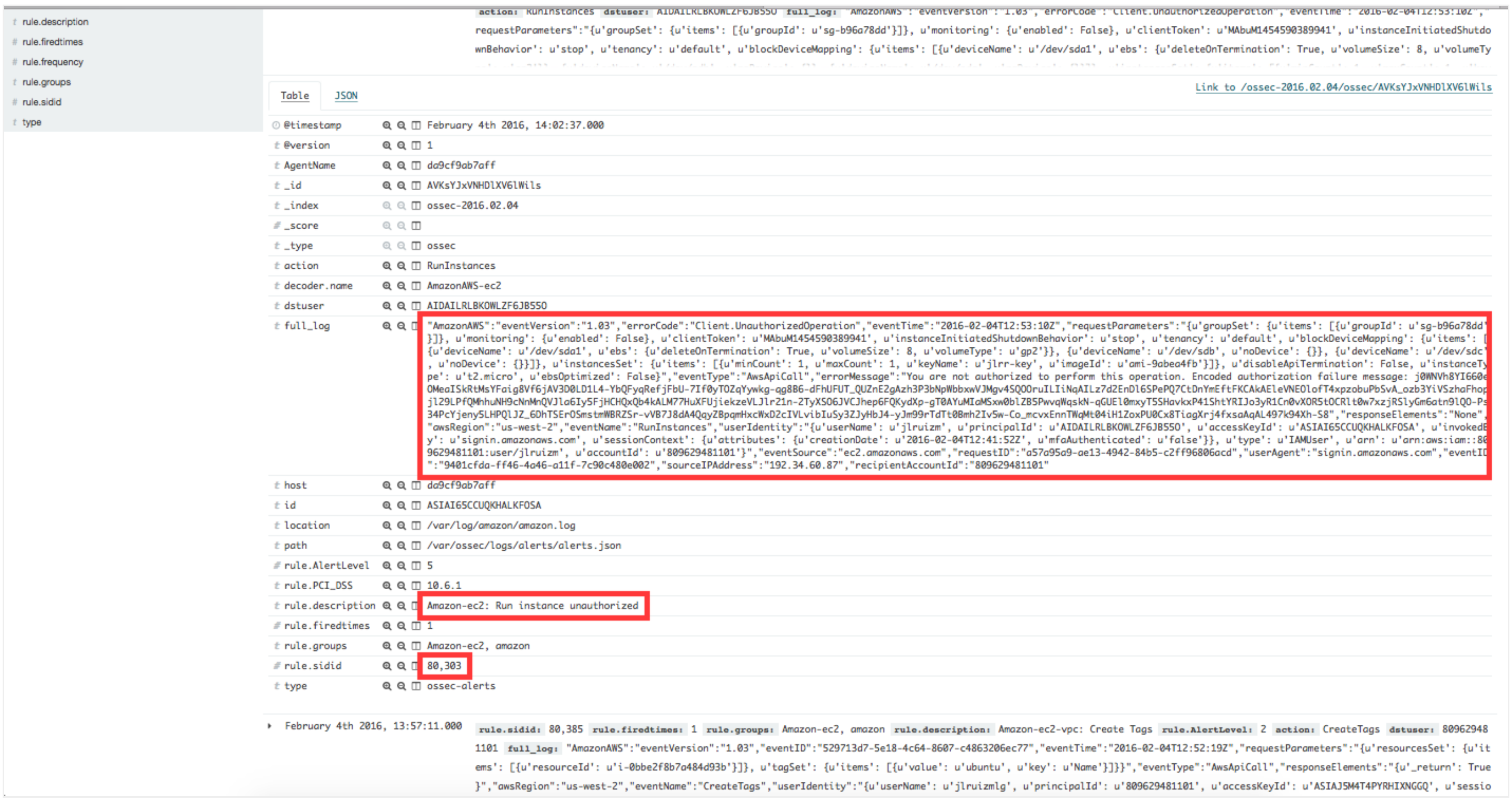
When a user tries to run an instance **without relevant permissions**, then the log message will match `rule 80303` and an alert will be generated as seen below:

Definition of rule 80303

Copied to clipboard

```
<rule id="80301" level="2">
    <if_sid>80301</if_sid>
    <match>"errorCode":"Client.UnauthorizedOperation"</match>
    <description>Amazon-ec2: Run instance unauthorized</description>
    <group>amazon,pci_dss_10.6.1,</group>
</rule>
```

Kibana will show this alert



```
rule.description
rule.firedtimes
rule.frequency
rule.groups
rule.sidid
type

action: RunInstances dstuser: AIDAILRLBKOWLZF6JB55O full_log: "AmazonAWS":"eventVersion":"1.03","errorCode":"Client.UnauthorizedOperation","eventTime":"2016-02-04T12:53:10Z",
requestParameters":"{u'groupSet': {u'items': [{u'groupId': u'sg-b96a78dd'}]}, u'monitoring': {u'enabled': False}, u'clientToken': u'MAbuM1454590389941', u'instanceInitiatedShutdo
wnBehavior': u'stop', u'tenancy': u'default', u'blockDeviceMapping': {u'items': [{u'deviceName': u'/dev/sda1', u'ebs': {u'deleteOnTermination': True, u'volumeSize': 8, u'volumeTy

Table   JSON                                                         Link to /ossec-2016.02.04/ossec/AVKsYJxVNHDlXV6lWils

@timestamp        February 4th 2016, 14:02:37.000
@version          1
AgentName         da9cf9ab7aff
_id               AVKsYJxVNHDlXV6lWils
_index            ossec-2016.02.04
_score
_type             ossec
action            RunInstances
decoder.name      AmazonAWS-ec2
dstuser           AIDAILRLBKOWLZF6JB55O
full_log          "AmazonAWS":"eventVersion":"1.03","errorCode":"Client.UnauthorizedOperation","eventTime":"2016-02-04T12:53:10Z","requestParameters":"{u'groupSet': {u'items': [{u'groupId': u'sg-b96a78dd'
                  }]}, u'monitoring': {u'enabled': False}, u'clientToken': u'MAbuM1454590389941', u'instanceInitiatedShutdownBehavior': u'stop', u'tenancy': u'default', u'blockDeviceMapping': {u'items': [
                  {u'deviceName': u'/dev/sda1', u'ebs': {u'deleteOnTermination': True, u'volumeSize': 8, u'volumeType': u'gp2'}}, {u'deviceName': u'/dev/sdb', u'noDevice': {}}, {u'deviceName': u'/dev/sdc'
                  , u'noDevice': {}}]}, u'instancesSet': {u'items': [{u'minCount': 1, u'maxCount': 1, u'keyName': u'jlrr-key', u'imageId': u'ami-9abea4fb'}]}, u'disableApiTermination': False, u'instanceTy
                  pe': u't2.micro', u'ebsOptimized': False}","eventType":"AwsApiCall","errorMessage":"You are not authorized to perform this operation. Encoded authorization failure message: j0WNVh8YI660e
                  OMeaISkRtMsYFaig8Vf6jAV3D0LD1L4-YbQFyqRefjFbU-7If0yTOZqYywkg-qg8B6-dFhUFUT_QUZnE2gAzh3P3bNpWbbxwVJMgv4SQOOruILIiNqAILz7d2EnDl6SPePQ7CtDnYmEftFKCAkAEleVNEOlofT4xpzobuPbSvA_ozb3YiVSzhaFhop
                  jl29LPfQMhhuNH9cNnMnQVJla6Iy5FjHCHQxQb4kALM77HuXFUjiekzeVLJlr21n-2TyXSO6JVCJhep6FQKydXp-gT0AYuMIaMSxw0blZB5PwvqWqskN-qGUEl0mxyT5SHavkxP41ShtYRIJo3yR1Cn0vXOR5tOCRlt0w7xzjRSlyGm6atn9lQO-Ps
                  34PcYjeny5LHPQlJZ_6DhTSErOSmstmWBRZSr-vVB7J8dA4QqyZBpqmHxcWxD2cIVLvibIuSy3ZJyHbJ4-yJm99rTdTt0Bmh2Iv5w-Co_mcvxEnnTWqMt04iH1ZoxPU0Cx8TiagXrj4fxsaAqAL497k94Xh-S8","responseElements":"None",
                  "awsRegion":"us-west-2","eventName":"RunInstances","userIdentity":"{u'userName': u'jlruizm', u'principalId': u'AIDAILRLBKOWLZF6JB55O', u'accessKeyId': u'ASIAI65CCUQKHALKFOSA', u'invokedB
                  y': u'signin.amazonaws.com', u'sessionContext': {u'attributes': {u'creationDate': u'2016-02-04T12:41:52Z', u'mfaAuthenticated': u'false'}}, u'type': u'IAMUser', u'arn': u'arn:aws:iam::80
                  9629481101:user/jlruizm', u'accountId': u'809629481101'}","eventSource":"ec2.amazonaws.com","requestID":"a57a95a9-ae13-4942-84b5-c2ff96806acd","userAgent":"signin.amazonaws.com","eventID
                  ":"9401cfda-ff46-4a46-a11f-7c90c480e002","sourceIPAddress":"192.34.60.87","recipientAccountId":"809629481101"
host              da9cf9ab7aff
id                ASIAI65CCUQKHALKFOSA
location          /var/log/amazon/amazon.log
path              /var/ossec/logs/alerts/alerts.json
rule.AlertLevel   5
rule.PCI_DSS      10.6.1
rule.description  Amazon-ec2: Run instance unauthorized
rule.firedtimes   1
rule.groups       Amazon-ec2, amazon
rule.sidid        80,303
type              ossec-alerts

▸ February 4th 2016, 13:57:11.000   rule.sidid: 80,385 rule.firedtimes: 1 rule.groups: Amazon-ec2, amazon rule.description: Amazon-ec2-vpc: Create Tags rule.AlertLevel: 2 action: CreateTags dstuser: 80962948
                                    1101 full_log: "AmazonAWS":"eventVersion":"1.03","eventID":"529713d7-5e18-4c64-8607-c4863206ec77","eventTime":"2016-02-04T12:52:19Z","requestParameters":"{u'resourcesSet': {u'it
                                    ems': [{u'resourceId': u'i-0bbe2f8b7a484d93b'}]}, u'tagSet': {u'items': [{u'value': u'ubuntu', u'key': u'Name'}]}}","eventType":"AwsApiCall","responseElements":"{u'_return': True
                                    }","awsRegion":"us-west-2","eventName":"CreateTags","userIdentity":"{u'userName': u'jlruizmlg', u'principalId': u'809629481101', u'accessKeyId': u'ASIAJ5M4T4PYRHIXNGGQ', u'sessio
```

