Qualys Container Security

API Release Notes

Version 1.26

June 26, 2023

Qualys Cloud Suite API gives you many ways to integrate your programs and API calls with Qualys capabilities. You'll find all the details in our user guides, available at the time of release. Just log in to your Qualys account and go to Help > Resources.

What's New

Detecting Container Secrets

Container Security Policy Management

Showing EC2 Instance ID in Container and Sensor Details

Capturing Namespace Labels and Annotations in Kubernetes Metadata

Qualys API 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

Detecting Container Secrets

Container secrets are digital credentials providing identity authentication and authorizing access to privileged accounts, applications, and services. They can include passwords, API keys, and other credentials that are needed for applications to function properly.

If these secrets are not properly secured, they can be accessed by unauthorized users, leading to malicious attacks. Therefore, discovering container secrets is one of the important aspects of container security that organizations must prioritize to protect their sensitive data, meet compliance requirements, and reduce the risk of security incidents.

With this release, we have introduced the following new APIs for container secrets detection:

List Secret Detectors

Show Details of a Secret Detector

Show Detected Secrets of an Image

List Secret Detectors

API affected	/csapi/v1.3//secretDetector
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Shows a list of secret detectors in your account.

Input Parameter

Parameter	Mandatory?	Data Type	Description
filter	Optional	string	Filter the secret detectors by providing a QQL search query.

Sample 1: Fetch a List of Secret Detectors

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/secretDetector'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>
```

Response:


```
{
    "data": [
        {
            "ruleUuid": "ff34aaee-e4c2-11ed-b5ea-0242ac120002",
            "created": "1682576371399",
            "updated": "1682576371399",
            "type": "system",
            "category": "PublicKey",
            "severity": "HIGH",
            "secretDetector": "SSH public key DSA",
            "status": "Active"
        },
        {
            "ruleUuid": "9559ac14-e4c2-11ed-b5ea-0242ac120002",
            "created": "1682576371290",
            "updated": "1682576371290",
            "type": "system",
            "category": "PublicKey",
```

```
    "severity": "HIGH",
    "secretDetector": "SSH public key RSA",
    "status": "Active"
},
{
    "ruleUuid": "02e9a634-c96c-11ed-afa1-0242ac120002",
    "created": "1681987259554",
    "updated": "1681987259554",
    "type": "system",
    "category": "Typeform",
    "severity": "LOW",
    "secretDetector": "Typeform API Token",
    "status": "Active"
},
{
    "ruleUuid": "dddeeb1a-c96b-11ed-afa1-0242ac120002",
    "created": "1681987259520",
    "updated": "1681987259520",
    "type": "system",
    "category": "Twitch",
    "severity": "LOW",
    "secretDetector": "Twitch API Token",
    "status": "Active"
},
{
    "ruleUuid": "d68b44e4-c96b-11ed-afa1-0242ac120002",
    "created": "1681987259478",
    "updated": "1681987259478",
    "type": "system",
    "category": "LinkedIn",
    "severity": "LOW",
    "secretDetector": "LinkedIn Client Id",
    "status": "Active"
},
{
    "ruleUuid": "abea5478-c96b-11ed-afa1-0242ac120002",
    "created": "1681987259448",
    "updated": "1681987259448",
    "type": "system",
    "category": "LinkedIn",
    "severity": "LOW",
    "secretDetector": "LinkedIn Client Secret",
    "status": "Active"
},
{
    "ruleUuid": "920f95cc-c96b-11ed-afa1-0242ac120002",
    "created": "1681987259408",
    "updated": "1681987259408",
    "type": "system",
```

```
            "category": "Shippo",
            "severity": "LOW",
            "secretDetector": "Shippo API Token",
            "status": "Active"
        },
        {
            "ruleUuid": "7b2123f8-c96b-11ed-afa1-0242ac120002",
            "created": "1681987259372",
            "updated": "1681987259372",
            "type": "system",
            "category": "Sendinblue",
            "severity": "LOW",
            "secretDetector": "Sendinblue API Token",
            "status": "Active"
        }

        ...
    ],
    "count": 85,
    "groups": {}
}
```

Show Details of a Secret Detector

API affected	csapi/v1.3/secretDetector/
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Shows details of a secret detector.

Input Parameter

Parameter	Mandatory?	Data Type	Description
secretDetectorId	Mandatory	string	Provide the ID/UUID of the secret detector of which you want to fetch details.

Sample: Fetch Details of a Secret Detector

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/secretDetector/02e9a634-c96c-11ed-afa1-
0242ac120002'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>
```

