ThreatConnect® Management API User Guide

Document Version 1.0

Technical Guide

April 5, 2022

10020-02 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 I F: 703.229.4489
www.ThreatConnect.com

Table of Contents

Overview

The Management API allows administrators to query their ThreatConnect instance to check health, status, and activity. Using REST API commands, administrators can monitor their instance to ensure it is in a healthy state. Additional endpoints allow in-depth checks, like thread dumps and Java® virtual machine (JVM) statistics. The API also supports a few administrative tasks, like clearing the entity cache and resetting locked user accounts. The API is also extensible using custom SQL queries that can be called directly using REST endpoints.

Important: Extending the API with custom SQL is considered an advanced technique, and care must be taken in a production environment to not tax the database with expensive queries. This feature is not supported in Dedicated Cloud instances.

Configuration

To use the API, the system configuration `statuskey` property must be set with a user-generated key. This key will be used in all API request headers to authenticate to the instance. Because this is an administrative feature, standard ThreatConnect API keys will not work.

Note: These instructions apply to On-Premises ThreatConnect instances only. Users running Dedicated Cloud instances should email success@threatconnect.com to request a `statuskey`.

To apply this key, users must run the following SQL on their instance with their custom value (limit is 255 characters). This property is hidden in the **System Settings** UI screen.

```
update systemconfig set value = 'abcd' where name = 'statusKey';
```

All references in this document will use the variables in Table 1 to make requests. Users must use their instance details in place of these variables.

Table 1

Variable	Description
{{statuskey}}	The user's status key defined in this section.
{{baseUrl}}	The user's instance fully qualified domain name (e.g., **https://app.threatconnect.com**).

Use the following header to authenticate to the Management API:

```
Header: statuskey: {{statuskey}}
```

API Detail

Retrieve License Information

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/license"`
HTTP	`GET {{baseUrl}}/api/v1/management/license`

Sample Response

Status 200 OK


```
{
    "status": "Success",
    "data": {
        "indicatorLimit": 2147483647,
        "userLimit": 999,
        "organizationLimit": 2147483647,
        "docStorageLimit": 9223372036854775807,
        "apiLimit": 999,
        "taxiiLimit": 999
    }
}
```

Retrieve JVM Stats

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/jvm/stats"`
HTTP	`GET {{baseUrl}}/api/v1/management/jvm/stats`

Sample Response

Status 200 OK

```
{
    "status": "Success",
    "data": {
        "maxMemoryMb": 629,
        "heapMemoryUsed": 4437496096,
        "heapMemoryCommitted": 5825888256,
        "openFileHandles": 3619
    }
}
```

Available Parameters

Name	Description
instance	Specifies the server for which to retrieve information. Accepted values include **tc-app**, **tc-job**, and **tc-mon**.

Retrieve JVM Thread Dump

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/jvm/threadDump"`
HTTP	`GET {{baseUrl}}/api/v1/management/jvm/threadDump`

Sample Response

Status 200 OK

```
"Reference Handler"
   java.lang.Thread.State: RUNNABLE
        at
java.base@11.0.6/java.lang.ref.Reference.waitForReferencePendingList(Native Method)
        at
java.base@11.0.6/java.lang.ref.Reference.processPendingReferences(Reference.java:24
1)
        at
java.base@11.0.6/java.lang.ref.Reference$ReferenceHandler.run(Reference.java:213)
"Finalizer"
   java.lang.Thread.State: WAITING
        at java.base@11.0.6/java.lang.Object.wait(Native Method)
        at
java.base@11.0.6/java.lang.ref.ReferenceQueue.remove(ReferenceQueue.java:155)
        at
java.base@11.0.6/java.lang.ref.ReferenceQueue.remove(ReferenceQueue.java:176)
        at
java.base@11.0.6/java.lang.ref.Finalizer$FinalizerThread.run(Finalizer.java:170)
...
```

Available Parameters

Name	Description
instance	Specifies the server for which to retrieve information. Accepted values include **tc-app**, **tc-job**, and **tc-mon**.
type	Specifies the response format. Accepted values include **json** and **raw**.