Start instances in EC2

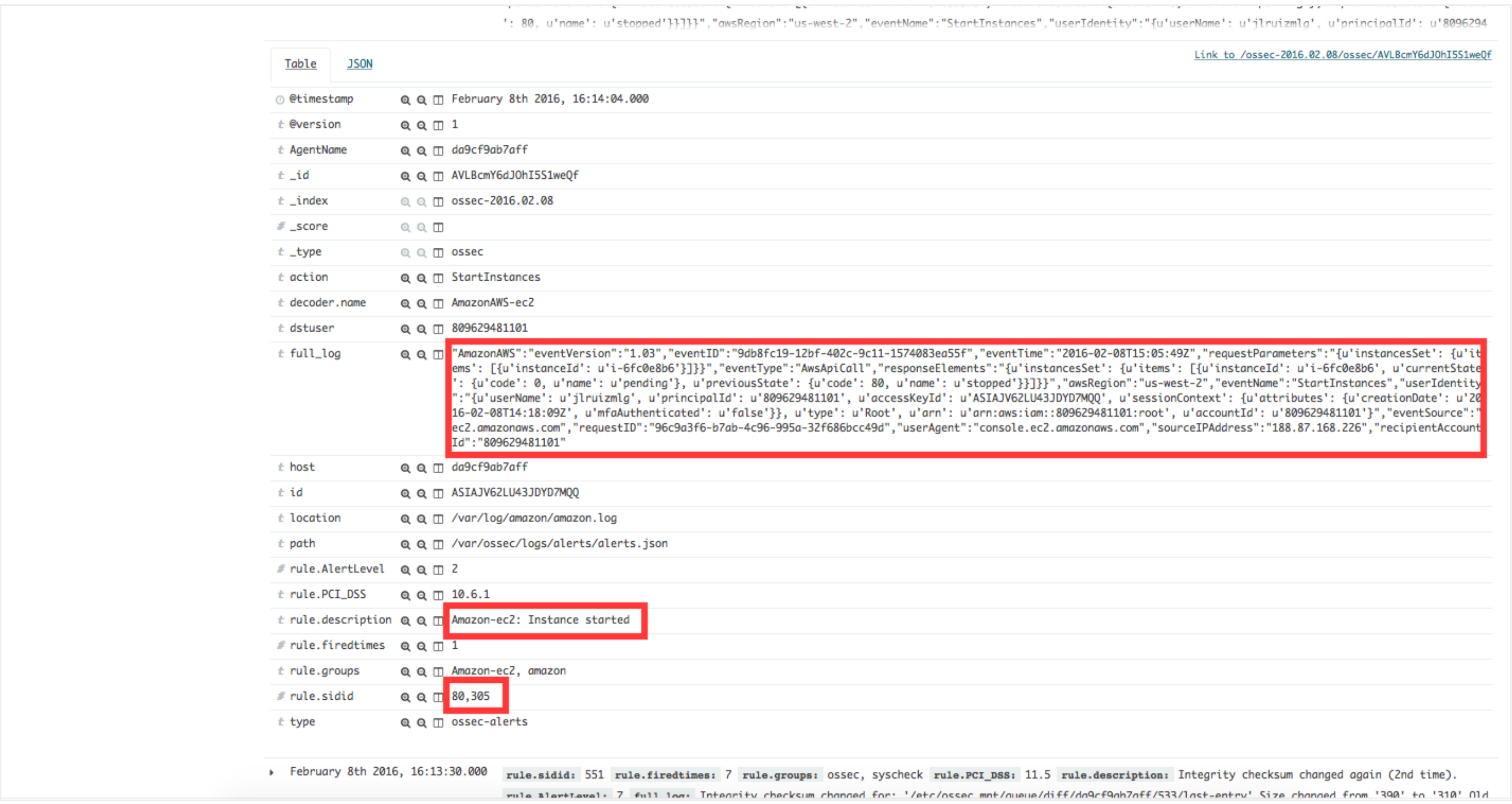
When an instance in EC2 is started, the log message will match `rule 80305` and an alert will be generated as shown below:

Definition of rule 80305

Copied to clipboard

```
<rule id="80305" level="2">
    <if_sid>80300</if_sid>
    <action>StartInstances</action>
    <description>Amazon-ec2: Instance started</description>
    <group>amazon,pci_dss_10.6.1,</group>
</rule>
```

Kibana will show this alert



```
': 80, u'name': u'stopped'}}]}}","awsRegion":"us-west-2","eventName":"StartInstances","userIdentity":"{u'userName': u'jlruizmlg', u'principalId': u'8096294

Table   JSON                                                         Link to /ossec-2016.02.08/ossec/AVLBcmY6dJOhI5S1weQf

@timestamp        February 8th 2016, 16:14:04.000
@version          1
AgentName         da9cf9ab7aff
_id               AVLBcmY6dJOhI5S1weQf
_index            ossec-2016.02.08
_score
_type             ossec
action            StartInstances
decoder.name      AmazonAWS-ec2
dstuser           809629481101
full_log          "AmazonAWS":"eventVersion":"1.03","eventID":"9db8fc19-12bf-402c-9c11-1574083ea55f","eventTime":"2016-02-08T15:05:49Z","requestParameters":"{u'instancesSet': {u'it
                  ems': [{u'instanceId': u'i-6fc0e8b6'}]}}","eventType":"AwsApiCall","responseElements":"{u'instancesSet': {u'items': [{u'instanceId': u'i-6fc0e8b6', u'currentState
                  ': {u'code': 0, u'name': u'pending'}, u'previousState': {u'code': 80, u'name': u'stopped'}}]}}","awsRegion":"us-west-2","eventName":"StartInstances","userIdentity
                  ":"{u'userName': u'jlruizmlg', u'principalId': u'809629481101', u'accessKeyId': u'ASIAJV62LU43JDYD7MQQ', u'sessionContext': {u'attributes': {u'creationDate': u'20
                  16-02-08T14:18:09Z', u'mfaAuthenticated': u'false'}}, u'type': u'Root', u'arn': u'arn:aws:iam::809629481101:root', u'accountId': u'809629481101'}","eventSource":"
                  ec2.amazonaws.com","requestID":"96c9a3f6-b7ab-4c96-995a-32f686bcc49d","userAgent":"console.ec2.amazonaws.com","sourceIPAddress":"188.87.168.226","recipientAccount
                  Id":"809629481101"
host              da9cf9ab7aff
id                ASIAJV62LU43JDYD7MQQ
location          /var/log/amazon/amazon.log
path              /var/ossec/logs/alerts/alerts.json
rule.AlertLevel   2
rule.PCI_DSS      10.6.1
rule.description  Amazon-ec2: Instance started
rule.firedtimes   1
rule.groups       Amazon-ec2, amazon
rule.sidid        80,305
type              ossec-alerts

▸ February 8th 2016, 16:13:30.000   rule.sidid: 551 rule.firedtimes: 7 rule.groups: ossec, syscheck rule.PCI_DSS: 11.5 rule.description: Integrity checksum changed again (2nd time).
                                    rule.AlertLevel: 7 full_log: Integrity checksum changed for: '/etc/ossec_mnt/queue/diff/da9cf9ab7aff/533/last-entry' Size changed from '390' to '310' Old
```

