IAM use cases

AWS Identity and Access Management (IAM) enables you to securely control your users' access to AWS services and resources. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

Following are some use cases for Wazuh rules built in for IAM events.

Create user account

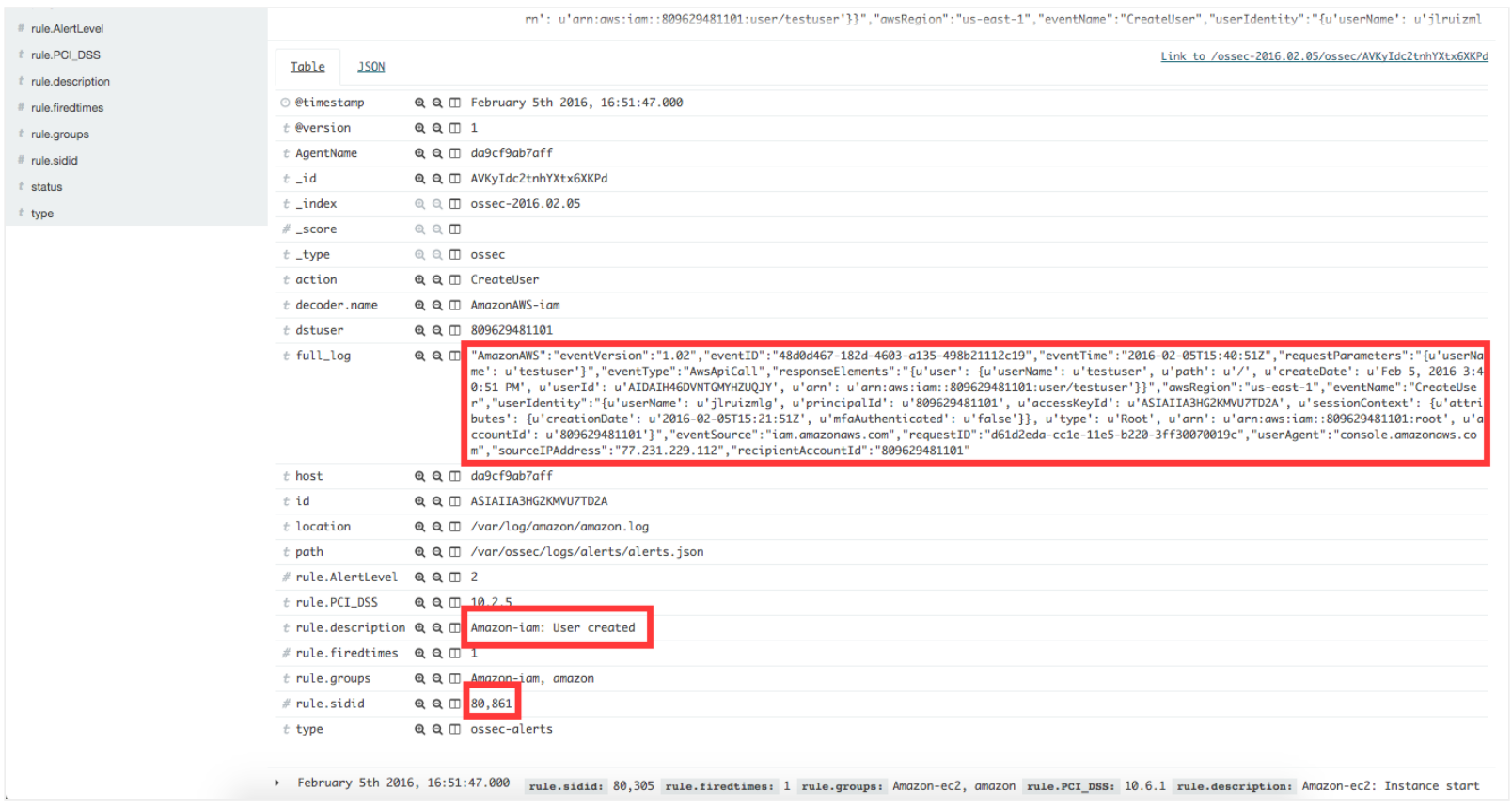
When we create a new user account in IAM, an AWS event is generated. As per the diagram at the beginning of this section, the log event flows to the Wazuh agent which passes it along to the Wazuh manager. The latter then analyzes the event and finds that it matches rule 80861. This results in an alert being generated, which can be seen in Kibana.

