Qualys TotalCloud v2.x

API Release Notes

Version 2.8

February 12, 2024

What's New?

Added New Parameter in Alerting Response Rules APIs

Qualys API Server URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys Platform and get the API URL

In some of the API Release Notes, the API gateway URL for Qualys US Platform 1 (https://gateway.qg1.apps.qualys.com) is used in sample API requests.

For this API Release Notes, instead of providing any platform-specific URL, <qualys_base_url> is mentioned in the sample API requests. If you are on another platform, replace this URL with the appropriate gateway URL for your account.

Added New Parameter in Alerting Response Rules APIs

APIs affected	/rest/v1/rules /rest/v1/rules/{ruleId}
Method	Post, Put, Get
New or Updated APIs	Updated

With this release, we have added the ruleSeverity field in input and response of the following Alerting Response Rules APIs. Now, you can get a list of all alerting rules based on the rule severity. Also, you can create or update alerting rules with specific severity.

- Create Rules API
- Update Rules API
- Get Rules API
- Get Rules by ID API

Input Parameter

Parameter	Mandatory /Optional	Data Type	Description
ruleSeverity	Optional	String	Specify the rule severity as LOW, MEDIUM, HIGH, or NONE

Refer to the TotalCloud API user guide for details on all available input parameters of Response Rules API.

Create Rules API

Create a rule and define the criteria for generating alerts based on the actions specified.

Sample for Create Rule API

API Request:

```
curl --location --request PUT
"<qualys_base_url>//cloudview-
api/rest/v1/rules?cloudType=AWS&ruleType=simple_alert%20'
\
--header 'Content-Type: application/json' \
--header 'Authorization: Basic xxxxxxxxxxxxxxxxxxxxxxxxxxxx' \
"--data""{
    \"actionRequests\": [
        {
```

```
            \"actionId\": \"10bae250-xxxx-xxxx-xxxx-d35faca48182\",
          \"actionType\": \"qemail\"
          }
      ],
      \"aggregate\": \"true\",
      \"aggregationKey\": \"account.id\",
      \"description\": \"Public API Rule 22663\",
      \"durationHour\": 0,
      \"fromHourInUTC\": 0,
      \"fromMinuteInUTC\": 0,
      \"ruleSeverity\":\"MEDIUM\",
      \"name\": \"AWS_simple_aws_Email123\",
      \"qql\": \"cid:1 and control.result:FAIL\"
}"\" ]}"
```

Response:

```
{"success":"52a21c50-xxxx-xxxx-xxxx-d35faca48182"}
```

Update Rules API

Update a rule and define the criteria for generating alerts based on the actions specified.

Sample for Update Rule API

API Request:

```
curl --location --request PUT
"<qualys_base_url>ccloudview-api/rest/v1/rules/52a21c50-xxxx-xxxx-
xxxx-d35faca48182?ruleType=simple_alert' \
-H 'userUuid: 50db60ff-xxxx-xxxx-xxxx-8f29c5a46f12' \
-H 'username: qates_vr8' \
-H 'customerUuid: 10f9d6dd-xxxx-xxxx-xxxx-06a0b92cf87' \
-H 'Content-Type: application/json' \
-H 'Authorization: Basic xxxxxxxxxxxxxxxxxxxxxxxxxxxx' \
--data-raw '{
    "actionRequests": [
        {
            "actionType": "qemail",
            "alert": null,
            "externalActionId": null,
            "externalActionName": null,
            "externalActionType": null,
            "emailRecipients": [
                "john_doe@qualys.com"
            ],
            "actionId": "10bae250-xxxx-xxxx-xxxx-d35faca48182",
        "slackChannel": null,
            "subject": null,
```

```
            "name": null
        }
    ],
    "aggregate": true,
    "aggregationKeys": [
        "account.id"
    ],
    "ruleSeverity": "MEDIUM",
    "matchCount": 3,
    "name": "Test",
    "baseQuery": "",
    "ruleType": "simple_alert",
    "slideTime": 900000,
    "datasource": "AWS-MONITOR",
    "qql": "cid:1 and control.result:FAIL"
}'
```

Response:

```
{"success":"52a21c50-xxxx-xxxx-xxxx-d35faca48182"}
```

Get Rules API

Get the list of rules.

