Splunk® Enterprise Getting Data In 8.0.0

Send metrics to a metrics index

Generated: 11/16/2019 2:08 pm
Send metrics to a metrics index

If you gather metrics data, you can send it directly to a metrics index using HEC.

Send metrics in JSON format

Use the HEC /collector REST API endpoint to send metrics data over HTTP or HTTPS in JSON format from a client that is not natively supported to a metrics index.

Create a HEC data input for a Metrics index. Then, use the /collector REST API endpoint to send data to the metrics index using the following format:

```
http://<Splunk_host>:<HTTP_port>/services/collector \
-H "Authorization: Splunk <HEC_token>" \
-d <metrics_data>
```

You need to provide metrics event data and the following values:

- The Splunk host machine (an IP address, host name, or load balancer name)
- An HTTP port number
- An HEC token value

**Examples** The following example shows a command that sends a metric measurement to a metrics index, with the following values:

- Splunk host machine: "localhost"
- HTTP port number: "8088"
- HEC token value: "b0221cd8-c4b4-465a-9a3c-273e3a75aa29"

```
curl -k https://localhost:8088/services/collector \
-H "Authorization: Splunk b0221cd8-c4b4-465a-9a3c-273e3a75aa29" \
-d '{"time":1486683865.000,"source":"disk","host":"host_99","fields":{"region":"us-west-1","datacenter":"us-west-1a","rack":"63","os":...version":"0","service_environment":"test","path":"/dev/sda1","fstype":"ext3","_value":1099511627776,"metric_name":"total"}'}
```

This command sends two metrics measurements:

```
curl -k http://<IP address or host name or load balancer name>:8088/services/collector \
-H "Authorization: Splunk 98a1e071-bc35-410b-8642-78ce7d829083" \
-d '{"time":1505501013.000,"source":"disk","host":"host_99","fields":{"region":"us-west-1","datacenter":"us-west-1a","rack":"63","os":...version":"0","service_environment":"test","path":"/dev/sda1","fstype":"ext3","_value":999311222774,"metric_name":"total"}'}
```
Send metrics in collectd format

Use the HEC /collector/raw REST API endpoint to send metrics data over HTTP or HTTPS in collectd JSON format to a metrics index.

Create a HEC data input for a Metrics index and select the Metrics > collectd_http pre-trained source type. Then, use the /collector/raw REST API endpoint to send data directly to a metrics index using the following format:

```
http://<Splunk_host>:<HTTP_port>/services/collector/raw?source_type=collectd_http
- H "Authorization: Splunk <HEC_token>"
- d "<metrics_data>"
```

You need to provide metrics data in collectd format and the following values:

- The Splunk host machine (an IP address, host name, or load balancer name)
- An HTTP port number
- An HEC token value

Because collectd is supported natively, you can configure collectd to send data to a metrics index. For more, see Get metrics in from collectd in the Metrics manual.

Example

The following example shows a command that sends a metric measurement to a metrics index, with the following values:

- Splunk host machine: "localhost"
- HTTP port number: "8088"
- HEC token value: "b0221cd8-c4b4-465a-9a3c-273e3a75aa29"

```
curl -k
- H "Authorization: Splunk b0221cd8-c4b4-465a-9a3c-273e3a75aa29"
- d 
  ['{"values":[164.9196798931339196],"dstypes":["derive"],"dsnames":["value"],"time":1505356687.894,"interval":10.000,"host":"collectd","plugin":"protocols","plugin_instance":"IpExt","type":"protocol_counter","type_instance":"InOctets"}']
```
For more information

For more information, see:

- Overview of metrics in the *Metrics* manual
- Create metrics indexes in the *Managing Indexers and Clusters of Indexers* manual
- /collector and /collector/raw in the *REST API Reference Manual*