RASP

JIRA 2151

RASP Implementation

JIAR link - onejira.verizon.com/browse/NTSCS-2151

Runtime Application Self-Protection (RASP).

Monitoring & Protection for Cloud Applications. Enable Faster Vulnerability Remediation & Significantly Reduce Push Delays With Contrast! Deliver Security-as-Code. Embrace DevSecOps. Real-time Results. Self-protecting Software

Requirement - Install RASP on API servers in dev environments.

Note - Front-end Frameworks such as React.js, Vue.js, Angular.js, etc. does not require RASP

URL - <https://onesecurity.verizon.com/rasp/index.jsp>

1. Deploy RASP

Download RPM(recommended for AWS servers) files from

oneartifactoryprod.verizon.com/artifactory/GX4V\_AppSec\_GTS/rasp/rv4/2/jee/rpm/rasprpmel6.rpm

save in /apps/opt/rasp

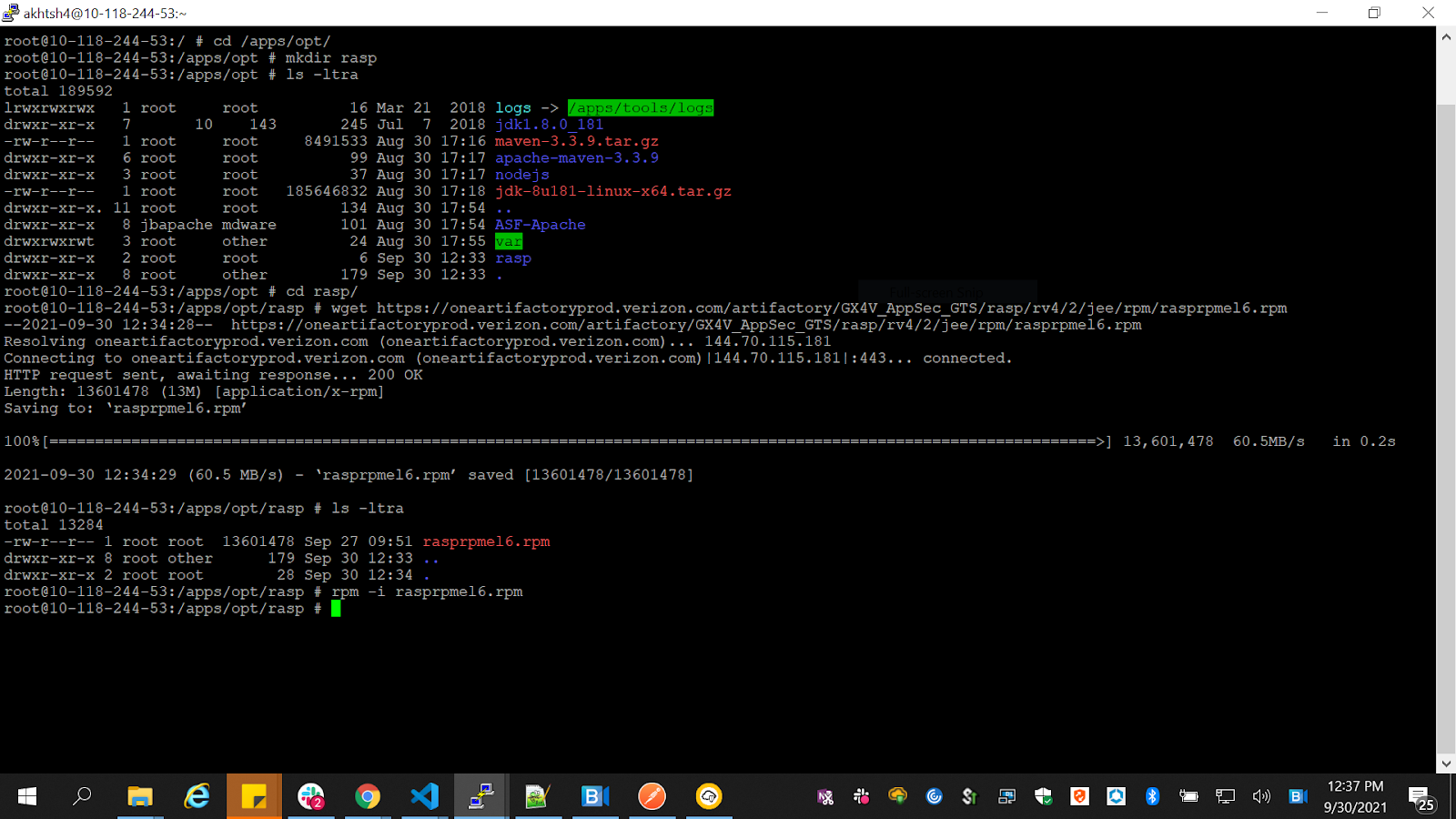
# cd /apps/opt

# mkdir rasp

# cd rasp

# wget oneartifactoryprod.verizon.com/artifactory/GX4V\_AppSec\_GTS/rasp/rv4/2/jee/rpm/rasprpmel6.rpm

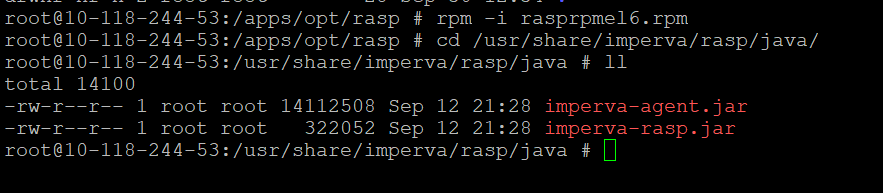
