VPC Use cases

Using an Amazon VPC (Virtual Private Cloud), you can logically isolate your AWS assets from the rest of AWS. You can even set up your own virtual networking in the cloud. It is important to carefully monitor what happens with your VPC as it represent a critical part of your cloud infrastructure.

Create VPC

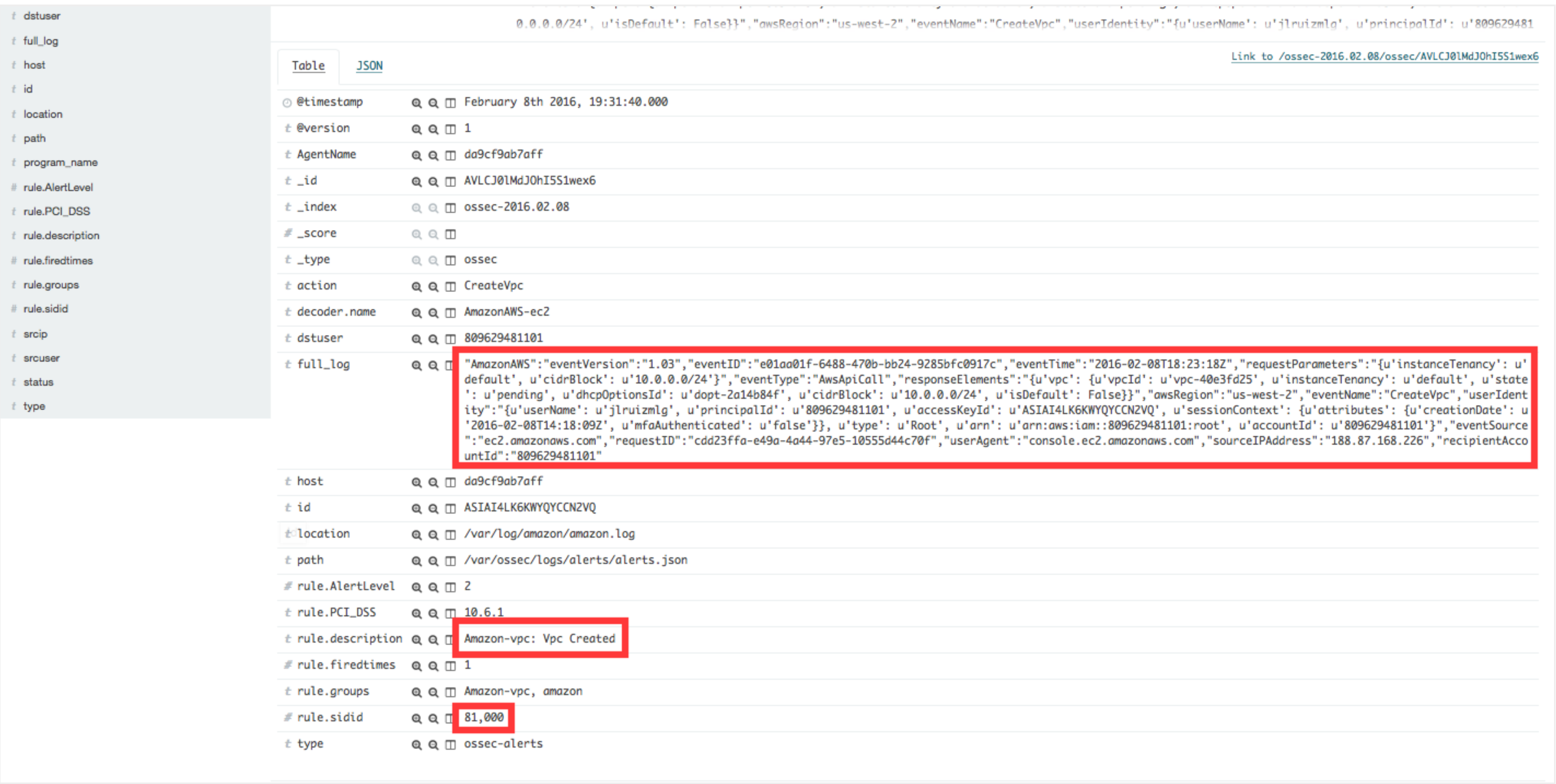
If a VPC is created, `rule 81000` will apply and an alert will be generated as shown below:

Definition of rule 81000

Copied to clipboard

```
<rule id="81000" level="2">
    <if_sid>80300</if_sid>
    <action>CreateVpc</action>
    <description>Amazon-vpc: Vpc Created</description>
    <group>amazon,pci_dss_10.6.1,</group>
</rule>
```

