

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

rule.AlertLevel

rule.PCI_DSS

rule.description

rule.firedtimes

rule.groups

rule.sidid

status

type

m::809629481101:user/jlruizm is not authorized to perform: iam:CreateUser on resource: arn:aws:iam::809629481101:user/testuser2","responseElements": "None", "awsRegion": "us-east-1", "eventName": "CreateUser", "userIdentity": "{u'userName': u'jlruizm', u'principalId': u'AIDAILRLBKOWLZF6

TableJSON

February 5th 2016, 17:02:58.000

1

da9cf9ab7aff

AVKyLBQKtnhYXtx6XKPn

ossec-2016.02.05

ossec

CreateUser

AmazonAWS-iam

AIDAILRLBKOWLZF6J8550

"AmazonAWS":{"eventVersion":"1.02","errorCode":"AccessDenied","eventTime":"2016-02-05T15:56:45Z","requestParameters":{"None"},"eventType":"AwsApiCall","errorMessage":{"User: arn:aws:iam::809629481101:user/jlruizm is not authorized to perform: iam:CreateUser on resource: arn:aws:iam::809629481101:user/testuser2","responseElements": "None", "awsRegion": "us-east-1", "eventName": "CreateUser", "userIdentity": "{u'userName': u'jlruizm', u'principalId': u'AIDAILRLBKOWLZF6J8550', u'accessKeyId': u'ASIAICYKRXKTGWY4S3GA', u'invokedBy': u'signin.amazonaws.com', u'sessionContext': {u'attributes': {u'creationDate': u'2016-02-05T15:56:16Z', u'mfaAuthenticated': u'false'}}}, u'type': u'IAMUser', u'arn': u'arn:aws:iam::809629481101:user/jlruizm', u'accountId': u'809629481101"},"eventSource": "iam.amazonaws.com", "requestID": "0e74548d-cc21-11e5-92fb-396f3fb88cdb", "userAgent": "signin.amazonaws.com", "eventID": "a4fc3bcc-010d-48ed-803a-0bd92264308f", "sourceIPAddress": "192.34.63.158", "recipientAccountId": "809629481101"

da9cf9ab7aff

ASIAICYKRXKTGWY4S3GA

/var/log/amazon/amazon.log

/var/ossec/logs/alerts/alerts.json

5

10.2.4, 10.2.5

Amazon-iam: User creation denied

1

Amazon-iam, amazon

80,862

ossec-alerts

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

location	@timestamp	February 4th 2016, 13:38:04.000
path	@version	1
rule.AlertLevel	AgentName	da9cf9ab7aff
rule.PCI_DSS	_id	AVKsSiB9NHd1XV6lWlly
rule.description	_index	ossec-2016.02.04
rule.firedtimes	_score	
rule.frequency	_type	ossec
rule.groups	action	ConsoleLogin
rule.sidid	decoder.name	AmazonAWS-signin
type	decoder.parent	AmazonAWS-signin
	dstuser	jlruiзм
	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'jlruiзм', u'accessKeyId': u'', u'type': u'IAMUser', u'principalId': u'AIDAILRLBKOWLZF6JB550', 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"}
	host	da9cf9ab7aff
	location	/var/log/amazon/amazon.log
	path	/var/ossec/logs/alerts/alerts.json
	rule.AlertLevel	5
	rule.PCI_DSS	10.2.4, 10.2.5
	rule.description	Amazon-signin: User Login failed
	rule.firedtimes	6
	rule.groups	Amazon-iam, amazon, authentication_failed
	rule.sidid	80,802
	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