# rpm -i  rasprpmel6.rpm



It will create /usr/share/imperva/rasp/java/

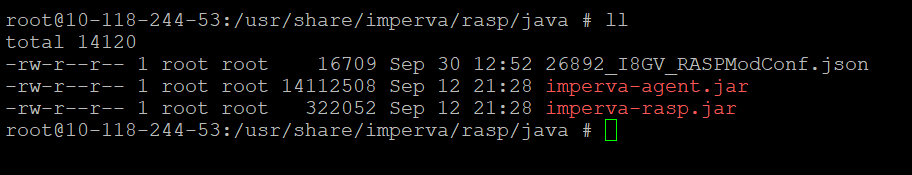
folder and create 2 files

1. Imperva-agent.jar
2. Imperva-rasp.jar



Copy file  26892\_I8GV\_RASPModConf.json in

/usr/share/imperva/rasp/java/



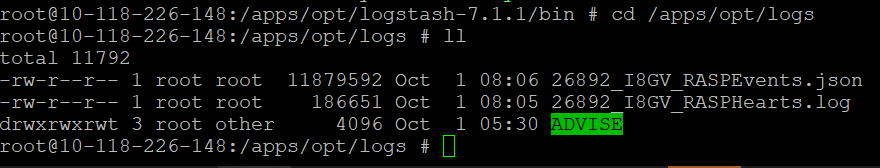
Command to run RASP

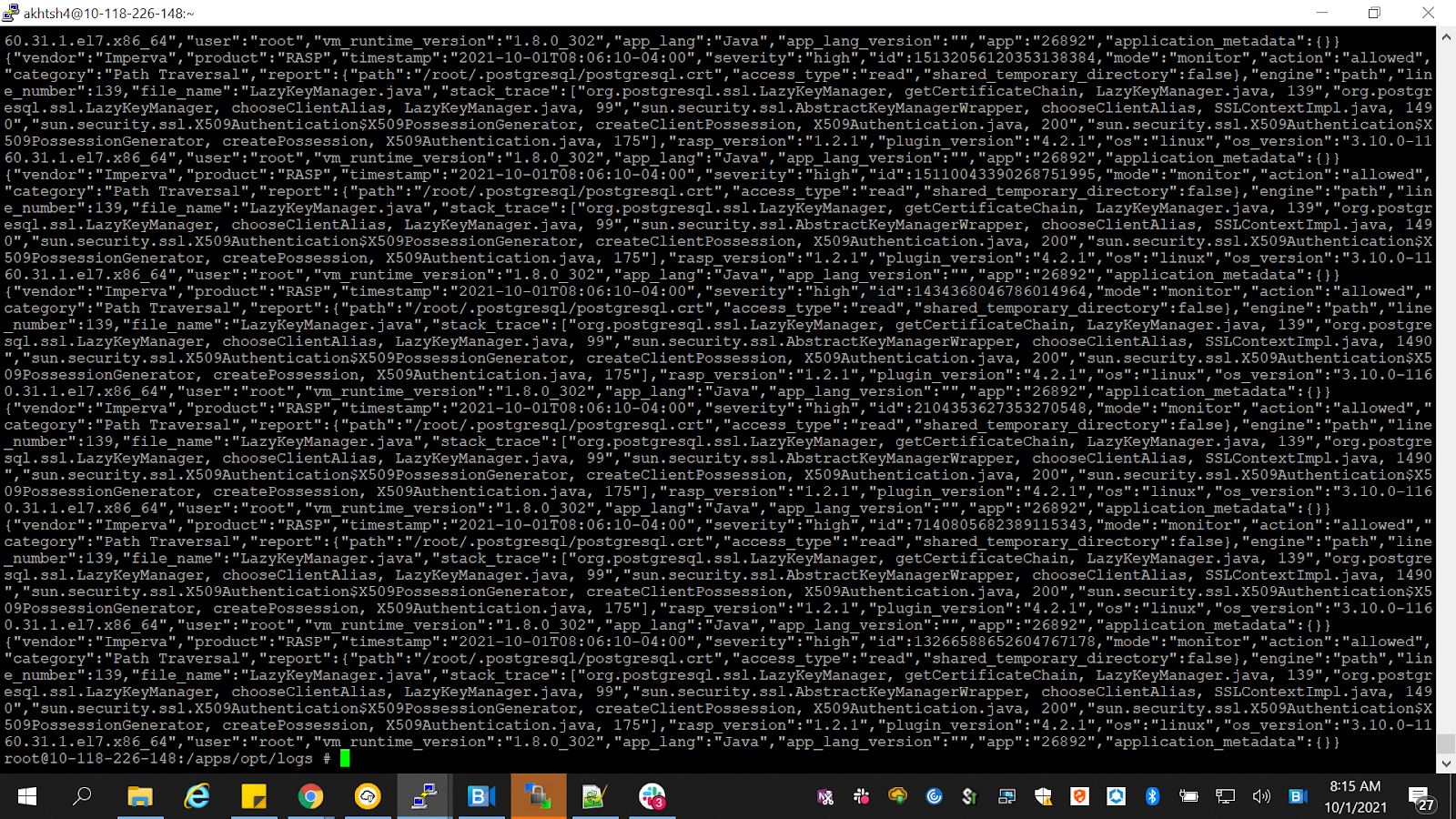
cd /apps/opt/vendoruserservice

nohup java -javaagent:/usr/share/imperva/rasp/java/imperva-agent.jar -Dimperva.raspjarpath=/usr/share/imperva/rasp/java/imperva-rasp.jar -Dimperva.config=/usr/share/imperva/rasp/java/26892\_I8GV\_RASPModConf.json -Dimperva.disable\_csrf -Dimperva.disable\_http -jar vendoruserservice.jar &

Check the logs in 2 files created

/apps/opt/logs





Sending logs to the splunk dashboard

1. Downloaded rasp\_logship\_aws\_np.zip from oneartifactory using this link: https://oneartifactoryprod.verizon.com/ui/repos/tree/General/GX4V\_AppSec\_GTS%2Frasp%2Flogshipping%2Frasp\_logship\_aws\_np.zip