Response:

```
{
    "ruleUuid": "02e9a634-c96c-11ed-afa1-0242ac120002",
    "type": "system",
    "category": "Typeform",
    "severity": "LOW",
    "secretDetector": "Typeform API Token",
    "status": "Active",
    "regex": "(?i)(?P<key>typeform[a-z0-9_ .\\-
,]{0,25})(=|>|:=|\\|\\|:|<=|=>|:).{0,5}(?P<secret>tfp_[a-z0-9\\-
_\\.=]{59})",
    "created": "1681987259554",
    "updated": "1681987259554",
    "createdBy": "System",
    "updatedBy": "System"
}
```

Show Detected Secrets of an Image

API affected	csapi/v1.3/images/{imageSha}/secrets
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Shows a list of detected secrets for an image.

Input Parameter

Parameter	Mandatory?	Data Type	Description
imageSha	Mandatory	string	Specify the SHA value of an image.

Sample: Fetch a List of detected secrets for an image

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/images/561f23db5e2d22838992ab8a5d3a52ee1097
085735290a9fd3c41ac7ff639983/secrets'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:


```
{
    "data": [
        {
            "secretType": "Asymmetric Private Key",
            "category": "AsymmetricPrivateKey",
            "severity": "HIGH",
            "ruleUuid": "d68b44e4-c96b-11ed-afa1-0242ac120002",
            "lastUpdated": "1615188407216",
            "matches": [
                {
                    "startLine": 5,
                    "endLine": 10,
                    "match": "BEGIN RSA PRIVATE KE"
                }
            ],
            "layerSha":
"sha2563d762ca8378d40f3029bb10de71ec98652580cb8859248250d812bede6998505",
            "filePath": "root/jignal.pem"
```

```
        },
        {
            "secretType": "Shopify Token",
            "category": "shopify",
            "severity": "HIGH",
            "ruleUuid": "d68b44e4-c96b-11ed-afa1-0242ac120002",
            "lastUpdated": "1615188407216",
            "matches": [
                {
                    "startLine": 10,
                    "endLine": 15,
                    "match": "BEGIN RSA PRIVATE KE"
                }
            ],
            "layerSha":
"sha2563d762ca8378d40f3029bb10de71ec98652580cb8859248250d812bede6998505",
            "filePath": "root/jignal.pem"
        }
    ],
    "count": 2,
    "groups": {}
}
```

Container Security Policy Management

With this release, we have introduced policies in Container Security for managing configurations, vulnerability management, compliance, access, and auditing in containerized environment, and thus automating the process of securing images and containers. Policies provide a combination of rules that assess specific artifacts such as images, and containers, and provide actions associated with the rules.

We have introduced the following new APIs for Container Security policy management:

List Policies

Create a New Policy

Show Details of a Policy

Delete a Policy

Update a Policy

Activate or Deactivate a Policy

List Policies

API affected	csapi/v1.3/centralizedPolicy
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Retrieves a list of policies from your account.

Input Parameters

Parameter	Mandatory?	Data Type	Description
filter	Optional	string	Filter the policies by providing a QQL search query.
pageNumber	Optional	integer	Specify the page to be returned.
pageSize	Optional	integer	Specify the number of records to display per page.
sort	Optional	string	Specify how to sort the records in the response. The supported values are: - policyName:desc/asc - created:desc/asc - updated:desc/asc - policyMode:desc/asc Where, "asc" and "desc" mean ascending and descending, respectively.

Sample: List All Policies from Your Account

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/centralizedPolicy?pageNumber=1&pageSize=50&
sort=created%3Adesc'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:

```
{
  "data": [
    {
```

```
      "uuid": "098777a1-4b76-4df5-9868-50ca570c548a",
      "policyName": "Test-011",
      "description": "test",
      "policyMode": "ACTIVE",
      "createdBy": "quays_ab6",
      "created": "1683261602526",
      "updatedBy": "quays_ab6",
      "updated": "1683261629891",
      "assetType": "CICD",
      "isDefault": false,
      "tagIds": null
    }
  ],
  "count": 1,
  "groups": {}
}
```

Create or Update a Policy

API affected	csapi/v1.3/centralizedPolicy
Operator	POST, PUT
New or Updated APIs	New
DTD or XSD Changes	NA

Creates a new policy or updates an existing policy.

