



CHECK POINT SKYLINE DEPLOYMENT

June 26, 2023

Dan Schneppenheim and Nick Zeigler

Contents

Introduction	2
Requirements.....	3
Linux.....	4
Prometheus.....	4
Grafana	6
Check Point Open Telemetry	7
Setting Up Grafana Dashboards.....	8

INTRODUCTION

Skyline quickly and efficiently monitors your Check Point server with industry-standard software and protocols (OpenTelemetry, Prometheus and Grafana).

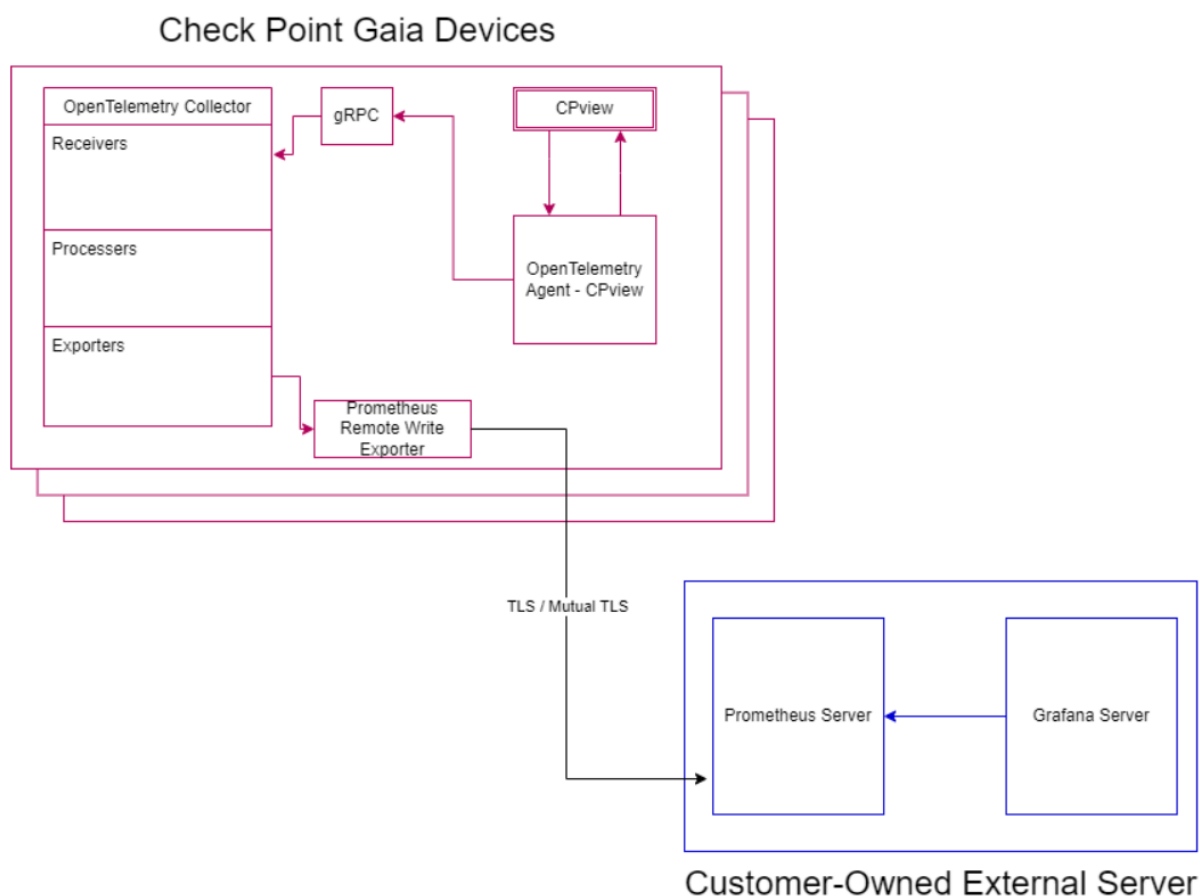
Skyline provides an OpenTelemetry CPView Agent service. The OpenTelemetry CPView Agent runs on Check Point server to collect and export health metrics from Check Point CPView tool to an external location.

There are four primary components:

OpenTelemetry CPView Agent: Runs on Check Point Servers. It is a service that queries CPView at defined intervals, collects the metrics, and exports them to an OpenTelemetry Collector.