Retrieve Status of Feeds

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/feeds"`
HTTP	`GET {{baseUrl}}/api/v1/management/feeds`

Sample Response

Status 200 OK

```
{
    "status": "Success",
    "data": [{
            "name": "SNP TI",
            "nextRunTime": "2021-03-01T16:00:00.000Z",
            "cronSchedule": "0 0 19-23/2,0-18/2 ? * *",
            "type": "JOB",
            "lastExecutionResponse": {
                "sessionId": "c3c50137-a65b-4fee-9ebe-27f494895998",
                "status": "Detached"
            }
        },
        {
            "name": "CAL Retail-themed NRDs",
            "status": "Complete",
            "nextRunTime": "2022-03-16T13:24:27.321Z",
            "type": "BULK",
            "lastExecutionResponse": {
                "startTime": "2022-03-15T13:28:04.333Z"
            }
        },
        {…}
    ]
}
```

Available Parameters

Name	Description
type	Specifies the type of feed for which information should be retrieved. Accepted values, which are case sensitive, include **BULK**, **JOB**, **SOURCE_FEED**, and **TAXII**.

Retrieve Server Logs

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/core/{{server}}/server.log"`
HTTP	`GET {{baseUrl}}/api/v1/management/core/{{server}}/server.log`

Note: Replace `{{server}}` with the name of the server (**tc-app**, **tc-job**, or **tc-mon**) for which the server log will be retrieved.

Sample Response

Status 200 OK
`<Contents of Server log>`

Note: To view the contents of the logs, save the JSON response to a ZIP file and then extract the file.

Retrieve Job Logs

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/log/job/{{sessionId}}"`
HTTP	`GET {{baseUrl}}/api/v1/management/log/job/{{sessionId}}`

Note: Replace `{{sessionId}}` with the `sessionId` of the Job for which logs will be retrieved. A Job's `sessionId` can be found using the `/v1/management/feeds` endpoint.

Sample Response

Status 200 OK
`<raw contents of Job logs>`

Note: To view the contents of the logs, save the JSON response to a ZIP file and then extract the file.

Retrieve Job Log List

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/log/job/{{sessionId}}/listFiles"`
HTTP	`GET {{baseUrl}}/api/v1/management/log/job/{{sessionId}}/listFiles`

Note: Replace `{{sessionId}}` with the `sessionId` of the Job for which a list of log files will be retrieved. A Job's `sessionId` can be found using the `/v1/management/feeds` endpoint.

Sample Response

Status 200 OK

```
{
    "status": "Success",
    "data": [
        {
            "fileName": "stdout.log"
        },
        {
            "fileName": "stderr.log"
        },
        {
            "fileName": "CrossIntelSharingApp.log"
        }
    ]
}
```

Retrieve Service Logs

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/log/service/{{sessionId}}"`
HTTP	`GET {{baseUrl}}/api/v1/management/log/service/{{sessionId}}`

Note: Replace `{{sessionId}}` with the session ID of the Service for which logs will be retrieved. A Service's session ID can be found on the **Services** tab of the **Playbooks** screen in the ThreatConnect UI. See the "Viewing a Service" section of *Playbook Services* for more information.

Sample Response

Status 200 OK
`<raw contents of Service logs>`

Note: To view the contents of the logs, save the JSON response to a ZIP file and then extract the file.

Retrieve Service Log List

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/log/service/{{sessionId}}/listFiles"`
HTTP	`GET {{baseUrl}}/api/v1/management/log/service/{{sessionId}}/listFiles`

Note: Replace `{{sessionId}}` with the session ID of the Service for which logs will be retrieved. A Service's session ID can be found on the **Services** tab of the **Playbooks** screen in the ThreatConnect UI. See the "Viewing a Service" section of *Playbook Services* for more information.

Sample Response

Status 200 OK

```
{
    "status": "Success",
    "data": [
        {
            "fileName": "stdout.log"
        },
        {
            "fileName": "stderr.log"
        },
        {
            "fileName": "app.log"
        }
    ]
}
```

Retrieve Playbook Activity Stats

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/playbooks/activity/stats"`
HTTP	`GET {{baseUrl}}/api/v1/management/playbooks/activity/stats`

Sample Response

Status 200 OK


```
{
    "status": "Success",
    "data": {
        "queueSize": 0,
        "workerCount": 6,
        "publicServers": [
            {
                "name": "tc-job",
                "specs": {
                    "os": "CentOS Linux | GNU/Linux  7 (Core) build 4.14.219-
119.340.amzn1.x86_64 ",
                    "diskGb": 196,
                    "cpuCount": 16,
                    "memGb": 61
                },
                "consumerCount": 6
            }
        ],
        "privateServers": [],
        "executionsTotal": 31614,
        "executionsToday": 248,
        "maxExecutionLimit": 10000,
        "brokerConnectionCount": 27
    }
}
```