Input Parameters

Parameter	Mandatory?	Data Type	Description
policyName	Mandatory	string	Enter a policy name up to 150 characters.
description	Mandatory	string	Enter a description for the policy up to 250 characters.
policyType	Mandatory	string	Specify the policy type. Currently, the only available value is: IMAGESCAN
policyMode	Mandatory	string	Specify the policy mode as active to enforce the policy or inactive to keep the policy deactivated.
assetType	Mandatory	string	Specify the asset type. Currently, only "CICD" is supported.
isDefault	Mandatory	string	Specify whether to make it a default policy. The valid values are: true or false.

tagIds	Mandatory	string	Specify the UUIDs of tags to associate them with the policy.
centralizedPolicy Rules	At least one active rule is mandatory	-	Provide rules as part of the policy evaluation. `[ { "name": "Rule123", "type": "IMAGESCAN_VULN_SEVERITYCOUNT", "action": "DENY", "isEnabled": true, "stopProcessing": false, "sortOrder": 0, "metaData": {"operator":"GREATER_THAN","severityLevel":1,"threshold":1} } ]` This rule reads: If the count of vulnerabilities with severity level 1 is greater than 1, deny/fail the CICD build. Where, - **name**: Specify the name of the rule. - **type**: Specify the type of the rule. Currently, you can create rules related to only the count of vulnerabilities of specific severity and the valid value is: "IMAGESCAN_VULN_SEVERITYCOUNT". - **action**: Specify ALLOW or DENY to pass or fail the CICD pipeline build. - **isEnabled**: Specify whether enforce the rule or keep it deactivated. The valid values are: true or false. - **operator**: Specify the operator of the equation. The valid values are GREATER_THAN and GREATER_THAN_EQUAL_TO. - **threshold**: Specify the maximum number of vulnerabilities allowed. - **severityLevel**: Specify the severity level of vulnerabilities.

Sample: Create a New Policy

API Request:

```
curl -X 'POST'
'<qualys_base_url>/csapi/v1.3/centralizedPolicy'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
-H 'Content-Type: application/json'
```

Request Body:

```
{
  "policyName": "Policy1214",
  "policyType": "IMAGESCAN",
  "policyMode": "ACTIVE",
  "description": "Policy1234",
  "createdBy": "quays_ab6",
  "updatedBy": "quays_ab6",
  "centralizedPolicyRules": [
    {
      "name": "Rule123",
      "type": "IMAGESCAN_VULN_SEVERITYCOUNT",
      "action": "DENY",
      "isEnabled": true,
      "stopProcessing": false,
      "sortOrder": 0,
      "metaData":
{"operator":"GREATER_THAN","severityLevel":1,"threshold":1}
    }
  ],
  "assetType": "CICD",
  "isDefault": false,
  "tagIds": [
"095a966f-fb5f-4eb5-8d43-b77d1a740876"
  ]
}
```

Response:

```
{
  "uuid": "d967073a-28d8-414d-b96d-3d19eaa20935"
}
Response Code: 200
```

Show Policy Details

API affected	/csapi/v1.3/centralizedPolicy/{policyId}
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Shows details of a policy.

Input Parameter

Parameter	Mandatory	Data Type	Description
policyId	Yes	string	Specify the UUID of the policy of which you want to fetch details.

Sample: Fetch Details of a Policy

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/centralizedPolicy/7a64bbd7-67a8-4c39-981e-
6345c62bacb2'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:


```
{
  "uuid": "7a64bbd7-67a8-4c39-981e-6345c62bacb2",
  "policyName": "Policy123",
  "policyType": "IMAGESCAN",
  "policyMode": "ACTIVE",
  "description": "Policy123",
  "createdBy": "user1",
  "created": "1683537516989",
  "updatedBy": "user1",
  "updated": "1683537516989",
  "centralizedPolicyRules": [
    {
      "name": "Rule123",
      "type": "IMAGESCAN_VULN_SEVERITYCOUNT",
      "action": "DENY",
      "isEnabled": true,
      "stopProcessing": false,
```

```
      "sortOrder": 0,
      "metaData":
"{\"operator\":\"GREATER_THAN\",\"severityLevel\":1,\"threshold\":1}"
    }
  ],
  "version": 1,
  "assetType": "CICD",
  "isDefault": false,
  "tagIds": [
    {
      "uuid": "cf203e51-490f-47d4-b271-bdc4822f6181",
      "id": 7624640,
      "name": "Tag-101",
      "backgroundColor": "#B6D7A8",
      "foregroundColor": "#000000",
      "icon": null,
      "criticalityScore": 0,
      "tagType": null
    },
    {
      "uuid": "383318ae-3e32-420a-a3dc-4deaab5ee283",
      "id": 7624639,
      "name": "Tag-10",
      "backgroundColor": "#F9CB9C",
      "foregroundColor": "#000000",
      "icon": null,
      "criticalityScore": 0,
      "tagType": null
    }
  ]
}
```