NOTE: In this guide replace “username” with logged in user and “x.x.x.x” with the IP address of the Skyline Server.

NOTE: If you are copying and pasting the instructions, you may want to put them in a plain text document so you don't have to worry about formatting errors.



REQUIREMENTS

Server	Description
<p>Check Point Server R80.40 and higher</p>	<p>With these minimal Jumbo versions:</p> <ul style="list-style-type: none"> • Jumbo Hotfix Accumulator for R81.20 – Take 8 • Jumbo Hotfix Accumulator for R81.10 – Take 79 • Jumbo Hotfix Accumulator for R81 – Take 77 • Jumbo Hotfix Accumulator for R80.40 – Take 190 <p>Note: When enabled, the Skyline agent consumes approximately 50MB of RAM.</p>
<p>External Server to run Prometheus and Grafana</p>	<ul style="list-style-type: none"> • Prometheus <p>A third-party software the collects, stores, and queries metrics with a dedicated Timeseries Database.</p> <p>The Prometheus server exposes a Remote Write Endpoint to which data can be pushed and stores the data in its local database.</p> <p>Check Point supports Prometheus version 2.37.1 and higher.</p> • Grafana <p>A third-party software the connects to multiple data sources/databases [such as Prometheus] and visualizes the data, builds graphs, dashboards, and alerts.</p> <p>Check Point supports Grafana version 9 and higher.</p>

LINUX

In this guide we are using Linux version Ubuntu 22.04.02. Run through the standard installation and ensure that you give the system a static IP address as this will be used with the CPView Agent.

Ensure that you enable SSH on the Linux system for configuration purposes.

Ensure that you update your version of Linux completely after installation. With Ubuntu you would run the command `apt-get update` and `apt-get upgrade`.

PROMETHEUS

During this process we will download and configure Prometheus.

1. Use `wget` to download the Prometheus package.

```
wget
https://github.com/prometheus/prometheus/releases/download/v2.38.0/prometheus-2.38.0.linux-amd64.tar.gz
```

2. Next we are going to create a few required directories.

```
sudo mkdir /etc/prometheus
sudo mkdir /var/lib/prometheus
```

3. We will now extract the downloaded package using the TAR command.

```
sudo tar xvf prometheus-2.38.0.linux-amd64.tar.gz
```

4. We will now copy files from the extracted package into the directories that we created in step 2.

```
sudo cp prometheus-2.38.0.linux-amd64/prometheus /usr/local/bin/
sudo cp prometheus-2.38.0.linux-amd64/promtool /usr/local/bin/
sudo cp -r prometheus-2.38.0.linux-amd64/consoles /etc/prometheus
sudo cp -r prometheus-2.38.0.linux-amd64/console_libraries /etc/prometheus
```

5. Next create a `prometheus.yml` file in the home directory.

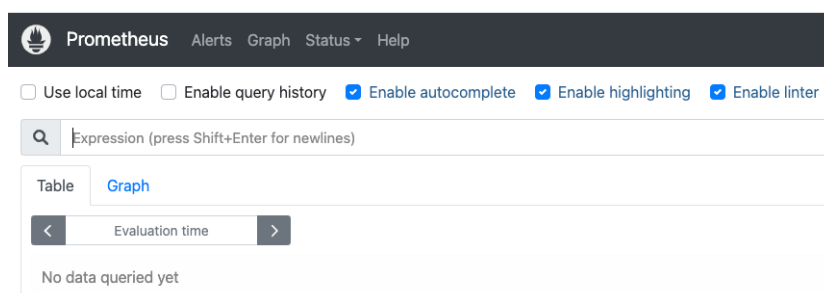
```
sudo touch ~/prometheus.yml
```

6. Start the Prometheus server with the following command. This will enable remote write to the server.

```
sudo prometheus --web.enable-remote-write-receiver
```

7. Open your web browser and navigate to Prometheus on your server ensuring you use port 9090.

```
http://x.x.x.x:9090
```



8. Once you have validated that the installation is complete you will need to CTRL-C to stop the service. In the next few steps, we will configure the service to start automatically.

