This document will help you to pass EDR “Threat Events” to ESM with the help of Docker. Go through section [what-activity-feed-does](https://github.com/mcafee-enterprise/mvision-edr-activity-feed#what-activity-feed-does) to understand difference between “threat Event, business events and Case-management event”. Steps mentioned here will not pass Business events and Case-management events. It will only pass threat events.

**Prerequisits** : Below steps are followed in Ubuntu 21.10. These steps will work on any machines that supports Docker. We have used Trellix ESM here as example to showcase how to trasfter the events from EDR to ESM.

**Step one:** Install docker on Ubuntu box following <https://docs.docker.com/engine/install/ubuntu/> . If you are using any other OS then install docker on the box accordingly.

**Step two:** verify that docker installed correctly. You can run the command “docker images” and should see one instance running saying “helow-world” like below (ignore all other images as you won’t see them)

Graphical user interface, text

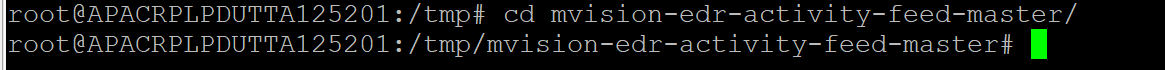
Description automatically generated

**Step 3:** Copying the Activity Feed to the Ubuntu box. I have coppied it to /tmp/ location.

Download the Activity feed following the steps mentioned in “Step 1” under [prerequisites](https://github.com/mcafee-enterprise/mvision-edr-activity-feed#prerequisites) section and copy the folder to the box.



**Step 4:** Navigate to the **“mvision-edr-activity-feed-master”** folder



**Step 5 :** Building a docker image with the ESM IP

This is the most important step. Here we will create a docker image using the ESM IP. You will need to use the below command:  
**docker build --rm --build-arg ESM\_IP=172.16.214.202 -t mvision-edr-activity-feed-tesm .**

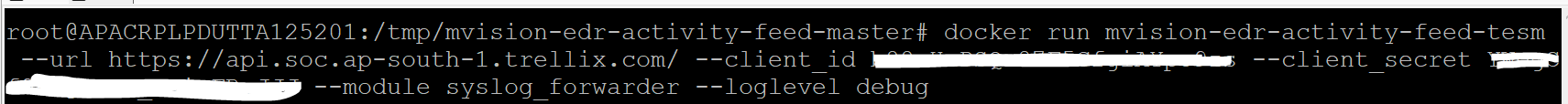
The image name here is “**mvision-edr-activity-feed-tesm”** which you can change as per your convinience. ESM\_IP is the ESM box IP. In this case Trellix ESM box IP.

**Step 6:** Generaetethethe client credential following the steps mentioned in [client-credential-generator](https://github.com/mcafee-enterprise/mvision-edr-activity-feed#client-credential-generator) section

**Steps 7:** You will need to use the below command to run the docker image we created in **“step 5”** above with the credentials created in **“step 6”**:

docker run mvision-edr-activity-feed-tesm --url https://api.soc.ap-south-1.trellix.com/ --client\_id <received from step 6> --client\_secret <received from step 6> --module syslog\_forwarder --loglevel debug

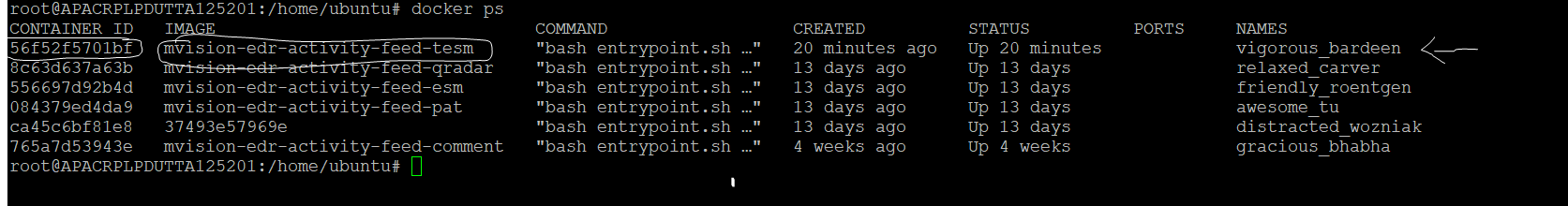
URL will be the region where your tenant is hosted. Check [URL list](https://docs.trellix.com/bundle/mvision-endpoint-detection-and-response-install-guide/page/GUID-FC03A249-0BBA-4DFC-AE5A-AF945515836C.html) to understand which URL you should use. The Tenant used here hosted in “**Asia Pacific South data center**“.



**Step 8:** verify that script started to work. You will receive below details post entering the command mentioned in step 7:

Text

Description automatically generated

**Step 9 :** Run the command “**docker ps**” to see the container ID

Example from above screenshot, **56f52f5701bf** is the container IDfor **“mvision-edr-activity-feed-tesm”**

This is all from sender side. Now the above container running Rsyslog by default and sending the traces to the ESM IP mentioned during the configuration. There is nothing else you can check on this box.