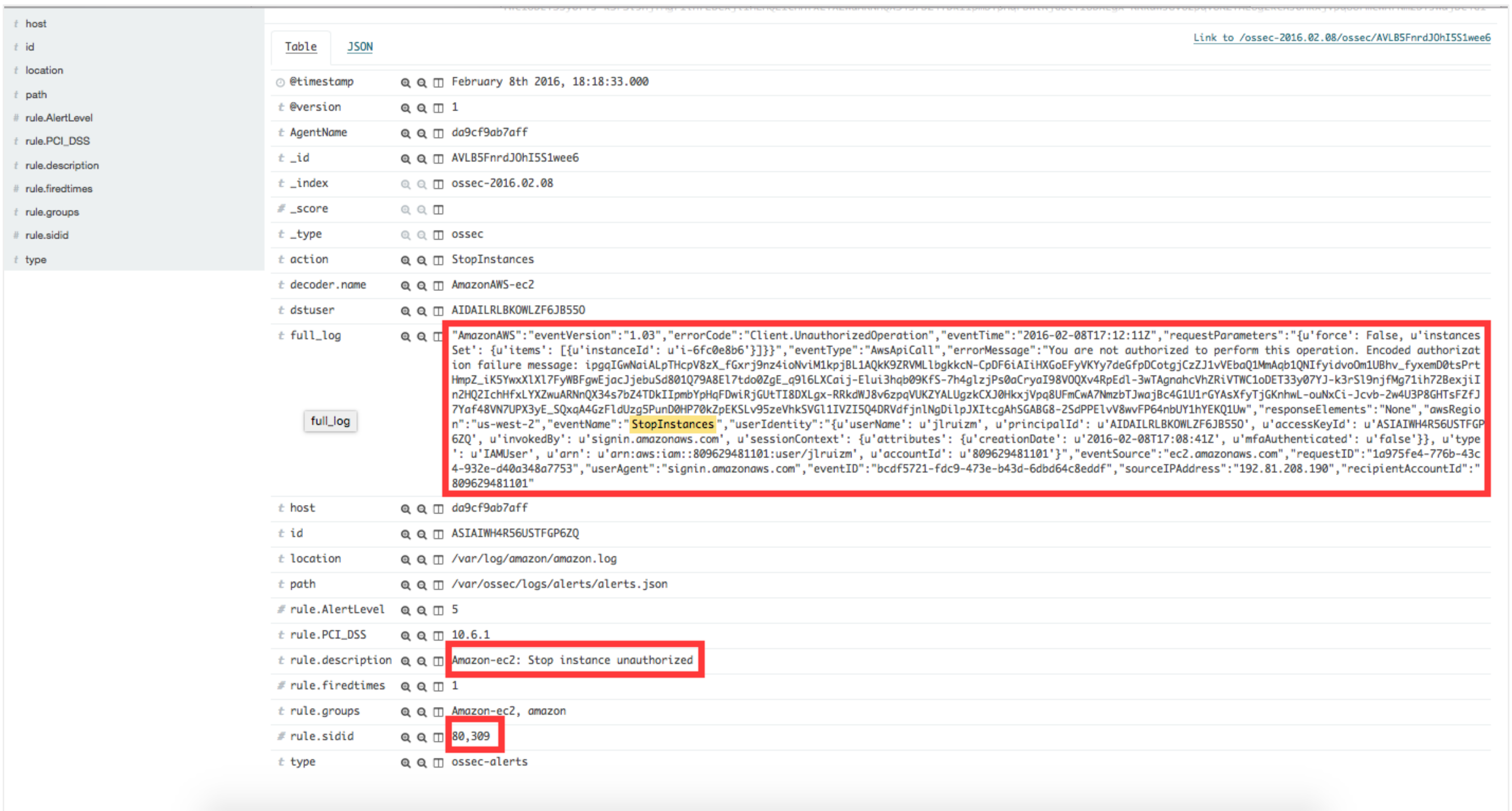
If a user tries to start instances **without relevant permissions**, `rule 80306` will apply and an alert will be generated as shown below:

Definition of rule 80306

Copied to clipboard

```
<rule id="80306" level="5">
    <if_sid>80305</if_sid>
    <match>"errorCode":"Client.UnauthorizedOperation"</match>
    <description>Amazon-ec2: Start instance unauthorized</description>
    <group>amazon,pci_dss_10.6.1,</group>
</rule>
```

Kibana will show this alert



host
id
location
path
rule.AlertLevel
rule.PCI_DSS
rule.description
rule.firedtimes
rule.groups
rule.sidid
type

Link to /ossec-2016.02.08/ossec/AVLB5FnrdJOhI5S1wee6

```
@timestamp         February 8th 2016, 18:18:33.000
@version           1
AgentName          da9cf9ab7aff
_id                AVLB5FnrdJOhI5S1wee6
_index             ossec-2016.02.08
_score
_type              ossec
action             StopInstances
decoder.name       AmazonAWS-ec2
dstuser            AIDAILRLBKOWLZF6JB55O
full_log           "AmazonAWS":"eventVersion":"1.03","errorCode":"Client.UnauthorizedOperation","eventTime":"2016-02-08T17:12:11Z","requestParameters":"{u'force': False, u'instances
                   Set': {u'items': [{u'instanceId': u'i-6fc0e8b6'}]}}","eventType":"AwsApiCall","errorMessage":"You are not authorized to perform this operation. Encoded authorizat
                   ion failure message: ipgqIGwNaiALpTHcpV8zX_fGxrj9nz4ioNviM1kpjBL1AQkK9ZRVMLlbgkkcN-CpDF6iAIiHXGoEFyVKYy7deGfpDCotgjCzZJ1vVEbaQ1MmAqb1QNIfyidvoOm1UBhv_fyxemD0tsPrt
                   HmpZ_iK5YwxXlXl7FyWBFgwEjacJjebuSd801Q79A8El7tdo0ZgE_q9l6LXCaij-Elui3hqb09KfS-7h4glzjPs0aCryaI98VOQXv4RpEdl-3wTAgnahcVhZRiVTWC1oDET33y07YJ-k3rSl9njfMg71ih72BexjiI
                   n2HQ2IchHfxLYXZwuARNnQX34s7bZ4TDkIIpmbYpHqFDwiRjGUtTI8DXLgx-RRkdWJ8v6zpqVUKZYALUgzkCXJ0HkxjVpq8UFmCwA7NmzbTJwajBc4G1U1rGYAsXfyTjGKnhwL-ouNxCi-Jcvb-2w4U3P8GHTsFZfJ
                   7Yaf48VN7UPX3yE_SQxqA4GzFldUzg5PunD0HP70kZpEKSLv95zeVhkSVGl1IVZI5Q4DRVdfjnlNgDilpJXItcgAhSGABG8-2SdPPElvV8wvFP64nbUY1hYEKQ1Uw","responseElements":"None","awsRegio
                   n":"us-west-2","eventName":"StopInstances","userIdentity":"{u'userName': u'jlruizm', u'principalId': u'AIDAILRLBKOWLZF6JB55O', u'accessKeyId': u'ASIAIWH4R56USTFGP
                   6ZQ', u'invokedBy': u'signin.amazonaws.com', u'sessionContext': {u'attributes': {u'creationDate': u'2016-02-08T17:08:41Z', u'mfaAuthenticated': u'false'}}, u'type
                   ': u'IAMUser', u'arn': u'arn:aws:iam::809629481101:user/jlruizm', u'accountId': u'809629481101'}","eventSource":"ec2.amazonaws.com","requestID":"1a975fe4-776b-43c
                   4-932e-d40a348a7753","userAgent":"signin.amazonaws.com","eventID":"bcdf5721-fdc9-473e-b43d-6dbd64c8eddf","sourceIPAddress":"192.81.208.190","recipientAccountId":"
                   809629481101"
host               da9cf9ab7aff
id                 ASIAIWH4R56USTFGP6ZQ
location           /var/log/amazon/amazon.log
path               /var/ossec/logs/alerts/alerts.json
rule.AlertLevel    5
rule.PCI_DSS       10.6.1
rule.description   Amazon-ec2: Stop instance unauthorized
rule.firedtimes    1
rule.groups        Amazon-ec2, amazon
rule.sidid         80,309
type               ossec-alerts
```