Delete a Policy

API affected	/csapi/v1.3/centralizedPolicy/{policyId}
Operator	DELETE
New or Updated APIs	New
DTD or XSD Changes	NA

Deletes a policy from your account.

Input Parameter

Parameter	Mandatory	Data Type	Description
policyId	Yes	string	Specify the UUID of the policy you want to delete.

Sample: Delete a Policy

API Request:

```
curl -X 'DELETE' \
'<qualys_base_url>/csapi/v1.3/centralizedPolicy/7a64bbd7-67a8-4c39-981e-
6345c62bacb2' \
-H 'accept: application/json' \
-H 'Authorization: Bearer <token>'
```

Response:

```
Response code 200
{
  "uuid": "7a64bbd7-67a8-4c39-981e-6345c62bacb2"
}
```

Activate or Deactivate a Policy

API affected	/csapi/v1.3/centralizedPolicy/{policyId}/mode
Operator	PUT
New or Updated APIs	New
DTD or XSD Changes	NA

Activates or deactivates a policy by changing the policy mode to active or inactive.

Input Parameters

Parameter	Mandatory?	Data Type	Description
policyId	Mandatory	string ($uuid)	Specify the UUID of the policy you want to activate or deactivate.
Request body	Mandatory	-	-

Sample: Deactivate a Policy

API Request:

```
curl -X 'PUT'
'<qualys_base-url>/csapi/v1.3/centralizedPolicy/7a64bbd7-67a8-4c39-981e-
6345c62bacb2/mode'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
-H 'Content-Type: application/json'
```

Request Body:

```
{
  "policyMode": "INACTIVE"
}
```

Response:

```
{
  "uuid": "7a64bbd7-67a8-4c39-981e-6345c62bacb2"
}
```

Show EC2 Instance ID in Container and Sensor Details

API affected	/csapi/v1.3/containers/{containerSha} /csapi/v1.3/sensors/{sensorId}
Operator	GET
New or Updated APIs	Updated
DTD or XSD Changes	NA

As the IP address of a host is not always unique and may change, searching for assets on a specific host using host's IP address may provide inaccurate results.

Cloud providers add an instance ID to hosts to uniquely identify them within the cloud environment. With this release, the EC2 instance ID is now displayed in the sensor details and the details of containers being scanned by the sensor.

Sample 1: Instance ID in Container Details

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/containers/647ae732d98e1bcceb7b02356bd7e873
eef13c5916c3a1e9d95700ab893cc09f'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:

```
{
    "portMapping": null,
    "imageId": "a6c0cb5dbd21",
    "created": "1683279176000",
    "updated": "1683622183866",
    "label": [
        {
            "key": "io.kubernetes.container.name",
            "value": "kube-flannel"
        },
        {
            "key":
"annotation.io.kubernetes.container.terminationMessagePath",
            "value": "/dev/termination-log"
        }
    ],
    "uuid": "a90b7cb5-c704-3343-b538-74c7807807a2",
    "sha":
"647ae732d98e1bcceb7b02356bd7e873eef13c5916c3a1e9d95700ab893cc09f",
```

```
    "privileged": false,
    "path": "/opt/bin/flanneld",
    "imageSha":
"a6c0cb5dbd21197123942b3469a881f936fd7735f2dc9a22763b6f777f24345e",
    "macAddress": "",
    "customerUuid": "6a849349-679f-ef25-8296-e51d4e3a0019",
    "ipv4": null,
    "ipv6": null,
    "name": "k8s_kube-flannel_kube-flannel-ds-mpmq6_kube-
flannel_5a737762-77c2-4763-9c1c-84c15a2684f0_0",
    "host": {
        "sensorUuid": "dae76860-22f7-4ef1-9a67-aef07944d92c",
        "hostname": "ip-10-82-9-150",
        "ipAddress": "10.82.9.150",
        "uuid": "86e028bd-f283-4468-a099-953a6a033728",
        "lastUpdated": "2023-05-09T08:47:15.854Z"
    },
    "hostArchitecture": [
        "x86_64"
    ],
    "state": "RUNNING",
    "imageUuid": "9baf9f85-f3bf-3259-b8d5-3cd51967d34a",
    "containerId": "647ae732d98e",
    "stateChanged": "1683528203674",
    "services": null,
    "users": [
        "root"
    ],
    "operatingSystem": "Alpine Linux 3.17.3",
...
    "cloudProvider": {
        "aws.ecs.container.subnetId": null,
        "aws.ec2.instanceId": "i-0ab8d3318979f529c",
        "aws.ecs.clusterName": null,
        "aws.ecs.container.macAddress": null,
        "aws.ecs.region.code": null,
        "aws.ecs.container.id": null,
        "aws.ecs.accountId": null
    }
}
```