If you want to verify the settings and what been sent to Syslog you can get inside the specific container and see **/etc/rsyslog.d/30-mvision.conf** file. It will show the information like below

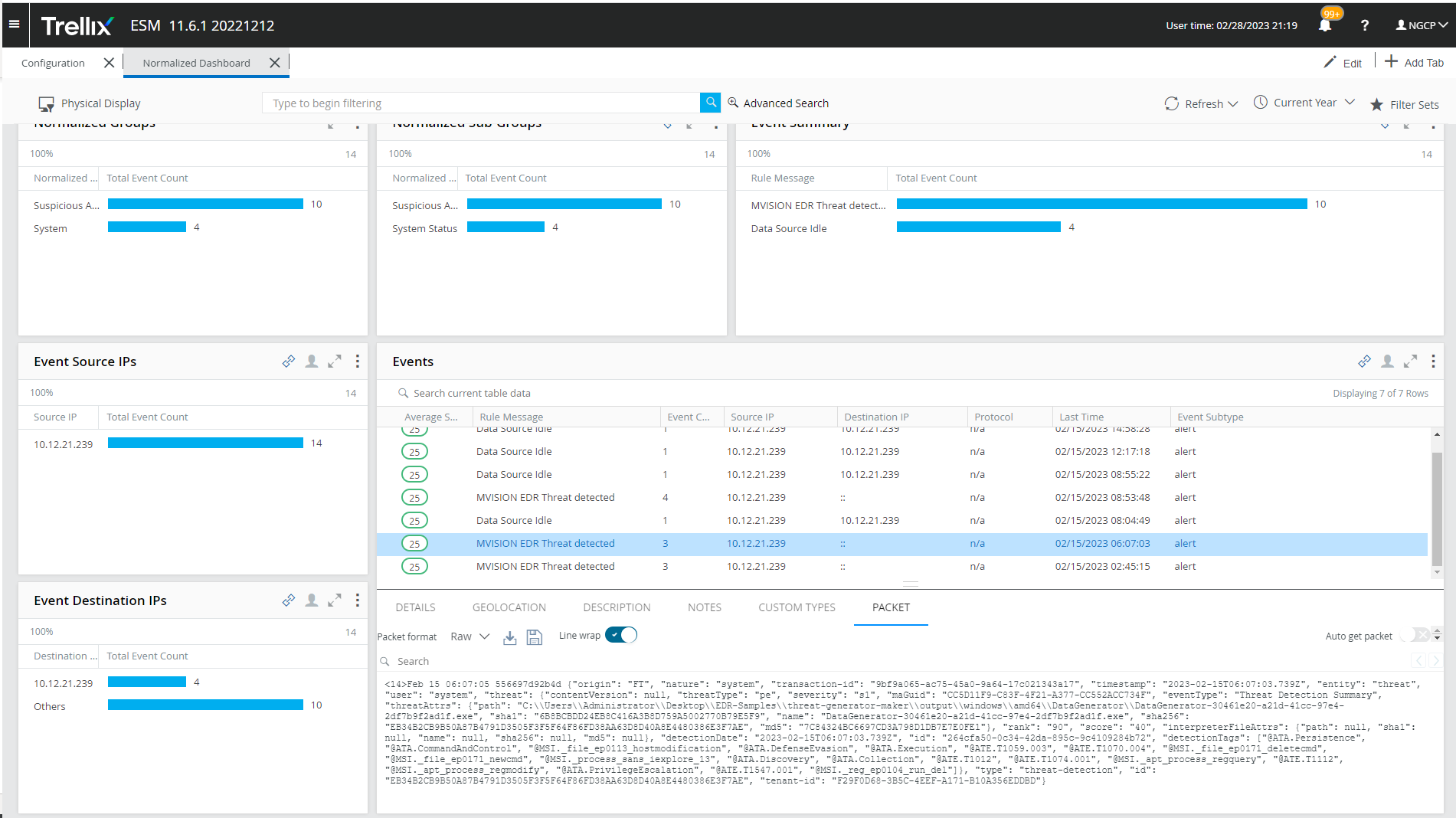
Text

Description automatically generated

**Creating receiver at ESM side:**

You will have to follow the step by step mentioned in [setup-esm-datasource](https://github.com/mcafee-enterprise/mvision-edr-activity-feed#setup-esm-datasource) section to create the receiver.

Once you have followed the steps and created the ESM data source, you should see the Threat Events like below:



Understand the [sample rule](https://github.com/mcafee-enterprise/mvision-edr-activity-feed/blob/master/RULE_MVISION_EDR_THREAT.xml) we have provided works with Trellix ESM. Depending on your ESM you will need to change that config file.