Sample for Get Rules API

API Request:

```
curl --location --request GET
"<qualys_base_url>c/cloudview-
api/rest/v1/rules?cloudType=AWS&pageNo=0&pageSize=10&ruleType=simple_aler
t&filter=ruleSeverity%3AMEDIUM'\
--header 'Accept: application/json' \
--header 'Authorization: Basic xxxxxxxxxxxxxxxxxxxxxxxxxxxx'
```

Response:

```
[
    {
        "id": "c90aa5a0-xxxx-xxxx-xxxx-13e0590c31e",
   "cloudType": "AWS",
        "ruleType": "simple_alert",
        "name": "MEDIUM Rule",
        "description": "Rule",
        "qql": "control.result:FAIL ",
        "aggregate": true,
```

```
    "aggregationKey": "account.id",
    "actions": [
        {
            "id": "10bae250-xxxx-xxxx-xxxx-35faca48182",
            "actionType": "qemail",
            "name": "AWS Email Action",
            "subject": "Test",
            "alert": "Test",
            "emailRecipients": [
                "john_doe@qualys.com"
            ],
            "slackChannel": null,
            "subjectParameters": [],
            "bodyParameters": []
        }
    ],
    "created": "2023-12-26T09:18:52.154+00:00",
    "createdBy": "John Doe",
    "createdById": "john_doe@qualys.com",
    "updated": "2023-12-26T09:18:52.154+00:00",
    "updatedBy": "John Doe",
    "updatedById": "john_doe@qualys.com",
    "lastRun": "1970-01-01T00:00:00.000+00:00",
    "ruleState": "ENABLED",
    "ruleSeverity": "MEDIUM",
    "durationHour": 0,
    "fromHourInUTC": 0,
    "fromMinuteInUTC": 0
},
{
    "id": "27e07b70-xxxx-xxxx-xxxx-cf1b3d21632d",
    "cloudType": "AWS",
    "ruleType": "simple_alert",
    "name": "Test",
    "description": "Test",
    "qql": "cid:45 and control.result:FAIL ",
    "aggregate": true,
    "aggregationKey": "account.id",
    "actions": [
        {
            "id": "10bae250-xxxx-xxxx-xxxx-d35faca48182",
            "actionType": "qemail",
            "name": "AWS Email Action",
            "subject": "Test",
            "alert": "Test",
            "emailRecipients": [
                "john_doe@qualys.com"
            ],
            "slackChannel": null,
```

```
                "subjectParameters": [],
                "bodyParameters": []
            }
        ],
        "created": "2023-12-22T10:09:12.876+00:00",
        "createdBy": "John Doe",
        "createdById": "john_doe@qualys.com",
        "updated": "2023-12-26T09:19:53.791+00:00",
        "updatedBy": "John Doe",
        "updatedById": "john_doe@qualys.com",
        "lastRun": "1970-01-01T00:00:00.000+00:00",
        "ruleState": "ENABLED",
        "ruleSeverity": "MEDIUM",
        "durationHour": 0,
        "fromHourInUTC": 0,
        "fromMinuteInUTC": 0
    }
]
```


Get Rules by ID API

Specify the rule ID and fetch rule details.

Sample for Get Rules by ID API

API Request:

```
curl --location --request GET
"<qualys_base_url>/cloudview-api/rest/v1/rules/311eb430-xxxx-xxxx-
xxxx-d35faca48182'\
--header 'Accept: application/json' \
--header 'Authorization: Basic xxxxxxxxxxxxxxxxxxxxxxxxxxxx'
```

Response:


```
{
    "id": "311eb430-xxxx-xxxx-xxxx-d35faca48182",
   "cloudType": "AWS",
    "ruleType": "simple_alert",
    "name": "AWS_simple_aws_Email",
    "description": "Public API Rule 22663",
    "qql": "cid:1 and control.result:FAIL",
    "aggregate": false,
    "actions": [
        {
            "id": "10bae250-xxxx-xxxx-xxxx-d35faca48182",
           "actionType": "qemail",
            "name": "AWS Email Action",
```

```
        "subject": "Test",
        "alert": "Test",
        "emailRecipients": [
            "john_doe@qualys.com"
        ],
        "slackChannel": null,
        "subjectParameters": [],
        "bodyParameters": []
    }
],
"created": "2023-12-22T10:16:37.875+00:00",
"createdBy": "John Doe",
"createdById": "john_doe@qualys.com",
"updated": "2023-12-22T10:16:37.875+00:00",
"updatedBy": "John Doe",
"updatedById": "john_doe@qualys.com",
"ruleState": "ENABLED",
"ruleSeverity": "NONE",
"durationHour": 0,
"fromHourInUTC": 0,
"fromMinuteInUTC": 0 }
```