MCAS SIEM Agent Helm Chart

[TOC]

Chart Details

This chart create a **Deployment** of one `replica`, which uses a token to reach out to Microsoft, pull SIEM data, and push it to an endpoint you configure through a Microsoft account.

References

- Download the agent's `.jar` file
- SIEM integration Walkthrough
- Troubleshooting Docs

Install / Upgrade / Delete

Install

1. Add the **Hotrock** chart repository:

```
# TODO
helm repo add hotrock https://github.com/technology-
spa/HOTROCK/charts/mcas-siemagent
```

2. Clone the repo:

```
git clone https://github.com/technology-spa/HOTROCK/charts/mcas-
siemagent/values.yaml
cd ./charts/mcas-siemagent
```

3. Download the agent's `.jar` filehere
4. Build and push the docker image from Dockerfile.
5. Update values.yaml for `image.*`
6. (Optional but recommended) Create a Secret in Kubernetes That Contains The Agent's `token`, or set it in values.yaml. Add your token to the file and save before creating it.

```
kubectl apply -f './mcas-siemagent-env-secrets.yaml'
```

7. Install the chart

```
helm install --name mcas-siemagent './charts/mcas-siemagent/'
# or
helm install --name mcas-siemagent hotrock/mcas-siemagent
```

Upgrade

```
helm upgrade mcas-siemagent './charts/mcas-siemagent/'
# or
helm upgrade mcas-siemagent hotrock/mcas-siemagent
```

Delete

```
helm del --purge mcas-siemagent
```

Configuration

See values.yaml

Parsing with Fluentd

Configure the SIEM Agent to forward to a fluentd `Service`, over a `port` of your choosing:

```
<source>
  @type tcp
  @log_level info
  @id in_syslog
  port 5170
  bind 0.0.0.0
  tag hotrock.mcas_siemagent
  <parse>
    @type regexp
    expression /(?<time>\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}.\d{3}Z) \w{3}:
(?<version>\d{1})\|(?<device_vendor>[^ ]+)\|(?<device_product>[^ ]+)\|(?
<device_version>[^ ]+)\|(?<signature_id>[^ ]+)\|(?<name>.+?)\|(?<severity>
(.+?))\|externalId=(?<externalId>[^ ]+) rt=(?<rt>[^ ]+) start=(?<start>[^
]+) end=(?<end>[^ ]+) msg=(?<msg>.+) suser=(?<suser>[^ ]+)
destinationServiceName=(?<Service Name>.+) cn1Label=(?<cn1Label>.+) cn1=(?
<cn1>.*) cs1Label=(?<cs1Label>.+) cs1=(?<cs1>.*) cs2Label=(?<cs2Label>.*)
cs2=(?<cs2>.*) cs3Label(?<cs3Label>.+) cs3=(?<cs3>.*) cs4Label=(?
<cs4Label>.+) cs4=(?<cs4>.*)/
  </parse>
</source>
```