9. Edit the prometheus.yml file located in /home/username/prometheus directory.
`sudo nano /home/username/prometheus-2.38.0.linux-amd64/prometheus.yml`

10. Once you have nano open, add in the following at the end of the file. Change out the x.x.x.x for the IP address of your prometheus server.

```
remote_write:
  - url: "http://x.x.x.x:9090/api/v1/write"
```

11. Next we will create the service file for Prometheus using the following commands.

```
sudo touch /etc/systemd/system/prometheus.service
sudo vi /etc/systemd/system/prometheus.service
```

12. Once vim is open, paste the following and save the file. Ensure that you change the "username" in the file paths to the logged in user.

```
[Unit]
Description=Prometheus Server
Documentation=https://prometheus.io/docs/introduction/overview/
After=network-online.target

[Service]
User=root
Restart=on-failure

ExecStart=/home/username/prometheus-2.38.0.linux-amd64/prometheus --
config.file=/home/username/prometheus-2.38.0.linux-amd64/prometheus.yml --
web.enable-remote-write-receiver

[Install]
WantedBy=multi-user.target
```

13. Next we will be setting the service to start on boot, but using the following commands.

```
sudo systemctl daemon-reload
sudo systemctl start prometheus
sudo systemctl status prometheus
sudo systemctl enable prometheus
```

14. A recommended reboot the Skyline server to ensure that everything starts a boot up.

GRAFANA

During this process we will download and configure Grafana.

1. Download and install the Grafana dependencies, as they do not get automatically installed.

```
sudo apt-get install -y adduser libfontconfig1
```

2. Download the Grafana package.

```
wget https://dl.grafana.com/enterprise/release/grafana-enterprise_10.0.0_amd64.deb
```

3. Install Grafana.

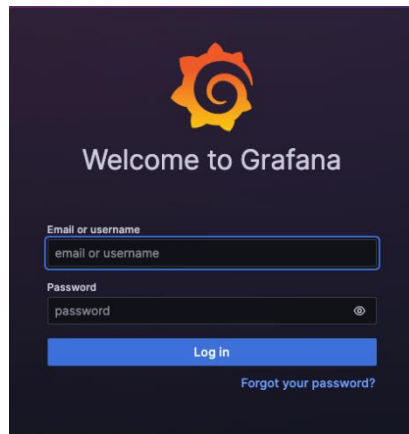
```
sudo dpkg -i grafana-enterprise_10.0.0_amd64.deb
```

4. Set Grafana to auto start with system boot using the following commands.

```
sudo /bin/systemctl daemon-reload
sudo /bin/systemctl enable grafana-server
sudo /bin/systemctl start grafana-server
```

5. Open your web browser and navigate to Grafana ensuring you use port 3000.

```
http://x.x.x.x:3000
```



6. Once you see the Grafana webpage, login with admin/admin and change the password.
7. Once you change the password. A recommended reboot your Skyline server to ensure that everything comes up smoothly.

CHECK POINT OPEN TELEMETRY

1. Login into your Check Point server and then login to “expert”

2. Use the Touch command to create the payload file.

```
touch payload-no-tls.json
```

3. Use VI and edit the payload file with the following information:

```
{
  "enabled":true,
  "export-targets": {"add": [
    {
      "enabled":true,
      "type": "prometheus-remote-write",
      "url": "http://x.x.x.x:9090/api/v1/write"
    }
  ]}
}
```

4. Run the following command to start sending CPView information to your Skyline server.

```
/opt/CPotelcol/REST.py --set_open_telemetry "$(cat payload-no-tls.json)"
```

5. You should see an output similar to this if you did everything correctly.




```
WARNING: For HTTPS/HTTP it is recommended to have both client and server
authentication(Server can be default)
{"message": "Operation has finished successfully"}
```