Stop instances in EC2

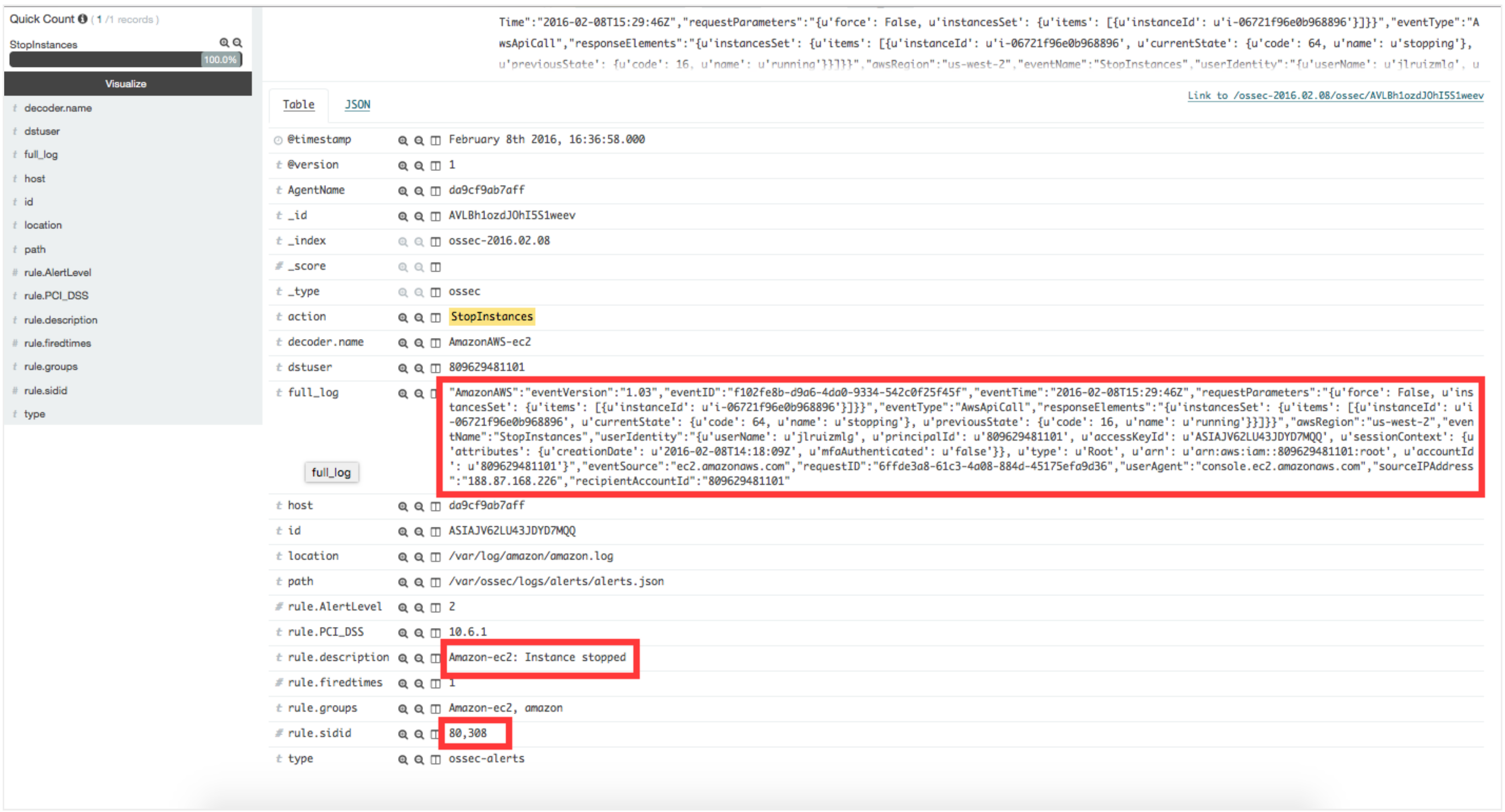
When an instance in EC2 is stopped, `rule 80308` will apply and an alert will be generated as shown below:

Definition of rule 80308

Copied to clipboard

```
<rule id="80308" level="2">
    <if_sid>80300</if_sid>
    <action>StopInstances</action>
    <description>Amazon-ec2: Instance stopped</description>
    <group>amazon,pci_dss_10.6.1,</group>
</rule>
```

Kibana will show this alert



```
Time":"2016-02-08T15:29:46Z","requestParameters":"{u'force': False, u'instancesSet': {u'items': [{u'instanceId': u'i-06721f96e0b968896'}]}}","eventType":"A
wsApiCall","responseElements":"{u'instancesSet': {u'items': [{u'instanceId': u'i-06721f96e0b968896', u'currentState': {u'code': 64, u'name': u'stopping'},
u'previousState': {u'code': 16, u'name': u'running'}}]}}","awsRegion":"us-west-2","eventName":"StopInstances","userIdentity":"{u'userName': u'jlruizmlg', u

                                                                        Link to /ossec-2016.02.08/ossec/AVLBh1ozdJOhI5S1weev

@timestamp         February 8th 2016, 16:36:58.000
@version           1
AgentName          da9cf9ab7aff
_id                AVLBh1ozdJOhI5S1weev
_index             ossec-2016.02.08
_score
_type              ossec
action             StopInstances
decoder.name       AmazonAWS-ec2
dstuser            809629481101
full_log           "AmazonAWS":"eventVersion":"1.03","eventID":"f102fe8b-d9a6-4da0-9334-542c0f25f45f","eventTime":"2016-02-08T15:29:46Z","requestParameters":"{u'force': False, u'ins
                   tancesSet': {u'items': [{u'instanceId': u'i-06721f96e0b968896'}]}}","eventType":"AwsApiCall","responseElements":"{u'instancesSet': {u'items': [{u'instanceId': u'i
                   -06721f96e0b968896', u'currentState': {u'code': 64, u'name': u'stopping'}, u'previousState': {u'code': 16, u'name': u'running'}}]}}","awsRegion":"us-west-2","even
                   tName":"StopInstances","userIdentity":"{u'userName': u'jlruizmlg', u'principalId': u'809629481101', u'accessKeyId': u'ASIAJV62LU43JDYD7MQQ', u'sessionContext': {u
                   'attributes': {u'creationDate': u'2016-02-08T14:18:09Z', u'mfaAuthenticated': u'false'}}, u'type': u'Root', u'arn': u'arn:aws:iam::809629481101:root', u'accountId
                   ': u'809629481101'}","eventSource":"ec2.amazonaws.com","requestID":"6ffde3a8-61c3-4a08-884d-45175efa9d36","userAgent":"console.ec2.amazonaws.com","sourceIPAddress
                   ":"188.87.168.226","recipientAccountId":"809629481101"
host               da9cf9ab7aff
id                 ASIAJV62LU43JDYD7MQQ
location           /var/log/amazon/amazon.log
path               /var/ossec/logs/alerts/alerts.json
rule.AlertLevel    2
rule.PCI_DSS       10.6.1
rule.description   Amazon-ec2: Instance stopped
rule.firedtimes    1
rule.groups        Amazon-ec2, amazon
rule.sidid         80,308
type               ossec-alerts
```