Retrieve Running Playbook Activity

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/playbooks/activity/running"`
HTTP	`GET {{baseUrl}}/api/v1/management/playbooks/activity/running`

Sample Response

Status 200 OK


```
{
    "status": "Success",
    "data": [
        {
            "sessionId": "d071342b-5496-4f65-b536-4c4b6afb5958",
            "playbookId": 8876,
            "playbookName": "PB Execution Monitor - DO NOT TOUCH",
            "groupXid": "NPNzmiAS",
            "playbookLastModified": "2022-01-24T13:59:42.526Z",
            "startTime": "2022-03-04T21:27:18.149Z"
        }
    ]
}
```

Retrieve Playbook Worker Stats

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/playbooks/activity/workers"`
HTTP	`GET {{baseUrl}}/api/v1/management/playbooks/activity/workers`

Sample Response

Status 200 OK


```
{
    "status": "Success",
    "data": [
        {
            "workerName": "Takodana",
            "serverName": "tc-job",
            "status": "IDLE",
            "lastSessionId": "bb1b3f83-dfe9-411d-a518-f964d97cc3a2",
            "lastActivityTime": "2021-03-01T15:15:00.503Z"
        },
        {
            "workerName": "Kashyyyk",
            "serverName": "tc-job",
            "status": "IDLE",
            "lastSessionId": "16e1ac4e-da0b-42bd-83cf-21b8d57c7cbc",
            "lastActivityTime": "2021-03-01T15:10:00.441Z"
        },
        {
            "workerName": "Polis Massa",
            "serverName": "tc-job",
            "status": "IDLE",
            "lastSessionId": "1dc4daf9-0a10-4f3d-9ab6-d464633ddeb5",
            "lastActivityTime": "2021-03-01T15:00:00.515Z"
        },
        {
            "workerName": "Naboo",
            "serverName": "tc-job",
            "status": "IDLE",
            "lastSessionId": "55260fb7-b08b-423f-9fca-183d0c2448ad",
            "lastActivityTime": "2021-03-01T15:20:00.426Z"
        },
        {
```

```
            "workerName": "Shili",
            "serverName": "tc-job",
            "status": "IDLE",
            "lastSessionId": "4141a4c5-364e-4bf5-8d08-e02c80a5f265",
            "lastActivityTime": "2021-03-01T15:05:00.399Z"
        },
        {
            "workerName": "Jedha",
            "serverName": "tc-job",
            "status": "IDLE",
            "lastSessionId": "14617e4e-ff0b-48a7-8b70-a872cad406b9",
            "lastActivityTime": "2021-03-01T15:17:16.231Z"
        }
    ]
}
```


Available Parameters

Name	Description
instance	Specifies the server for which to retrieve information. Accepted values include **tc-app**, **tc-job**, and **tc-mon**.

Update Playbook Worker Count

Commands

Curl	`curl -X PUT -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/playbooks/activity/workers?instance={{instanceName}}&count={{workerCount}}"`
HTTP	`PUT {{baseUrl}}/api/v1/management/playbooks/activity/workers?instance={{instanceName}}&count={{workerCount}}`

Note: Replace `{{instanceName}}` with the name of the server for which the Worker count will be updated, and replace `{{workerCount}}` with the new number of Workers for the specified server.

Sample Response

Status 200 OK

```
{
    "status": "Success"
}
```

Available Parameters

Name	Description
instance	Specifies the server for which the Worker count will be updated. Accepted values include **tc-app**, **tc-job**, and **tc-mon**.
count	Specifies the Worker count for the specified server. The default server is **tc-job**. **Important**: The `count` parameter is required when updating the Playbook worker count.

Retrieve a Playbook

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/playbooks/{{groupXid}}/download"`
HTTP	`GET {{baseUrl}}/api/v1/management/playbooks/{{groupXid}}/download`

Note: Replace `{{groupXid}}` with the `groupXid` of the Playbook for which information will be retrieved.