Sample 2: Instance ID in Sensor Details

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/sensors/826194dcacba'
-H 'accept: application/json'
```

```
-H 'Authorization: Bearer <token>'
```

Response:


```
{
    "uuid": "dae76860-22f7-4ef1-9a67-aef07944d92c",
    "activationUuid": "ba77c39a-8086-44c5-aa08-7140aec8315e",
    "hostname": "ip-10-x-x-x",
    "customerUuid": "6a849349-679f-ef25-8296-e51d4e3a0019",
    "dockerVersion": "23.0.5",
    "ipv4": "10.x.x.x",
    "os": "Ubuntu 22.04.2 LTS",
    "ipv6": "fe80::8da:56ff:fea5:613d",
    "sensorVersion": "1.26.1-0",
    "platform": "LINUX_SENSOR",
    "lastCheckedIn": "1683622119229",
    "label": [
        {
            "key": "image-source",
            "value": "SJC-POD04"
        },
        {
            "key": "name",
            "value": "Qualys Sensor Image"
        }
    ],
    "privileged": "false",
    "macAddress": "0a:da:56:a5:61:3d",
    "vulnSigVersion": null,
    "hostUuid": "86e028bd-f283-4468-a099-953a6a033728",
   ...
    "cluster": {
        "type": "KUBERNETES",
        "k8s": {
            "project": null,
            "pod": {
                "name": "qualys-container-sensor-n28mk",
                "uuid": "8beae725-d936-4fec-a50d-63d378279b24",
                "namespace": "qualys",
                "namespaceMetadata": {
                    "labels": [
                        "kubernetes.io/metadata.name:qualys"
                    ],
                    "annotations": null
                },
                "label": [
                    {
                        "key": "name",
```

```
                        "value": "qualys-container-sensor"
                    }
                ],
                "controller": [
                    {
                        "uuid": "6d0a6a96-6697-4c6f-9c9b-163df321faca",
                        "name": "qualys-container-sensor",
                        "type": "DaemonSet"
                    }
                ]
            },
            "node": {
                "name": "ip-10-x-x-x",
                "isMaster": false
            }
        },
        "version": "v1.26.3"
    },
    "cloudProvider": {
        "aws": {
            "ec2": {
                "instance-id": "i-0ab8d3318979f529c"
            }
        }
    }
}
```

Capture Namespace Labels and Annotations in Kubernetes Metadata

API affected	/csapi/v1.3/containers/{containerSha} /csapi/v1.3/sensors/{sensorId}
Operator	GET
New or Updated APIs	Updated
DTD or XSD Changes	NA

With this release, the sensor deployed on Kubernetes cluster now captures the namespace labels and annotations assigned on containers. You can retrieve these labels and annotations as part of the container and sensor details.

Sample 1: Labels and Annotations in Container Details

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/containers/647ae732d98e1bcceb7b02356bd7e873
eef13c5916c3a1e9d95700ab893cc09f'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:

```
{
    "portMapping": null,
    "imageId": "a6c0cb5dbd21",
    "created": "1683279176000",
    "updated": "1683622183866",
    "label": [
        {
            "key": "io.kubernetes.container.name",
            "value": "kube-flannel"
        },
        {
            "key":
"annotation.io.kubernetes.container.terminationMessagePath",
            "value": "/dev/termination-log"
        }
    ],
    "uuid": "a90b7cb5-c704-3343-b538-74c7807807a2",
    "sha":
"647ae732d98e1bcceb7b02356bd7e873eef13c5916c3a1e9d95700ab893cc09f",
   ...
```