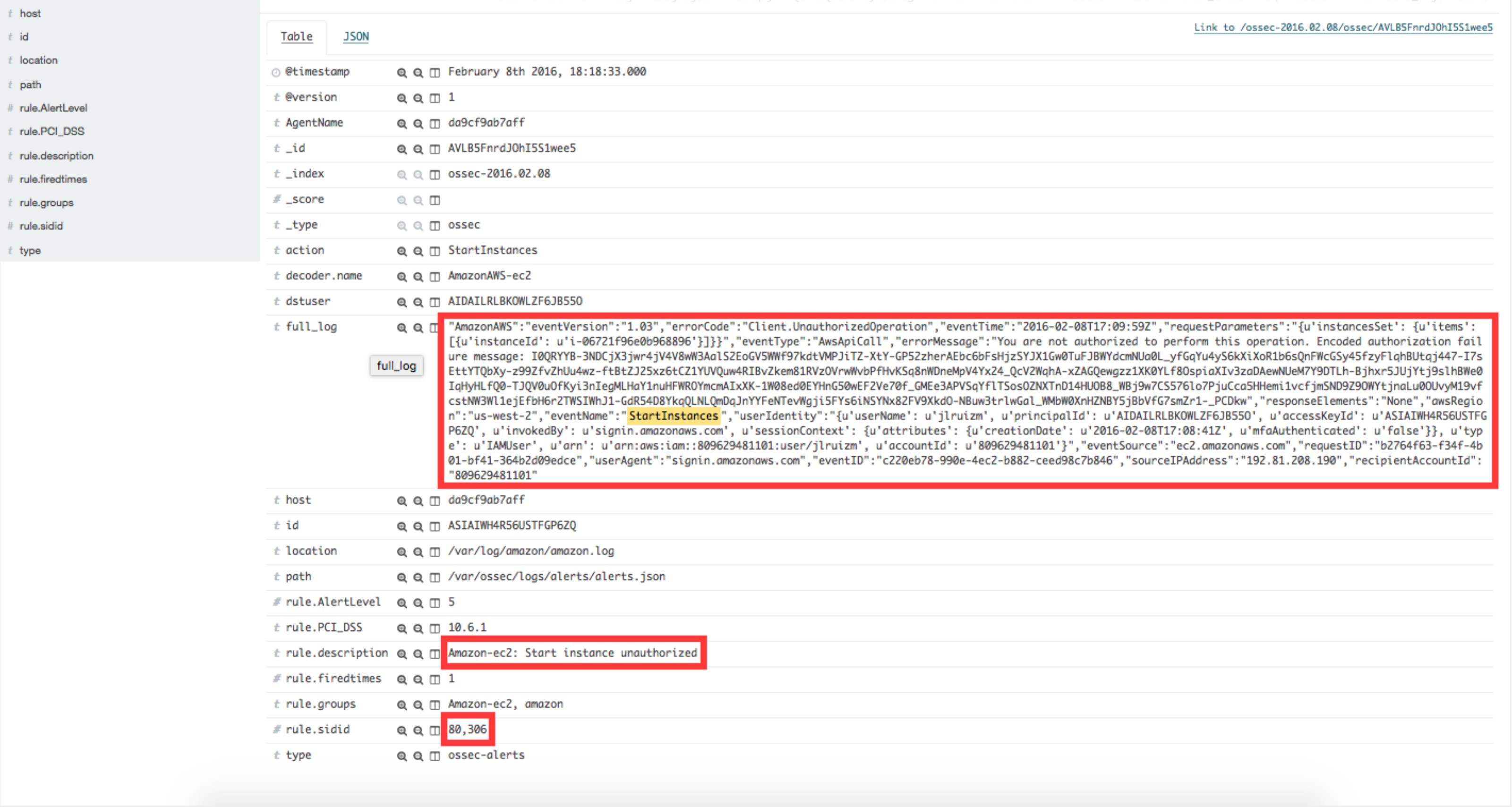
If a user tries to stop instances **without relevant permissions**, `rule 80306` will apply and an alert will be generated as shown below:

Definition of rule 80309

Copied to clipboard

```
<rule id="80309" level="5">
    <if_sid>80308</if_sid>
    <action>StopInstances</action>
    <match>"errorCode":"Client.UnauthorizedOperation"</match>
    <description>Amazon-ec2: Stop instance unauthorized</description>
    <group>amazon,pci_dss_10.6.1,</group>
</rule>
```

Kibana will show this alert



```
                                                                        Link to /ossec-2016.02.08/ossec/AVLB5FnrdJOhI5S1wee5

@timestamp         February 8th 2016, 18:18:33.000
@version           1
AgentName          da9cf9ab7aff
_id                AVLB5FnrdJOhI5S1wee5
_index             ossec-2016.02.08
_score
_type              ossec
action             StartInstances
decoder.name       AmazonAWS-ec2
dstuser            AIDAILRLBKOWLZF6JB55O
full_log           "AmazonAWS":"eventVersion":"1.03","errorCode":"Client.UnauthorizedOperation","eventTime":"2016-02-08T17:09:59Z","requestParameters":"{u'instancesSet': {u'items':
                   [{u'instanceId': u'i-06721f96e0b968896'}]}}","eventType":"AwsApiCall","errorMessage":"You are not authorized to perform this operation. Encoded authorization fail
                   ure message: I0QRYYB-3NDCjX3jwr4jV4V8wW3AalS2EoGV5WWf97kdtVMPJiTZ-XtY-GP52zherAEbc6bFsHjzSYJX1Gw0TuFJBWYdcmNUa0L_yfGqYu4yS6kXiXoR1b6sQnFWcGSy45fzyFlqhBUtqj447-I7s
                   EttYTQbXy-z99ZfvZhUu4wz-ftBtZJ25xz6tCZ1YUVQuw4RIBvZkem81RVzOVrwWvbPfHvKSq8nWDneMpV4Yx24_QcV2WqhA-xZAGQewgzz1XK0YLf8OspiaXIv3zaDAewNUeM7Y9DTLh-Bjhxr5JUjYtj9slhBWe0
                   IqHyHLfQ0-TJQV0uOfKyi3nIegMLHaY1nuHFWROYmcmAIxXK-1W08ed0EYHnG50wEF2Ve70f_GMEe3APVSqYflTSosOZNXTnD14HUOB8_WBj9w7CS576lo7PjuCca5HHemi1vcfjmSND9Z9OWYtjnaLu0OUvyM19vf
                   cstNW3Wl1ejEfbH6r2TWSIWhJ1-GdR54D8YkqQLNLQmDqJnYYFeNTevWgji5FYs6iNSYNx82FV9XkdO-NBuw3trlwGal_WMbW0XnHZNBY5jBbVfG7smZr1-_PCDkw","responseElements":"None","awsRegio
                   n":"us-west-2","eventName":"StartInstances","userIdentity":"{u'userName': u'jlruizm', u'principalId': u'AIDAILRLBKOWLZF6JB55O', u'accessKeyId': u'ASIAIWH4R56USTFG
                   P6ZQ', u'invokedBy': u'signin.amazonaws.com', u'sessionContext': {u'attributes': {u'creationDate': u'2016-02-08T17:08:41Z', u'mfaAuthenticated': u'false'}}, u'typ
                   e': u'IAMUser', u'arn': u'arn:aws:iam::809629481101:user/jlruizm', u'accountId': u'809629481101'}","eventSource":"ec2.amazonaws.com","requestID":"b2764f63-f34f-4b
                   01-bf41-364b2d09edce","userAgent":"signin.amazonaws.com","eventID":"c220eb78-990e-4ec2-b882-ceed98c7b846","sourceIPAddress":"192.81.208.190","recipientAccountId":
                   "809629481101"
host               da9cf9ab7aff
id                 ASIAIWH4R56USTFGP6ZQ
location           /var/log/amazon/amazon.log
path               /var/ossec/logs/alerts/alerts.json
rule.AlertLevel    5
rule.PCI_DSS       10.6.1
rule.description   Amazon-ec2: Start instance unauthorized
rule.firedtimes    1
rule.groups        Amazon-ec2, amazon
rule.sidid         80,306
type               ossec-alerts
```