Sample Response

Status 200 OK


```
{
    "name": "DomainTools Iris - Host Enrichment",
    "type": "Playbook",
    "panX": -947.0,
    "panY": -401.0,
    "zoom": 1.0,
    "logLevel": "WARN",
    "description": "This playbook begins with a User Action trigger on a Host
Indicator.  It requests the Domain Profile from DomainTools Iris and parses the
results.  It then adds an Attribute and Tags with the enrichment results from
DomainTools.",
    "roiDollarsPerHour": 75,
    "roiMinutes": 10,
    "priority": 6,
    "version": "2.2",
    "comment": "Auto-Saved on Tue Mar 15 16:47:18 UTC 2022",
    "jobList": [
…
```

Retrieve Playbook Queue Stats

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/queue/stats"`
HTTP	`GET {{baseUrl}}/api/v1/management/queue/stats`

Sample Response

Status 200 OK


```
{
    "status": "Success",
    "data": [
        {
            "queueName": "BatchJobQueue",
            "queueSize": 0,
            "messagesAdded": 0,
            "messagesProcessed": 0
        },
        {
            "queueName": "DNSMonitorQueue",
            "queueSize": 0,
            "messagesAdded": 0,
            "messagesProcessed": 0
        },
        {
            "queueName": "SearchClusterQueue",
            "queueSize": 0,
            "messagesAdded": 0,
            "messagesProcessed": 0
        },
        {
            "queueName": "InboundMailQueue",
            "queueSize": 0,
            "messagesAdded": 0,
            "messagesProcessed": 0
        },
        {
            "queueName": "JobExecutionQueue",
            "queueSize": 0,
            "messagesAdded": 0,
            "messagesProcessed": 0
```

```
        },
        {
            "queueName": "JobLogRequestQueue",
            "queueSize": 0,
            "messagesAdded": 0,
            "messagesProcessed": 0
        },
        {
            "queueName": "ServerLogRequestQueue",
            "queueSize": 0,
            "messagesAdded": 0,
            "messagesProcessed": 0
        },

        {
            "queueName": "PlaybookExecutionQueue",
            "queueSize": 0,
            "messagesAdded": 265,
            "messagesProcessed": 265
        }
    ]
}
```


Available Parameters

Name	Description
instance	Specifies the server for which to retrieve information. Accepted values include **tc-app**, **tc-job**, and **tc-mon**.

Retrieve Playbook Environments

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/playbooks/environments"`
HTTP	`GET {{baseUrl}}/api/v1/management/playbooks/environments`

Sample Response

Status 200 OK


```
{
    "status": "Success",
    "data": [
        {
            "name": "SOC Environment ",
            "active": true,
            "owners": [
                "SOC Organization"
            ],
            "playbooks": 34,
            "jobs": 73
        },
        {
            "name": "Demo Environment",
            "active": false,
            "owners": [
                "Demo Organization"
            ],
            "playbooks": 0,
            "jobs": 0
        }
    ]
}
```

Unlock a User

Commands

Curl	`curl -X POST -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/user/{{username}}/unlock"`
HTTP	`POST {{baseUrl}}/api/v1/management/user/{{username}}/unlock`

Note: Replace `{{username}}` with the username of the user account to be unlocked.

Sample Response

Status 200 OK

```
{
    "status": "Success"
}
```

Retrieve Logged-In Users

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/users/loggedIn"`
HTTP	`GET {{baseUrl}}/api/v1/management/users/loggedIn`

Sample Response

Status 200 OK

```
{
    "status": "Success",
    "data": [
        {
            "userName": "jsmith",
            "firstName": "John",
            "lastName": "Smith",
            "pseudonym": "JMS",
            "role": "Administrator"
        },
        {
            "userName": "pjones",
            "firstName": "Patrick",
            "lastName": "Jones",
            "pseudonym": "PFJ",
            "role": "Read Only User"
        }
    ]
}
```

Create Log Alert Subscriber

Commands

Curl	`curl -X PUT -H "statuskey: {{statuskey}}" -d "{ "name": "OOM Error", "className": "java.lang.OutOfMemoryError", "notifyType": "EMAIL", "notifyEndpoint": " jsmith@companyabc.com ", "threadDump": true }" "{{baseUrl}}/api/v1/management/alert/subscribers"`
HTTP	`PUT {{baseUrl}}/api/v1/management/alert/subscribers { "name": "OOM Error", "className": "java.lang.OutOfMemoryError", "notifyType": "EMAIL", "notifyEndpoint": "jsmith@companyabc.com", "threadDump": true }`

Note: This example uses the `className` field to create an exception log alert subscriber. To create a regular expression log alert subscriber, replace the `className` field with the `regex` field.