SETTING UP GRAFANA DASHBOARDS

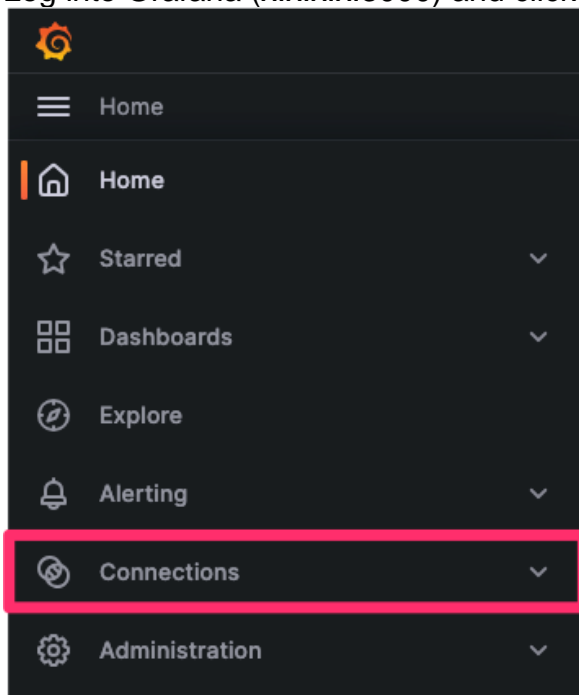
Next, we will set up the Grafana dashboards and finalize the configuration.

1. Download Granada Dashboards from sk178566.

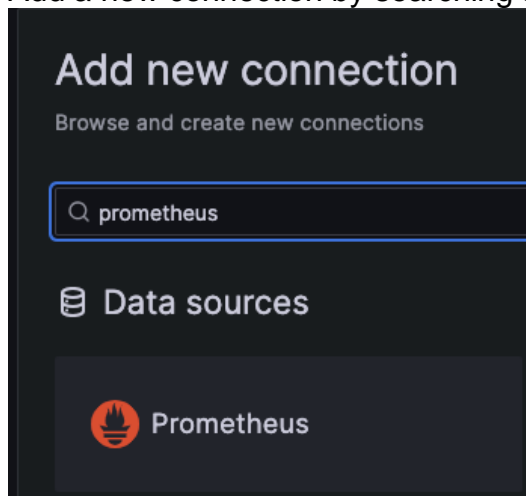
Downloads

Package Name	Download Link	Prerequisite	Release Date
Grafana Dashboards	 (TGZ)	Skyline GA	24 October 2022
Sample Payload File (no TLS)	 (JSON)	Skyline GA	28 December 2022
Sample Payload File (with TLS)	 (JSON)	Skyline GA	28 December 2022

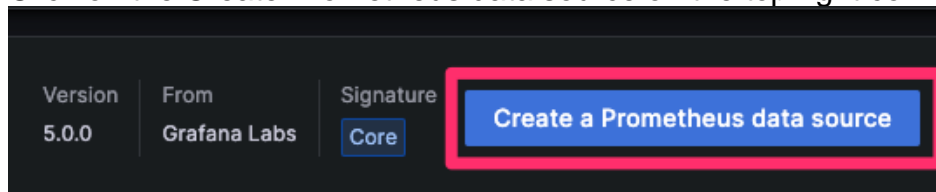
2. Unpack the TGZ file and you should have 4 files in the package. In this example we will be using the CP Dashboard – Single Machine.json file.
3. Log into Grafana (x.x.x.x:3000) and click on Connections on the menu dropdown.



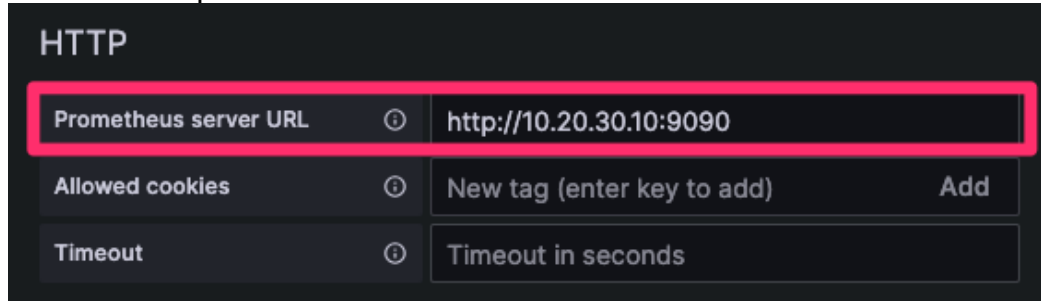
4. Add a new connection by searching and selecting Prometheus.