Kibana will show this alert



```
0.0.0.0/24', u'isDefault': False}}","awsRegion":"us-west-2","eventName":"CreateVpc","userIdentity":"{u'userName': u'jlruizmlg', u'principalId': u'809629481
```

Link to /ossec-2016.02.08/ossec/AVLCJ0lMdJOhI5S1wex6

```
@timestamp        February 8th 2016, 19:31:40.000
@version          1
AgentName         da9cf9ab7aff
_id               AVLCJ0lMdJOhI5S1wex6
_index            ossec-2016.02.08
_score
_type             ossec
action            CreateVpc
decoder.name      AmazonAWS-ec2
dstuser           809629481101
full_log          "AmazonAWS":"eventVersion":"1.03","eventID":"e01aa01f-6488-470b-bb24-9285bfc0917c","eventTime":"2016-02-08T18:23:18Z","requestParameters":"{u'instanceTenancy': u'
                  default', u'cidrBlock': u'10.0.0.0/24'}","eventType":"AwsApiCall","responseElements":"{u'vpc': {u'vpcId': u'vpc-40e3fd25', u'instanceTenancy': u'default', u'state
                  ': u'pending', u'dhcpOptionsId': u'dopt-2a14b84f', u'cidrBlock': u'10.0.0.0/24', u'isDefault': False}}","awsRegion":"us-west-2","eventName":"CreateVpc","userIdent
                  ity":"{u'userName': u'jlruizmlg', u'principalId': u'809629481101', u'accessKeyId': u'ASIAI4LK6KWYQYCCN2VQ', 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":"cdd23ffa-e49a-4a44-97e5-10555d44c70f","userAgent":"console.ec2.amazonaws.com","sourceIPAddress":"188.87.168.226","recipientAcco
                  untId":"809629481101"
host              da9cf9ab7aff
id                ASIAI4LK6KWYQYCCN2VQ
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-vpc: Vpc Created
rule.firedtimes   1
rule.groups       Amazon-vpc, amazon
rule.sidid        81,000
type              ossec-alerts
```

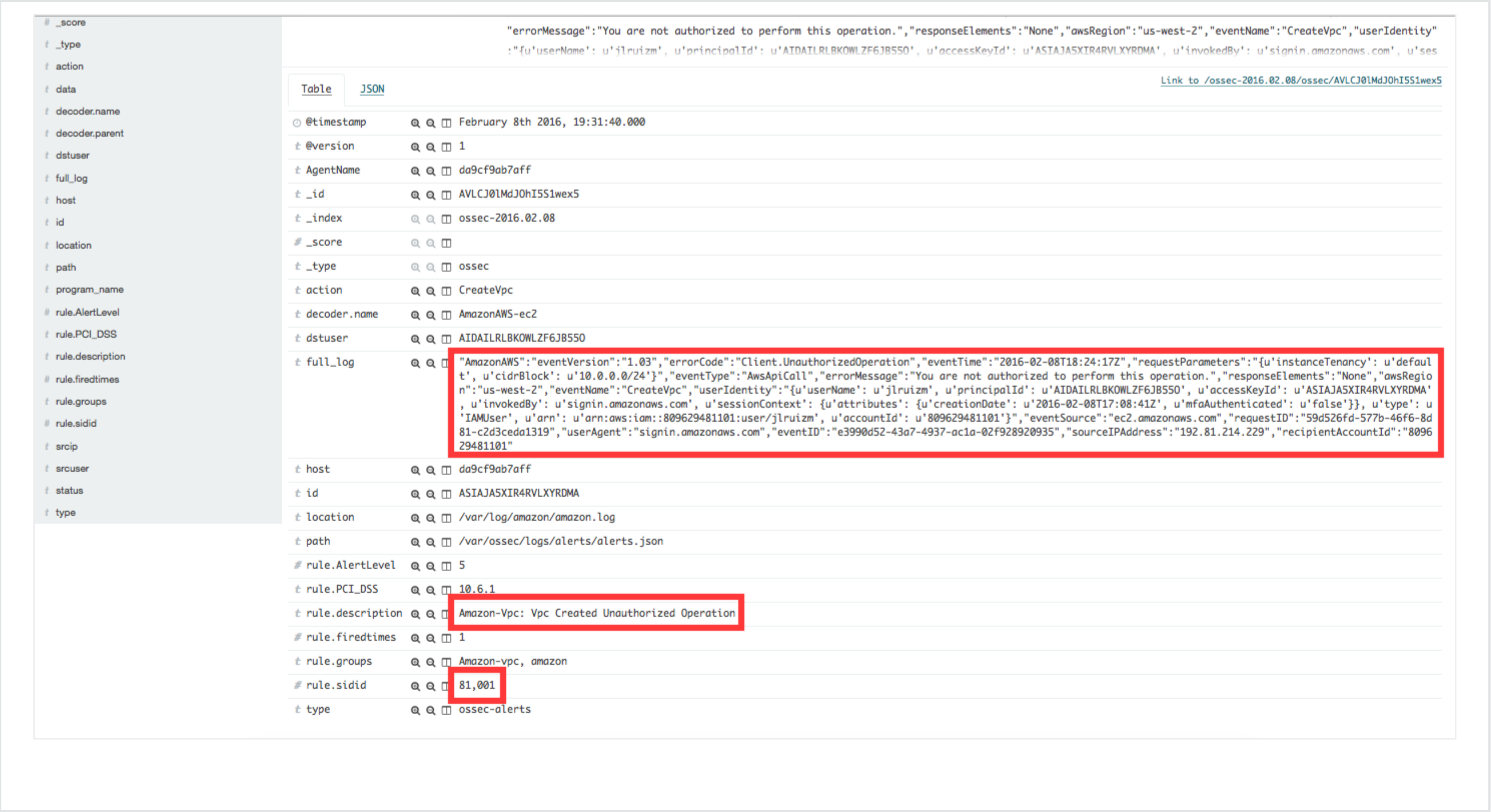
If a user without proper permissions attempts to create a VPC, `rule 81001` will apply:

Definition of rule 81001

Copied to clipboard

```
<rule id="81001" level="5">
    <if_sid>81000</if_sid>
    <match>"errorCode":"Client.UnauthorizedOperation"</match>
    <description>Amazon-Vpc: Vpc Created Unauthorized Operation</description>
    <group>amazon,pci_dss_10.6.1,</group>
</rule>
```

Kibana will show this alert



_score
_type
action
data
decoder.name
decoder.parent
dstuser
full_log
host
id
location
path
program_name
rule.AlertLevel
rule.PCI_DSS
rule.description
rule.firedtimes
rule.groups
rule.sidid
srcip
srcuser
status
type

```
"errorMessage":"You are not authorized to perform this operation.","responseElements":"None","awsRegion":"us-west-2","eventName":"CreateVpc","userIdentity"
:"{u'userName': u'jlruizm', u'principalId': u'AIDAILRLBKOWLZF6JB55O', u'accessKeyId': u'ASIAJA5XIR4RVLXYRDMA', u'invokedBy': u'signin.amazonaws.com', u'ses
```

Link to /ossec-2016.02.08/ossec/AVLCJ0lMdJOhI5S1wex5

@timestamp	February 8th 2016, 19:31:40.000
@version	1
AgentName	da9cf9ab7aff
_id	AVLCJ0lMdJOhI5S1wex5
_index	ossec-2016.02.08
_score	
_type	ossec
action	CreateVpc
decoder.name	AmazonAWS-ec2
dstuser	AIDAILRLBKOWLZF6JB55O
full_log	"AmazonAWS":"eventVersion":"1.03","errorCode":"Client.UnauthorizedOperation","eventTime":"2016-02-08T18:24:17Z","requestParameters":"{u'instanceTenancy': u'default', u'cidrBlock': u'10.0.0.0/24'}","eventType":"AwsApiCall","errorMessage":"You are not authorized to perform this operation.","responseElements":"None","awsRegion":"us-west-2","eventName":"CreateVpc","userIdentity":"{u'userName': u'jlruizm', u'principalId': u'AIDAILRLBKOWLZF6JB55O', u'accessKeyId': u'ASIAJA5XIR4RVLXYRDMA', 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":"59d526fd-577b-46f6-8d81-c2d3ceda1319","userAgent":"signin.amazonaws.com","eventID":"e3990d52-43a7-4937-ac1a-02f928920935","sourceIPAddress":"192.81.214.229","recipientAccountId":"809629481101"
host	da9cf9ab7aff
id	ASIAJA5XIR4RVLXYRDMA
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-Vpc: Vpc Created Unauthorized Operation
rule.firedtimes	1
rule.groups	Amazon-vpc, amazon
rule.sidid	81,001
type	ossec-alerts