Sample Response

Status 200 OK

```
{
    "status": "Success",
    "data": {
        "id": 1,
        "name": "OOM Error",
        "regex": null,
        "className": "java.lang.OutOfMemoryError",
        "notifyType": "EMAIL",
        "notifyEndpoint": "jsmith@companyabc.com",
        "serverName": null,
        "threadDump": true,
        "active": true
    }
}
```

Available Fields

Field	Description	Type	Required?
name	The name of the log alert subscriber.	String	True
className	The exception class name to use to detect exception log alerts.	String	True*
regex	The regular expression value to use when monitoring log files using a regular expression.	String	True*
notifyType	The type of notification that will be sent for the log alert subscriber. Accepted values include **EMAIL** and **WEBHOOK**.	String	True
notifyEndpoint	The email address (if `notifyType` is set to **EMAIL**) or URL (if `notifyType` is set to **WEBHOOK)** to which notifications will be sent.	String	True
serverName	The hostname of the server to monitor for the log alert subscriber.	String	False
threadDump	Determines whether to capture thread dumps and send them to the log alert subscriber.	Boolean	False

* If creating an exception log alert subscriber, `className` is required; if creating a regular expression log alert subscriber, `regex` is required.

Retrieve Log Alert Subscribers

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/alert/subscribers"`
HTTP	`GET {{baseUrl}}/api/v1/management/alert/subscribers`

Sample Response

Status 200 OK


```
{
    "status": "Success",
    "data": [
        {
            "id": 1,
            "name": "OOM Error",
            "regex": null,
            "className": "java.lang.OutOfMemoryError",
            "notifyType": "EMAIL",
            "notifyEndpoint": "jsmith@companyabc.com",
            "serverName": null,
            "threadDump": true,
            "active": true
        }
    ]
}
```

Disable Log Alert Subscriber

Commands

Curl	`curl -X POST -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/alert/subscribers/{{subscriberId}}/disable"`
HTTP	`POST {{baseUrl}}/api/v1/management/alert/subscribers/{{subscriberId}}/disable`

Note: Replace `{{subscriberId}}` with the ID of the log alert subscriber to be disabled.

Sample Response

Status 200 OK

```
{
    "status": "Success",
    "data": {
        "id": 1,
        "name": "OOM Error",
        "regex": null,
        "className": "java.lang.OutOfMemoryError",
        "notifyType": "EMAIL",
        "notifyEndpoint": "jsmith@companyabc.com",
        "serverName": null,
        "threadDump": true,
        "active": false
    }
}
```

Enable Log Alert Subscriber

Commands

Curl	`curl -X POST -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/alert/subscribers/{{subscriberId}}/enable"`
HTTP	`POST {{baseUrl}}/api/v1/management/alert/subscribers/{{subscriberId}}/enable`

Note: Replace `{{subscriberId}}` with the ID of the log alert subscriber to be enabled.

Sample Response

Status 200 OK

```
{
    "status": "Success",
    "data": {
        "id": 1,
        "name": "OOM Error",
        "regex": null,
        "className": "java.lang.OutOfMemoryError",
        "notifyType": "EMAIL",
        "notifyEndpoint": "jsmith@companyabc.com",
        "serverName": null,
        "threadDump": true,
        "active": true
    }
}
```

Delete Log Alert Subscriber

Commands

Curl	`curl -X DELETE -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/alert/subscribers/{{subscriberId}}"`
HTTP	`DELETE {{baseUrl}}/api/v1/management/alert/subscribers/{{subscriberId}}`

Note: Replace `{{subscriberId}}` with the ID of the log alert subscriber to be deleted.

Sample Response

Status 200 OK

```
{
    "status": "Success"
}
```

Retrieve Health Check Args

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/health/args"`
HTTP	`GET {{baseUrl}}/api/v1/management/health/args`

Sample Response

Status 200 OK

```
{
    "status": "Success",
    "data": [
        {
            "name": "Monthly Playbook Query",
            "args": [
                "enddate",
                "startdate"
            ]
        }
    ]
}
```

Clear Entity Cache

Commands

Curl	`curl -X POST -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/clearEntityCache"`
HTTP	`POST {{baseUrl}}/api/v1/management/clearEntityCache`

Sample Response

Status 200 OK

```
{
    "status": "Success"
}
```

Recreate Search Index

Commands

Curl	`curl -X POST -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/searchIndex/recreate"`
HTTP	`POST {{baseUrl}}/api/v1/searchIndex/recreate`

Sample Response

Status 200 OK

```
{
    "status": "Success"
}
```

Clear Master Keychain

Commands

Curl	`curl -X POST -H "statuskey: {{statuskey}}" "{{baseUrl}}/api/v1/management/clearMasterKeychain"`
HTTP	`POST {{baseUrl}}/api/v1/management/clearMasterKeychain`

Sample Response

Status 200 OK

```
{
    "status": "Success"
}
```

Custom Health Check (Count Playbooks in TRACE)

With the custom health checks, administrators can build queries and pull results via API calls. For example: showing the SQL process list, Playbooks in TRACE mode, or Playbook execution activity. Any SQL script that returns a dataset can be exposed as an API using the custom health-check feature.