Create Security Groups in EC2

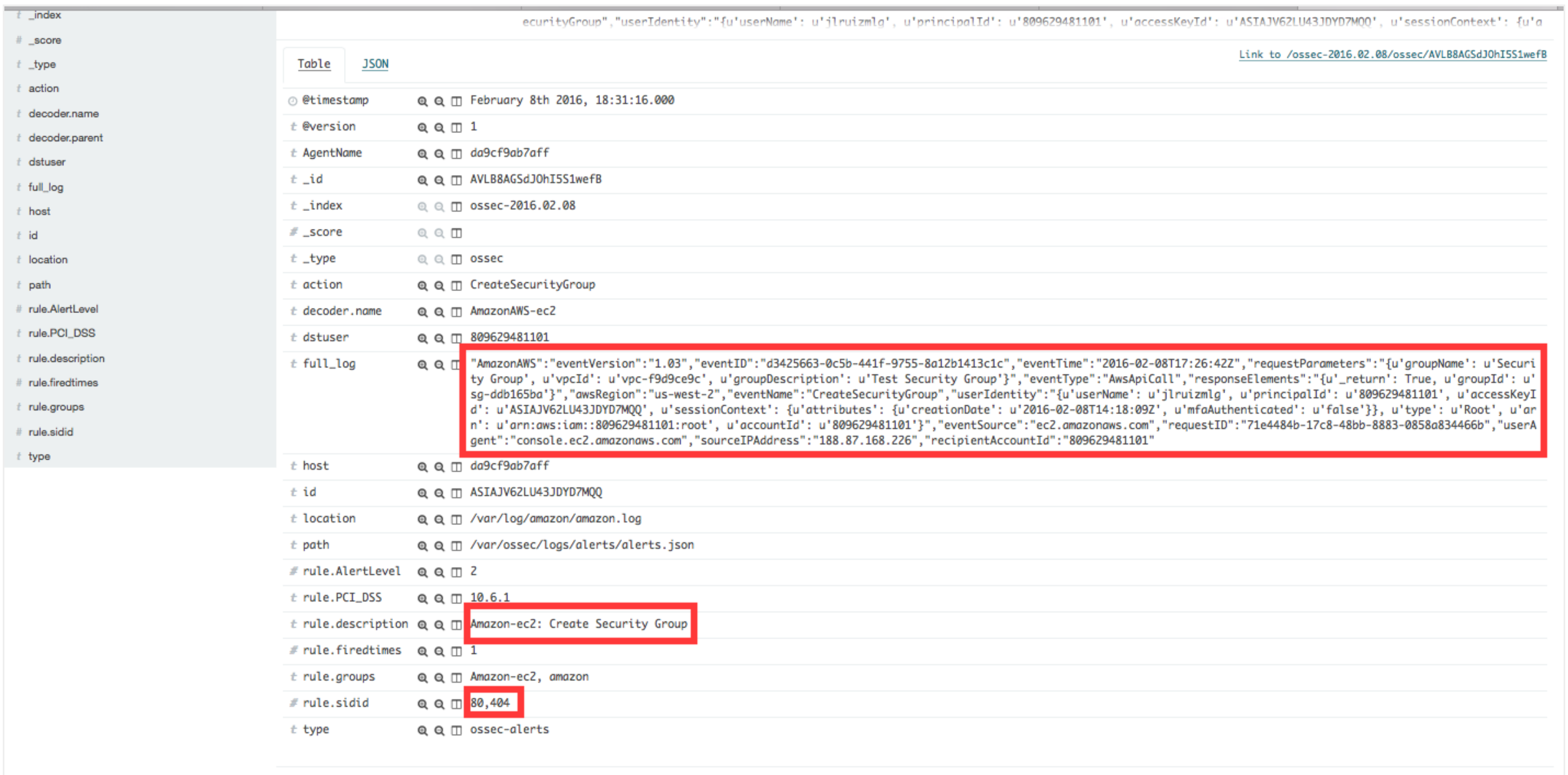
When a new security group is created, `rule 80404` will fire and an alert will be shown as follows:

Definition of rule 80404

Copied to clipboard

```
<rule id="80404" level="2">
    <if_sid>80300</if_sid>
    <action>CreateSecurityGroup</action>
    <description>Amazon-ec2: Create Security Group</description>
    <group>amazon,pci_dss_10.6.1,</group>
</rule>
```

Kibana will show this alert



```
ecurityGroup","userIdentity":"{u'userName': u'jlruizmlg', u'principalId': u'809629481101', u'accessKeyId': u'ASIAJV62LU43JDYD7MQQ', u'sessionContext': {u'a

@timestamp        February 8th 2016, 18:31:16.000
@version          1
AgentName         da9cf9ab7aff
_id               AVLB8AGSdJOhI5S1wefB
_index            ossec-2016.02.08
_score
_type             ossec
action            CreateSecurityGroup
decoder.name      AmazonAWS-ec2
dstuser           809629481101
full_log          "AmazonAWS":"eventVersion":"1.03","eventID":"d3425663-0c5b-441f-9755-8a12b1413c1c","eventTime":"2016-02-08T17:26:42Z","requestParameters":"{u'groupName': u'Securi
                  ty Group', u'vpcId': u'vpc-f9d9ce9c', u'groupDescription': u'Test Security Group'}","eventType":"AwsApiCall","responseElements":"{u'_return': True, u'groupId': u'
                  sg-ddb165ba'}","awsRegion":"us-west-2","eventName":"CreateSecurityGroup","userIdentity":"{u'userName': u'jlruizmlg', u'principalId': u'809629481101', u'accessKeyI
                  d': u'ASIAJV62LU43JDYD7MQQ', u'sessionContext': {u'attributes': {u'creationDate': u'2016-02-08T14:18:09Z', u'mfaAuthenticated': u'false'}}, u'type': u'Root', u'ar
                  n': u'arn:aws:iam::809629481101:root', u'accountId': u'809629481101'}","eventSource":"ec2.amazonaws.com","requestID":"71e4484b-17c8-48bb-8883-0858a834466b","userA
                  gent":"console.ec2.amazonaws.com","sourceIPAddress":"188.87.168.226","recipientAccountId":"809629481101"
host              da9cf9ab7aff
id                ASIAJV62LU43JDYD7MQQ
location          /var/log/amazon/amazon.log
path              /var/ossec/logs/alerts/alerts.json
rule.AlertLevel   2
rule.PCI_DSS      10.6.1
rule.description  Amazon-ec2: Create Security Group
rule.firedtimes   1
rule.groups       Amazon-ec2, amazon
rule.sidid        80,404
type              ossec-alerts
```