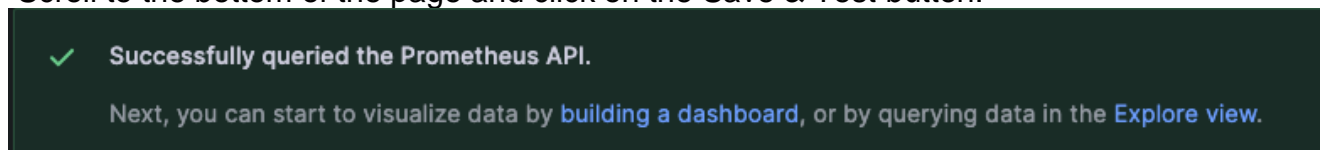
5. Click on the Create Prometheus data source on the top right corner.



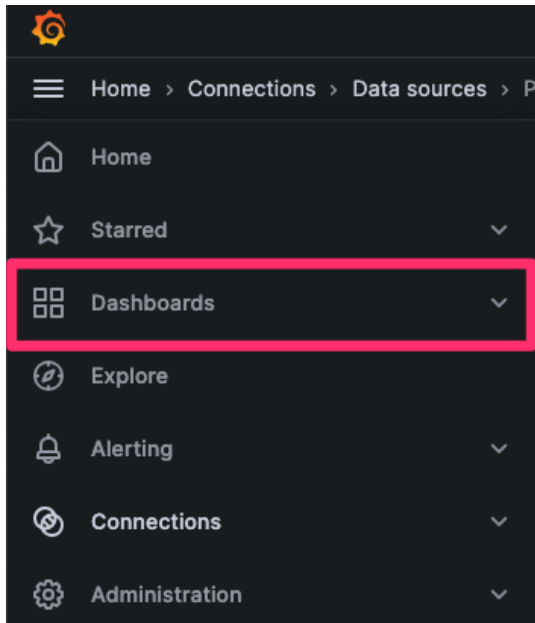
6. Add in the http information in the Prometheus server URL section.



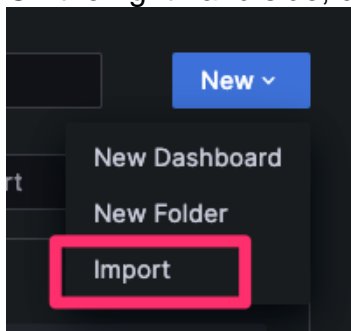
7. Scroll to the bottom of the page and click on the Save & Test button.



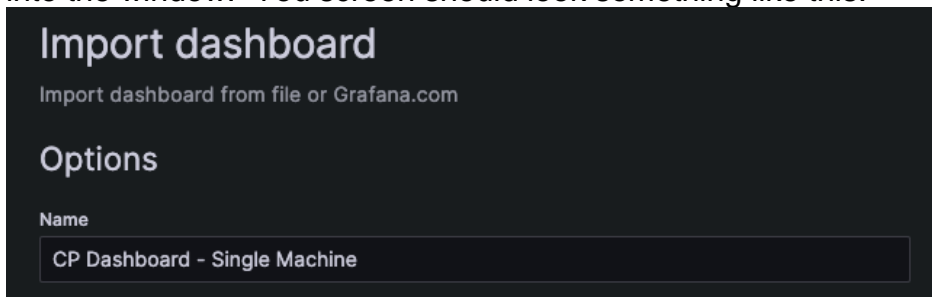
8. Next we will import the dashboard that was download from user center. Click on the menu and select Dashboards.



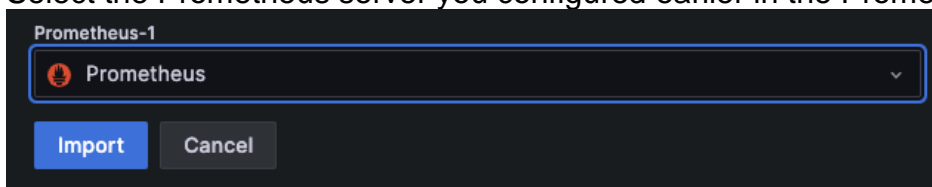
9. On the right hand side, click the New button and select Import.



10. Drag the CP Dashboard - Single Machine.json file you downloaded from usercenter into the window. Your screen should look something like this.



11. Select the Prometheus server you configured earlier in the Prometheus-1 section.



12. Click on Import.

13. If you have done everything correctly, you should see the overall system information of your Check Point device/server.