Important: Queries can break after an upgrade to the platform, based on database changes. There is no guarantee that ThreatConnect database tables will stay the same between upgrades, which may directly impact health-check queries. This feature is not supported in Dedicated Cloud instances.

Below is a sample SQL query to build a custom health-check API that returns all Playbooks in TRACE mode.

```
--- Playbooks in TRACE
INSERT INTO systemhealthcheck (name, type, category, description, command,
validation, filterDb, filterScript, hidden)
VALUES ('Playbooks in TRACE', 'DATABASE', 'Database', 'Playbooks in TRACE', 'select
count(*) as Playbook_Count from blueprint where status = ''Active'' and loglevel =
''TRACE''', null, null, null, 1);
```

Once the record is inserted into the database, the following API call will retrieve the results directly from the database.

Commands

Curl	`curl -X POST -H "statuskey: {{statuskey}}" -d '[ { "name": "Playbooks in TRACE" } ]' "{{baseUrl}}/api/v1/management/health?category=Database&name=Playbooks in TRACE"`
HTTP	`POST {{baseUrl}}/api/v1/management/health?category=Database&name=Playbooks in TRACE`

Sample Response

Status 200 OK


```
{
   "status": "Success",
   "data": [
       {
           "category": "Database",
           "name": "Playbooks in TRACE",
           "result": "184",
           "passed": true
       }
   ]
}
```

Custom Health Check (Top Table Counts)

This custom health check (sample only) allows administrators to check the largest tables by row count. Follow the steps below to create this health-check API.

Important: Queries can break after an upgrade to the platform, based on database changes. There is no guarantee that ThreatConnect database tables will stay the same between upgrades, which may directly impact health-check queries. This feature is not supported in Dedicated Cloud instances.

```
-- Top Table Counts
INSERT INTO systemhealthcheck (name, type, category, description, command,
validation, filterDb, filterScript, hidden)
VALUES ('Statement For Counts', 'DATABASE', 'Database', 'Statement For Counts',
'select (select count(*) from indicator) indicator_count, (select count(*) from
indicatorattribute) indicatorattribute_count, (select count(*) from indicator_tag)
indicator_tag_count, (select count(*) from alert) alert_count, (select count(*)
from jobexecution) jobexecution_count, (select count(*) from blueprintexecution)
blueprintexecution_count from license;', null, null, null, 1);
```

Once the record is inserted into the database, the following API call will retrieve the results directly from the database.

Commands

Curl	`curl -X POST -H "statuskey: {{statuskey}}" -d '[ { "name": "Statement For Counts" } ]' "{{baseUrl}}/api/v1/management/health?category=Database&name=Statement For Counts"`
HTTP	`POST {{baseUrl}}/api/v1/management/health?category=Database&name=Statement For Counts`

Sample Response

Status 200 OK


```
{
   "status": "Success",
   "data": [
       {
           "category": "Database",
           "name": "Top table counts",
           "result": [
               {
                   "indicator_count": 16627832,
                   "indicatorattribute_count": 38487028,
                   "indicator_tag_count": 20003691,
                   "alert_count": 1200154,
                   "jobexecution_count": 238904,
                   "blueprintexecution_count": 31620
               }
           ],
           "passed": true
       }
   ]
}
```

Retrieve Instance Status

Commands

Curl	`curl -X GET -H "statuskey: {{statuskey}}" "{{baseUrl}}/status"`
HTTP	`GET {{baseUrl}}/status`

Sample Response

Status 200 OK

```
{
    "Product Version": "6.5.0",
    "DB Status": "OK",
    "HTTP Status": "OK",
    "Filesystem status (JBoss Server Log)": "OK (122861MB remaining)",
    "Filesystem status (Bulk Reports)": "OK (122861MB remaining)",
    "Filesystem status (Local Storage)": "N/A",
    "Filesystem status (TC Server Log)": "OK (122861MB remaining)",
    "Current Time": "2022-04-05T15:44:36.279+0000",
    "Message": "System OK."
}
```