Definition of rule 80861

Copied to clipboard

```
<rule id="80861" level="2">
    <if_sid>80860</if_sid>
    <action>CreateUser</action>
    <description>Amazon-iam: User created</description>
    <group>amazon,pci_dss_10.2.5,</group>
</rule>
```

Kibana will show this alert



Create user account without permissions

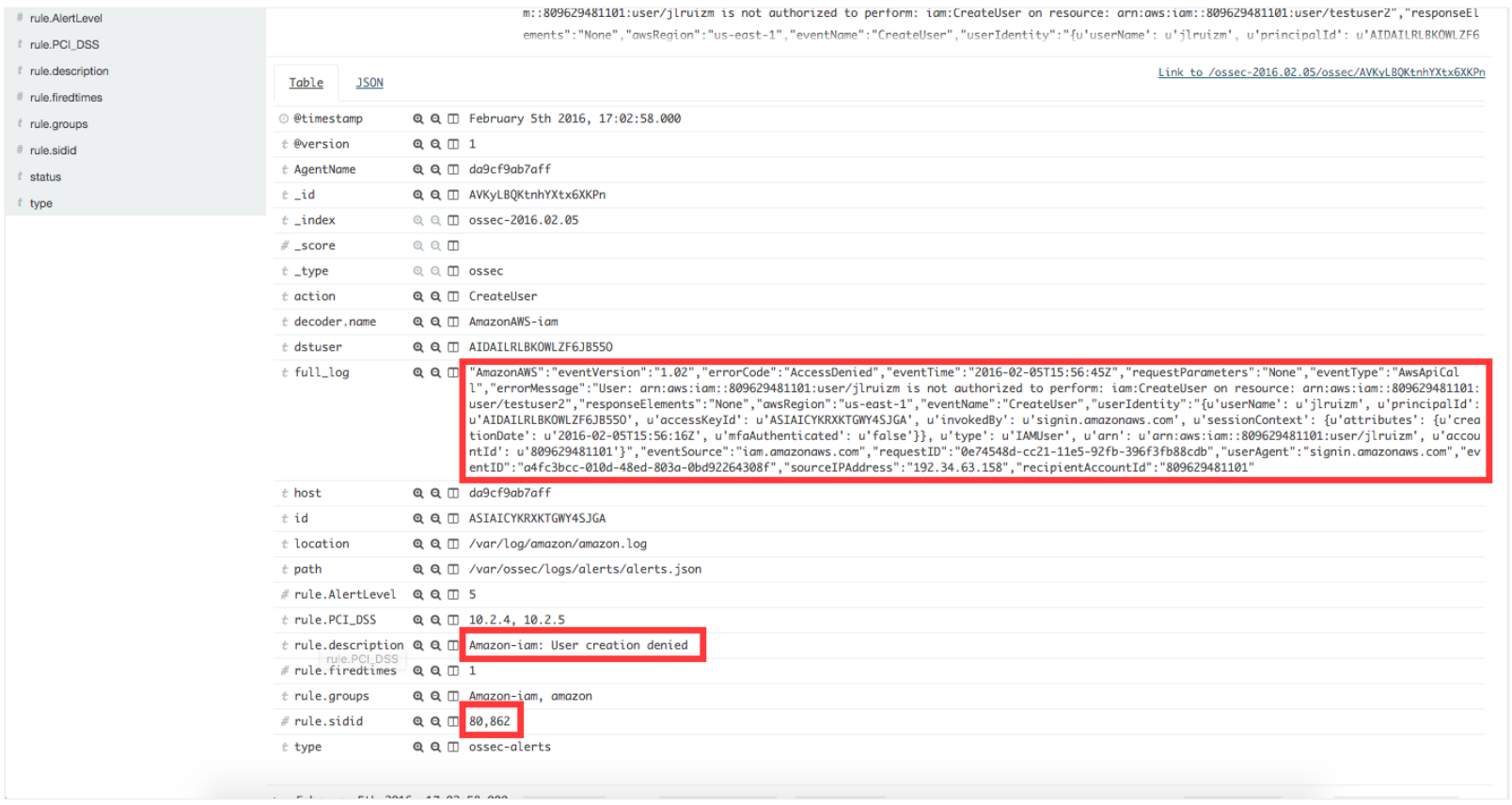
If a user without permission to create new users, attempts to create a new user, then the log message generated will match `rule 80862` and Kibana will show the alert as follows:

Definition of rule 80862

Copied to clipboard

```
<rule id="80862" level="2">
    <if_sid>80861</if_sid>
    <match>"errorCode":"AccessDenied"</match>
    <description>Amazon-iam: User creation denied</description>
    <group>amazon,pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>
```

Kibana will show this alert



User login failed

When a user tries to log in with an invalid password, a new event and log message will be generated. This log message will match `rule 80802`, generating an alert that will be shown in Kibana as follows:

Definition of rule 80802

Copied to clipboard

```
<rule id="80802" level="2">
    <if_sid>80801</if_sid>
    <match>'ConsoleLogin': u'Failure'</match>
    <description>Amazon-signin: User Login failed</description>
    <group>amazon,authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>
```

Kibana will show this alert

t location	@timestamp	February 4th 2016, 13:38:04.000
t path	t @version	1
# rule.AlertLevel	t AgentName	da9cf9ab7aff
t rule.PCI_DSS	t _id	AVKsSiB9NHDlXV6lWilY
t rule.description	t _index	ossec-2016.02.04
# rule.firedtimes	# _score	
t rule.groups	t _type	ossec
# rule.sidid	t action	ConsoleLogin
t type	t decoder.name	AmazonAWS-signin
	t decoder.parent	AmazonAWS-signin
	t dstuser	jlruizm
	t full_log	"AmazonAWS":"eventVersion":"1.02","eventID":"b922fe62-7002-49f9-be47-af4a31c4379c","eventTime":"2016-02-04T12:29:41Z","additionalEventData":"{u'MFAUsed': u'No', u'LoginTo': u'https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode=true', u'MobileVersion': u'No'}","requestParameters":"None","eventType":"AwsConsoleSignIn","errorMessage":"Failed authentication","responseElements":"{u'ConsoleLogin': u'Failure'}","awsRegion":"us-east-1","eventName":"ConsoleLogin","userIdentity":"{u'userName': u'jlruizm', u'accessKeyId': u'', u'type': u'IAMUser', u'principalId': u'AIDAILRLBKOWLZF6JB55O', u'accountId': u'809629481101'}","eventSource":"signin.amazonaws.com","userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/48.0.2564.97 Safari/537.36","sourceIPAddress":"192.34.60.87","recipientAccountId":"809629481101"
	t host	da9cf9ab7aff
	t location	/var/log/amazon/amazon.log
	t path	/var/ossec/logs/alerts/alerts.json
	# rule.AlertLevel	5
	t rule.PCI_DSS	10.2.4, 10.2.5
	t rule.description	Amazon-signin: User Login failed
	# rule.firedtimes	6
	t rule.groups	Amazon-iam, amazon, authentication_failed
	# rule.sidid	80,802
	t type	ossec-alerts

Possible break-in attempt

When more than 4 authentication failures occur in a **360** second time window, this fires `rule 80803` and generates an alert.

Definition of rule 80803

Copied to clipboard

```
<rule id="80803" level="10" frequency="4" timeframe="360">
    <if_matched_sid>80802</if_matched_sid>
    <description>Possible breakin attempt (high number of login attempts).</description>
    <group>amazon,authentication_failures,pci_dss_11.4,pci_dss_10.2.4,pci_dss_10.2.5,</group>
</rule>
```

Kibana will show this alert

Login success

After a successful login, the `rule 80801` will match the log message generated by this event and a new alert will be shown in Kibana:

Definition of rule 80801

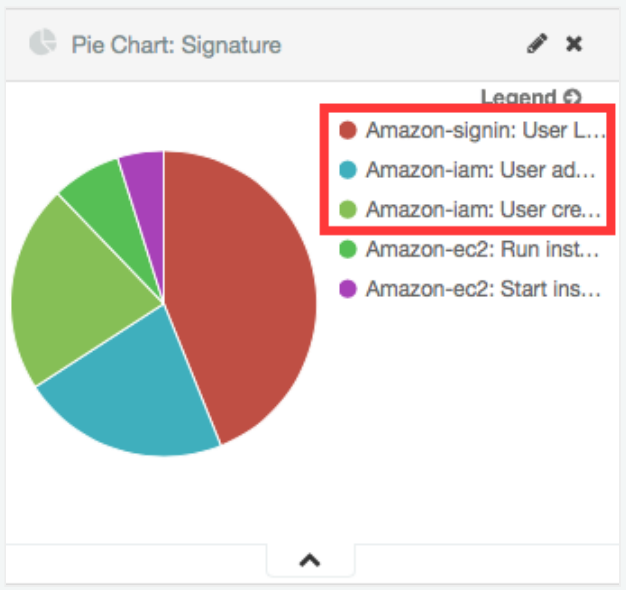
Copied to clipboard

```
<rule id="80801" level="2">
    <if_sid>80800</if_sid>
    <action>ConsoleLogin</action>
    <description>Amazon-signin: User Login Success</description>
    <group>amazon,authentication_success,pci_dss_10.2.5,</group>
</rule>
```

Kibana will show this alert

The Kibana Dashboards will show:

Pie Chart



Stacked Groups