```
"host": {
    "sensorUuid": "dae76860-22f7-4ef1-9a67-aef07944d92c",
    "hostname": "ip-10-82-9-150",
    "ipAddress": "10.82.9.150",
    "uuid": "86e028bd-f283-4468-a099-953a6a033728",
    "lastUpdated": "2023-05-09T08:47:15.854Z"
},
"hostArchitecture": [
    "x86_64"
],
"state": "RUNNING",
"imageUuid": "9baf9f85-f3bf-3259-b8d5-3cd51967d34a",
"containerId": "647ae732d98e",
"stateChanged": "1683528203674",
"services": null,
"users": [
    "root"
],
"operatingSystem": "Alpine Linux 3.17.3",
...

"cluster": {
    "type": "KUBERNETES",
    "k8s": {
        "project": null,
        "pod": {
            "name": "kube-flannel-ds-mpmq6",
            "uuid": "5a737762-77c2-4763-9c1c-84c15a2684f0",
            "namespace": "kube-flannel",
            "namespaceMetadata": {
                "labels": [
                    "kubernetes.io/metadata.name:kube-system",
                   "jlabel2:pod-securitykubernetes.io-enforce_check",
                    "jlabel:pod-securitykubernetes.io-enforce"

                ],
                "annotations": [
                    "testcsv1:kube-sec*check.io/special#123",
                    "process.test:kube-sec*check.io/special#123"
                ]
            },
            "label": [
                {
                    "key": "tier",
                    "value": "node"
                }

            ],
          ...
```

```
            },
            "node": {
                "name": "ip-10-82-9-150",
                "isMaster": false
            }
        },
        "version": "v1.26.3"
    },
    "cloudProvider": {
        "aws.ecs.container.subnetId": null,
        "aws.ec2.instanceId": "i-0ab8d3318979f529c",
        "aws.ecs.clusterName": null,
        "aws.ecs.container.macAddress": null,
        "aws.ecs.region.code": null,
        "aws.ecs.container.id": null,
        "aws.ecs.accountId": null
    }
}
```


Sample 2: Labels and Annotations in Sensor Details

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/sensors/826194dcacba'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:


```
{
    "uuid": "dae76860-22f7-4ef1-9a67-aef07944d92c",
    "activationUuid": "ba77c39a-8086-44c5-aa08-7140aec8315e",
    "hostname": "ip-10-x-x-x",
    "customerUuid": "6a849349-679f-ef25-8296-e51d4e3a0019",
    "dockerVersion": "23.0.5",
    "ipv4": "10.x.x.x",
    "os": "Ubuntu 22.04.2 LTS",
    "ipv6": "fe80::8da:56ff:fea5:613d",
    "sensorVersion": "1.26.1-0",
    "platform": "LINUX_SENSOR",
    "lastCheckedIn": "1683622119229",
    "label": [
        {
            "key": "image-source",
            "value": "SJC-POD04"
        },
        {
```

```
            "key": "name",
            "value": "Qualys Sensor Image"
        }
    ],
    "privileged": "false",
    "macAddress": "0a:da:56:a5:61:3d",
    "vulnSigVersion": null,
    "hostUuid": "86e028bd-f283-4468-a099-953a6a033728",
...
    "cluster": {
        "type": "KUBERNETES",
        "k8s": {
            "project": null,
            "pod": {
                "name": "qualys-container-sensor-n28mk",
                "uuid": "8beae725-d936-4fec-a50d-63d378279b24",
                "namespace": "qualys",
                "namespaceMetadata": {
                    "labels": [
                        "kubernetes.io/metadata.name:qualys"
                    ],
                    "annotations": null
                },
                "label": [
                    {
                        "key": "name",
                        "value": "qualys-container-sensor"
                    }
                ],
                "controller": [
                    {
                        "uuid": "6d0a6a96-6697-4c6f-9c9b-163df321faca",
                        "name": "qualys-container-sensor",
                        "type": "DaemonSet"
                    }
                ]
            },
            "node": {
                "name": "ip-10-x-x-x",
                "isMaster": false
            }
        },
        "version": "v1.26.3"
    },
    "cloudProvider": {
        "aws": {
            "ec2": {
                "instance-id": "i-0ab8d3318979f529c"
            }
```

```
            }
        }
    }
```