path	@version	1
rule.AlertLevel	AgentName	da9cf9ab7aff
Quick Count (1 / 1 records)	_id	AVKsSiB9NHd1XV6lWild
10	_index	ossec-2016.02.04
Visualize	_score	
rule.PCI_DSS	_type	ossec
rule.description	action	ConsoleLogin
rule.firedtimes	decoder.name	AmazonAWS-signin
rule.frequency	decoder.parent	AmazonAWS-signin
rule.groups	dstuser	jlruiзм
rule.sidid	full_log	"AmazonAWS":{"eventVersion":"1.02","eventID":"df9de854-9835-4939-d9c7-204707e4c8cf","eventTime":"2016-02-04T12:31:57Z","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'jlruiзм', u'accessKeyId': u'', u'type': u'IAMUser', u'principalId': u'AIDAILRLBKOWLZF6JB550', 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"}
type	host	da9cf9ab7aff
	location	/var/log/amazon/amazon.log
	path	/var/ossec/logs/alerts/alerts.json
	rule.AlertLevel	10
	rule.PCI_DSS	11.4, 10.2.4, 10.2.5
	rule.description	Possible breakin attempt (high number of login attempts).
	rule.firedtimes	1
	rule.frequency	4
	rule.groups	Amazon-iam, amazon, authentication_failures
	rule.sidid	80,803
	type	ossec-alerts

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

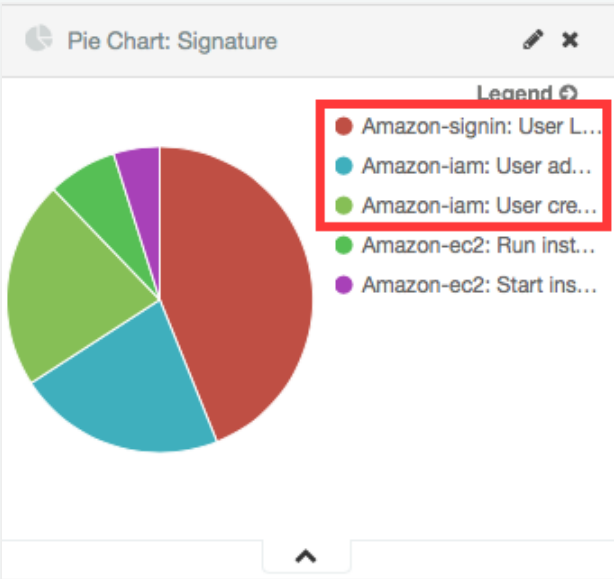
```
<rule id="80801" level="2">
  <if_sid>80800</if_sid>
  <action>ConsoleLogin</action>
  <description>Amazon-signin: User Login Success</description>
  <group>amazon,authentication_success,pci_dss_10.2.5,</group>
</rule>
```

Kibana will show this alert

@timestamp	February 4th 2016, 13:48:32.000
@version	1
AgentName	da9cf9ab7aff
_id	AVKsU7gVNHDLXV6lW1l
_index	ossec-2016.02.04
_score	
_type	ossec
action	ConsoleLogin
decoder.name	AmazonAWS-signin
decoder.parent	AmazonAWS-signin
dstuser	jlruizm
full_log	<div> <div> "AmazonAWS":{"eventVersion":"1.02","eventID":"a2c63121-5afb-43bf-b8ef-04856b48438c","eventTime":"2016-02-04T12:41:52Z","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","responseElements":{"u'ConsoleLogin': u'Success'}}","awsRegion":"us-east-1","eventName":"ConsoleLogin","userIdentity":{"u'userName': u'jlruizm', u'type': u'IAMUser', u'arn': u'arn:aws:iam:809629481101:user/jlruizm', u'principalId': u'AIDAILRLBKOWLZF6J8550', 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"</div> </div>
host	da9cf9ab7aff
location	/var/log/amazon/amazon.log
path	/var/ossec/logs/alerts/alerts.json
rule.AlertLevel	2
rule.PCI_DSS	10.2.5
rule.description	Amazon-signin: User Login Success
rule.firedtimes	1
rule.groups	Amazon-iam, amazon, authentication_success
rule.sidid	80,801
type	ossec-alerts

The Kibana Dashboards will show:

Pie Chart



Stacked Groups

