Qualys Container Security v1.x

API Release Notes

Version 1.7

November 16, 2020

Qualys Container Security API gives you many ways to integrate your programs and API calls with Qualys capabilities.

What's New

Container Runtime Security - Changes to Rule Parameters for Create/Update Policy

Container Runtime Security - New API to Delete Policies

Container Runtime Security - Pagination Now Supported for List Policies

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

This documentation uses the API server URL for Qualys US Platform 1 (https://qualysapi.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate server URL for your account.

Container Runtime Security - Changes to Rule Parameters for Create/Update Policy

APIs affected	/csapi/v1.2/runtime/policies
New or Updated APIs	Updated

We made several changes to the input parameters for defining policy rules when creating and updating runtime security policies. Also, you'll see new policy rule values in the response output when you list policies or get details for a specific policy. These changes will make defining policy rules easier than ever. See a summary of the changes below.

Updated RuleType values

We made the following changes to the RuleType input parameter values:

- listener changed to network_inbound

- network changed to network_outbound

- file changed to read

- write was added

- execution was removed (instead, use syscall for execution rules)

Added parameters

The following input parameters were added: IpAddress and Port. Use these inputs when the RuleType is network_inbound or network_outbound. These replace ListeningPort, ListeningAddr, RemotePort, RemoteIps.

Removed parameters

The following input parameters are no longer supported: ListeningPort, ListeningAddr, RemotePort, RemoteIps, Protocol.

Rule Samples

Please see the following sample rules for new and updated rule types.

Rule with type network_inbound


```
{
"ID": "5fa25442e677eb00012916bc",
"Name": "Block_sshd_communication",
"DateCreated": "0001-01-01T00:00:00Z",
"DateUpdated": "0001-01-01T00:00:00Z",
"InActive": false,
"RuleType": "network_inbound",
```

```
"Program": "*",
"Action": "deny",
"File": "",
"Port": 22,
"IpAddress": "*",
"Syscall": "",
"SyscallGroup": "",
"Arg1": "",
"Arg2": "",
"Arg3": ""
}
```


Rule with type network_outbound


```
{
"ID": "5fa24e78e677eb00012916b3",
"Name": "Deny_Outbound",
"DateCreated": "0001-01-01T00:00:00Z",
"DateUpdated": "0001-01-01T00:00:00Z",
"InActive": false,
"RuleType": "network_outbound",
"Program": "*",
"Action": "deny",
"File": "",
"Port": 22,
"IpAddress": "1.1.1.1",
"Syscall": "",
"SyscallGroup": "",
"Arg1": "",
"Arg2": "",
"Arg3": ""
}
```


Rule with type read


```
{
"ID": "5fa2512de677eb00012916b5",
"Name": "Deny_Hosts_Write_Attempt",
"DateCreated": "0001-01-01T00:00:00Z",
"DateUpdated": "0001-01-01T00:00:00Z",
"InActive": false,
"RuleType": "read",
"Program": "/bin/cat",
"Action": "deny",
"File": "/etc/hosts",
"Port": 0,
"IpAddress": "",
"Syscall": "",
```

```
"SyscallGroup": "",
"Arg1": "",
"Arg2": "",
"Arg3": ""
},
```


Rule with type write


```
{
"ID": "5fa25442e677eb00012916b7",
"Name": "Static file modification deny",
"DateCreated": "0001-01-01T00:00:00Z",
"DateUpdated": "0001-01-01T00:00:00Z",
"InActive": false,
"RuleType": "write",
"Program": "*",
"Action": "deny",
"File": "/var/www/html/*",
"Port": 0,
"IpAddress": "",
"Syscall": "",
"SyscallGroup": "",
"Arg1": "",
"Arg2": "",
"Arg3": ""
}
```

Container Runtime Security - New API to Delete Policies

APIs affected	/csapi/v1.2/runtime/policies/{policyId}
New or Updated APIs	New

Starting with this release you can delete Container Runtime Security policies using the API. You'll need to specify the policyId for the policy you want to delete as part of the API request. Note that you cannot delete a policy that is currently associated with an instrumented image/container.

Delete a security policy

/csapi/v1.2/runtime/policies/{policyId}

[DELETE]

Input Parameters:

Parameter	Description
policyId	(Required) Specify the ID of the policy to delete.

API request:

```
curl -X DELETE --header 'Accept: text/plain' --header 'Authorization:
Basic VVNFUk5BTUU6UEFTU1dPUkQ='
'https://gateway.qg1.apps.qualys.com/csapi/v1.2/runtime/policies/5fa97660
f19b060001e8ab6f'
```

Response:

```
response code 200
```

Container Runtime Security - Pagination Now Supported for List Policies

APIs affected	/csapi/v1.2/runtime/policies
New or Updated APIs	Updated

We now support pagination when you use the API to get a list of policies in your account. You'll use the input parameters pageNumber and pageSize to specify the page number to be returned and the number of records to be returned per page.

Get all policies in your account

/csapi/v1.2/runtime/policies

[GET]

Input Parameters:

Parameter	Description
pageNumber	The page to be returned. The default value is 1.
pageSize	The number of records per page to be included in the response. When not specified, you'll get 50 records.

API request:

In this sample, we've specified page 1 to be returned with 2 policies per page.

```
curl --location --request GET
'https://gateway.qg1.apps.qualys.com/csapi/v1.2/runtime/policies?pageNumb
er=1&pageSize=3' \
--header 'Authorization: Bearer <token>'
```

Response:

```
[
    {
        "ID": "5fa97a53243aec0001ef98ee",
        "Name": "My First Policy",
        "DateCreated": "2020-11-09T17:20:19.566Z",
        "DateUpdated": "2020-11-09T17:20:19.566Z",
        "Description": "first policy",
        "Mode": 0
    },
    {
        "ID": "5fa97660f19b060001e8ab6f",
        "Name": "Monitor Write for Bash",
```

```
        "DateCreated": "2020-11-09T17:03:28.772Z",
        "DateUpdated": "2020-11-09T17:07:40.557Z",
        "Description": "Monitor the Write event for mentioned bash files",
        "Mode": 0
    },
    {
        "ID": "5f9bc49314c4e000019db314",
        "Name": "Default Policy",
        "DateCreated": "0001-01-01T00:00:00Z",
        "DateUpdated": "2020-10-30T07:46:36.847Z",
        "Description": "Default group policy",
        "Mode": 0
    }
]
```