Allocate a new Elastic IP address

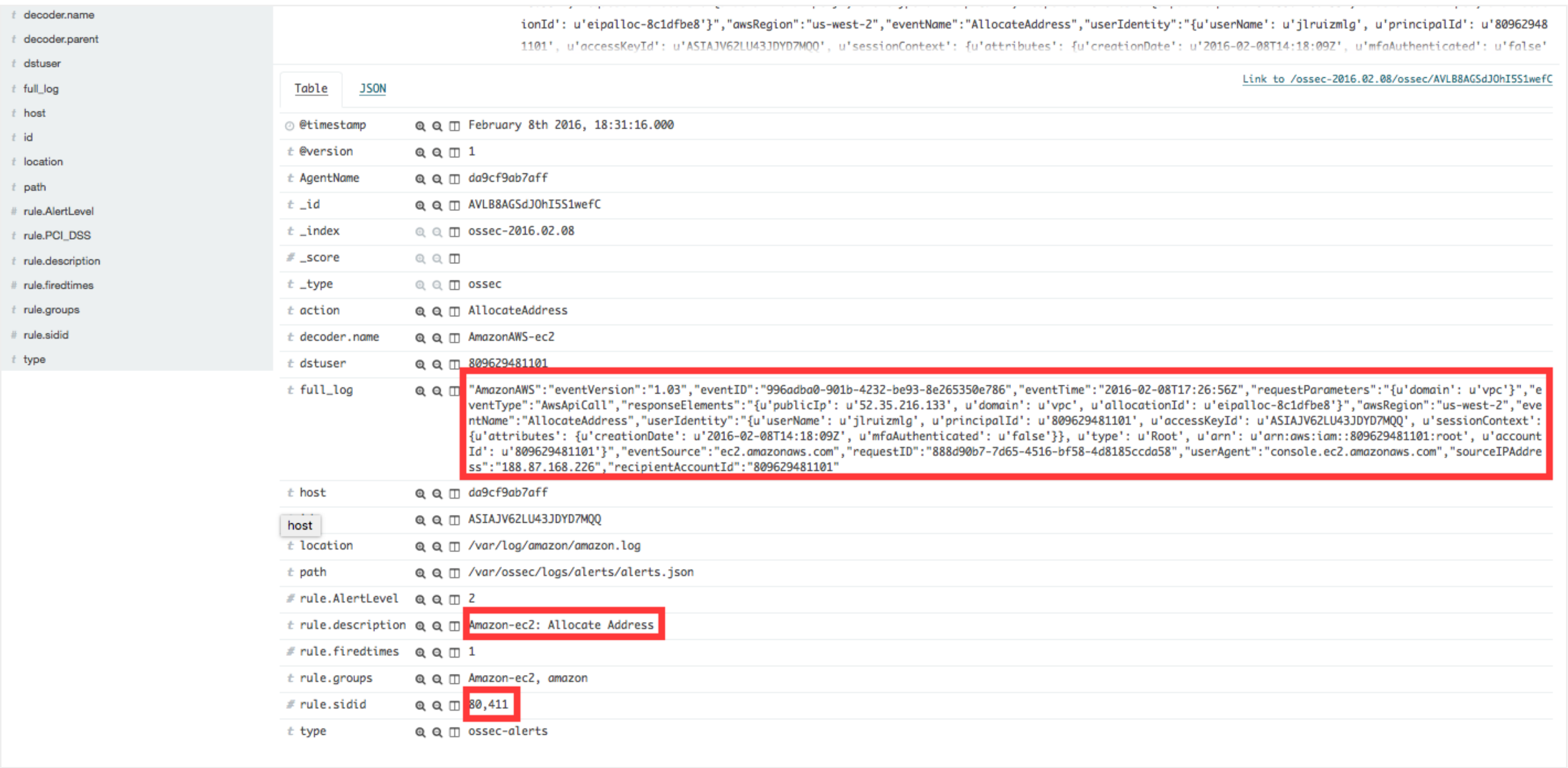
If a new Elastic IP is allocated, then `rule 80411` will apply:

Definition of rule 80411

Copied to clipboard

```
<rule id="80411" level="2">
    <if_sid>80300</if_sid>
    <action>AllocateAddress</action>
    <description>Amazon-ec2: Allocate Address</description>
    <group>amazon,</group>
</rule>
```

Kibana will show this alert



```
ionId': u'eipalloc-8c1dfbe8'}","awsRegion":"us-west-2","eventName":"AllocateAddress","userIdentity":"{u'userName': u'jlruizmlg', u'principalId': u'80962948
1101', u'accessKeyId': u'ASIAJV62LU43JDYD7MQQ', u'sessionContext': {u'attributes': {u'creationDate': u'2016-02-08T14:18:09Z', u'mfaAuthenticated': u'false'

Link to /ossec-2016.02.08/ossec/AVLB8AGSdJOhI5S1wefC

@timestamp        February 8th 2016, 18:31:16.000
@version          1
AgentName         da9cf9ab7aff
_id               AVLB8AGSdJOhI5S1wefC
_index            ossec-2016.02.08
_score
_type             ossec
action            AllocateAddress
decoder.name      AmazonAWS-ec2
dstuser           809629481101
full_log          "AmazonAWS":"eventVersion":"1.03","eventID":"996adba0-901b-4232-be93-8e265350e786","eventTime":"2016-02-08T17:26:56Z","requestParameters":"{u'domain': u'vpc'}","e
                  ventType":"AwsApiCall","responseElements":"{u'publicIp': u'52.35.216.133', u'domain': u'vpc', u'allocationId': u'eipalloc-8c1dfbe8'}","awsRegion":"us-west-2","eve
                  ntName":"AllocateAddress","userIdentity":"{u'userName': u'jlruizmlg', u'principalId': u'809629481101', u'accessKeyId': u'ASIAJV62LU43JDYD7MQQ', u'sessionContext':
                  {u'attributes': {u'creationDate': u'2016-02-08T14:18:09Z', u'mfaAuthenticated': u'false'}}, u'type': u'Root', u'arn': u'arn:aws:iam::809629481101:root', u'account
                  Id': u'809629481101'}","eventSource":"ec2.amazonaws.com","requestID":"888d90b7-7d65-4516-bf58-4d8185ccda58","userAgent":"console.ec2.amazonaws.com","sourceIPAddre
                  ss":"188.87.168.226","recipientAccountId":"809629481101"
host              da9cf9ab7aff
                  ASIAJV62LU43JDYD7MQQ
location          /var/log/amazon/amazon.log
path              /var/ossec/logs/alerts/alerts.json
rule.AlertLevel   2
rule.description  Amazon-ec2: Allocate Address
rule.firedtimes   1
rule.groups       Amazon-ec2, amazon
rule.sidid        80,411
type              ossec-alerts
```

Associate a new Elastic IP address

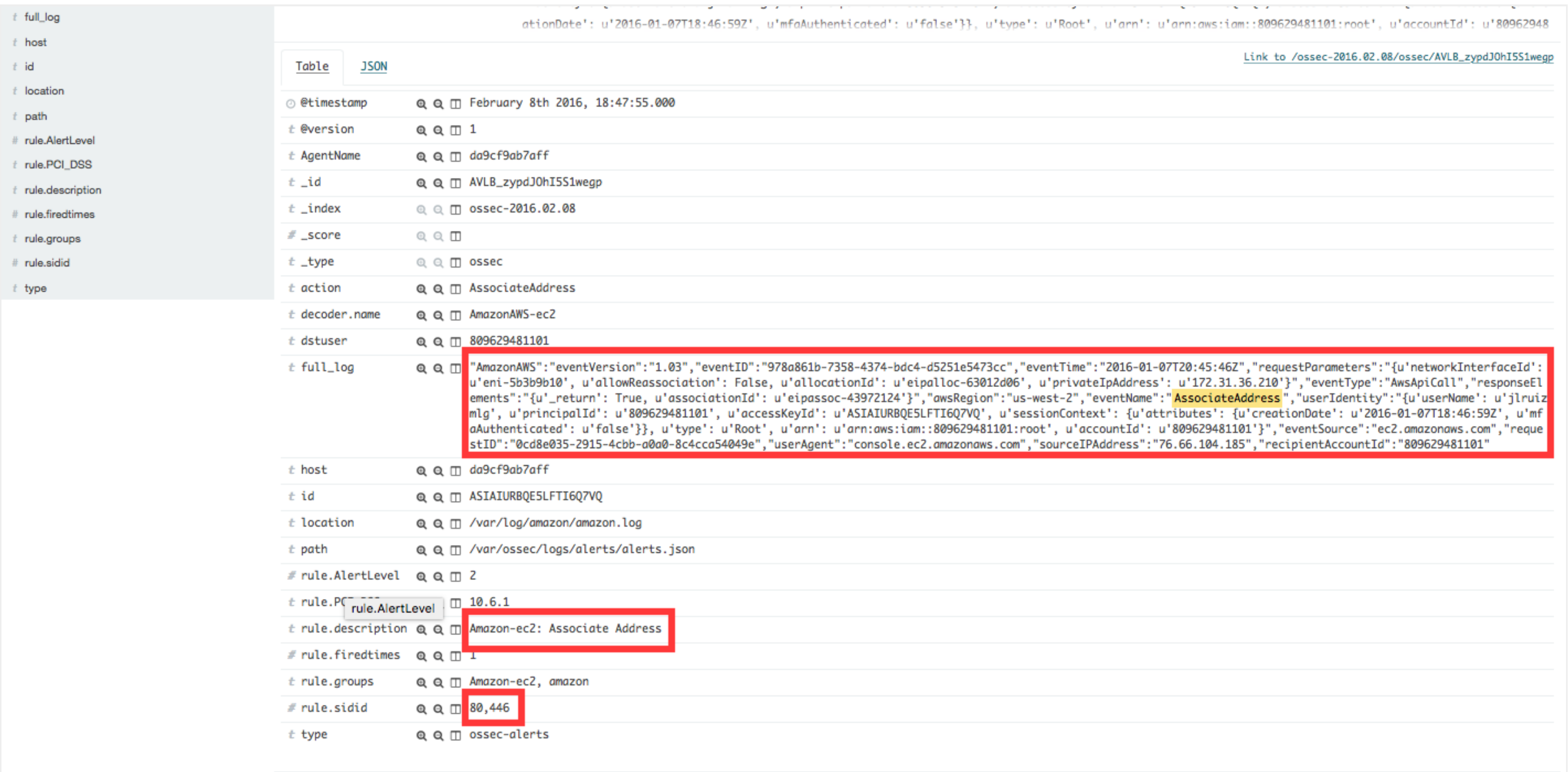
If an Elastic IP address is associated, then `rule 80446` will apply, generating the corresponding alert:

Definition of rule 80446

Copied to clipboard

```
<rule id="80446" level="2">
    <if_sid>80300</if_sid>
    <action>AssociateAddress</action>
    <description>Amazon-ec2: Associate Address</description>
    <group>amazon,pci_dss_10.6.1,</group>
</rule>
```

Kibana will show this alert



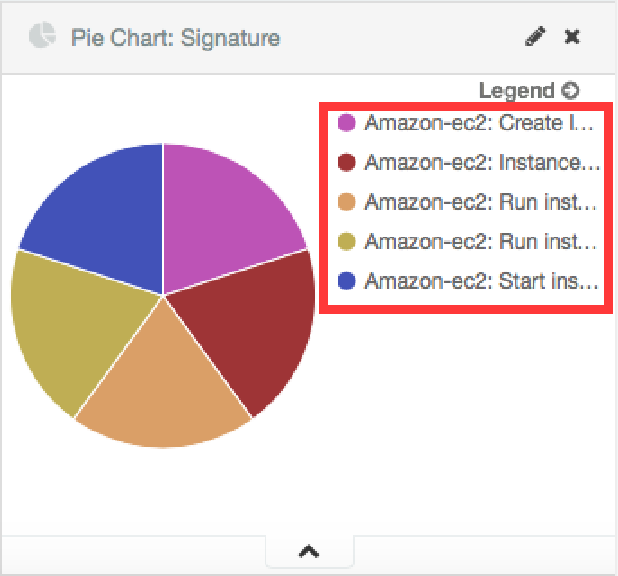
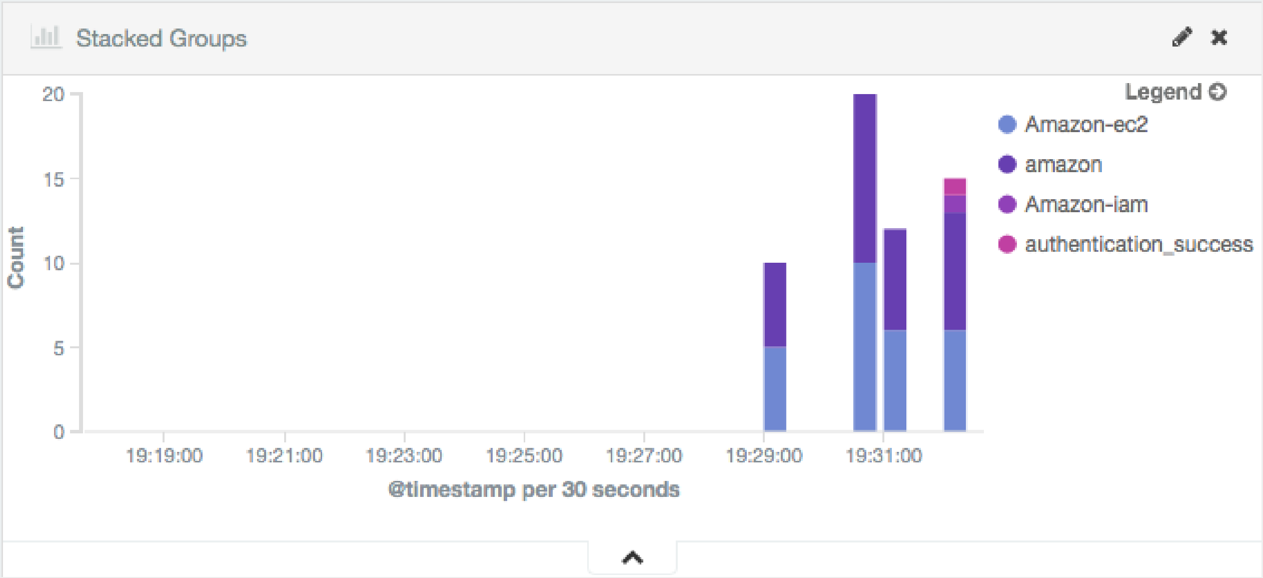
```
ationDate': u'2016-01-07T18:46:59Z', u'mfaAuthenticated': u'false'}}, u'type': u'Root', u'arn': u'arn:aws:iam::809629481101:root', u'accountId': u'80962948

Link to /ossec-2016.02.08/ossec/AVLB_zypdJOhI5S1wegp

@timestamp        February 8th 2016, 18:47:55.000
@version          1
AgentName         da9cf9ab7aff
_id               AVLB_zypdJOhI5S1wegp
_index            ossec-2016.02.08
_score
_type             ossec
action            AssociateAddress
decoder.name      AmazonAWS-ec2
dstuser           809629481101
full_log          "AmazonAWS":"eventVersion":"1.03","eventID":"978a861b-7358-4374-bdc4-d5251e5473cc","eventTime":"2016-01-07T20:45:46Z","requestParameters":"{u'networkInterfaceId':
                  u'eni-5b3b9b10', u'allowReassociation': False, u'allocationId': u'eipalloc-63012d06', u'privateIpAddress': u'172.31.36.210'}","eventType":"AwsApiCall","responseEl
                  ements":"{u'_return': True, u'associationId': u'eipassoc-43972124'}","awsRegion":"us-west-2","eventName":"AssociateAddress","userIdentity":"{u'userName': u'jlruiz
                  mlg', u'principalId': u'809629481101', u'accessKeyId': u'ASIAIURBQE5LFTI6Q7VQ', u'sessionContext': {u'attributes': {u'creationDate': u'2016-01-07T18:46:59Z', u'mf
                  aAuthenticated': u'false'}}, u'type': u'Root', u'arn': u'arn:aws:iam::809629481101:root', u'accountId': u'809629481101'}","eventSource":"ec2.amazonaws.com","reque
                  stID":"0cd8e035-2915-4cbb-a0a0-8c4cca54049e","userAgent":"console.ec2.amazonaws.com","sourceIPAddress":"76.66.104.185","recipientAccountId":"809629481101"
host              da9cf9ab7aff
id                ASIAIURBQE5LFTI6Q7VQ
location          /var/log/amazon/amazon.log
path              /var/ossec/logs/alerts/alerts.json
rule.AlertLevel   2
rule.PC           10.6.1
rule.description  Amazon-ec2: Associate Address
rule.firedtimes   1
rule.groups       Amazon-ec2, amazon
rule.sidid        80,446
type              ossec-alerts
```

The Kibana Dashboards will show:

Pie Chart	Stacked Groups

Pie Chart	Stacked Groups
	

Pie Chart: Signature
Legend
Amazon-ec2: Create I…
Amazon-ec2: Instance…
Amazon-ec2: Run inst…
Amazon-ec2: Run inst…
Amazon-ec2: Start ins…

Stacked Groups
20
15
10
5
0
Count
19:19:00
19:21:00
19:23:00
19:25:00
19:27:00
19:29:00
19:31:00
@timestamp per 30 seconds
Legend
Amazon-ec2
amazon
Amazon-iam
authentication_success