The unzipped file's directory is: /usr/share/imperva/rasp/rasp\_logship\_aws\_np/

2. Updated the following params in rasp\_logship\_aws\_np.conf file

path => ["/apps/opt/logs/26892\_I8GV\_RASPEvents.json"]

add\_field => {"source" => "/apps/opt/logs/26892\_I8GV\_RASPEvents.json"}

if [path] == "/apps/opt/logs/26892\_I8GV\_RASPEvents.json" {

add\_field => {"VSAD\_ID" => "I8GV"}

add\_field => {"vast\_id" => "26892"}

jaas\_path => "/usr/share/imperva/rasp/rasp\_logship\_aws\_np/kafka-jaas.conf"

kerberos\_config => "/usr/share/imperva/rasp/rasp\_logship\_aws\_np/krb5.conf"

ssl\_truststore\_location => "/usr/share/imperva/rasp/rasp\_logship\_aws\_np/truststore.jks"

3. Updated the following param in kafka-jaas.conf file

keyTab="/usr/share/imperva/rasp/rasp\_logship\_aws\_np/svc-omg\_secagen\_pprd.keytab";

4. update password in the rasp\_logship\_aws\_np.conf file

 {password is in separate file in the folder /usr/share/imperva/rasp/rasp\_logship\_aws\_np/ truststore\_nonprod\_password.txt  }

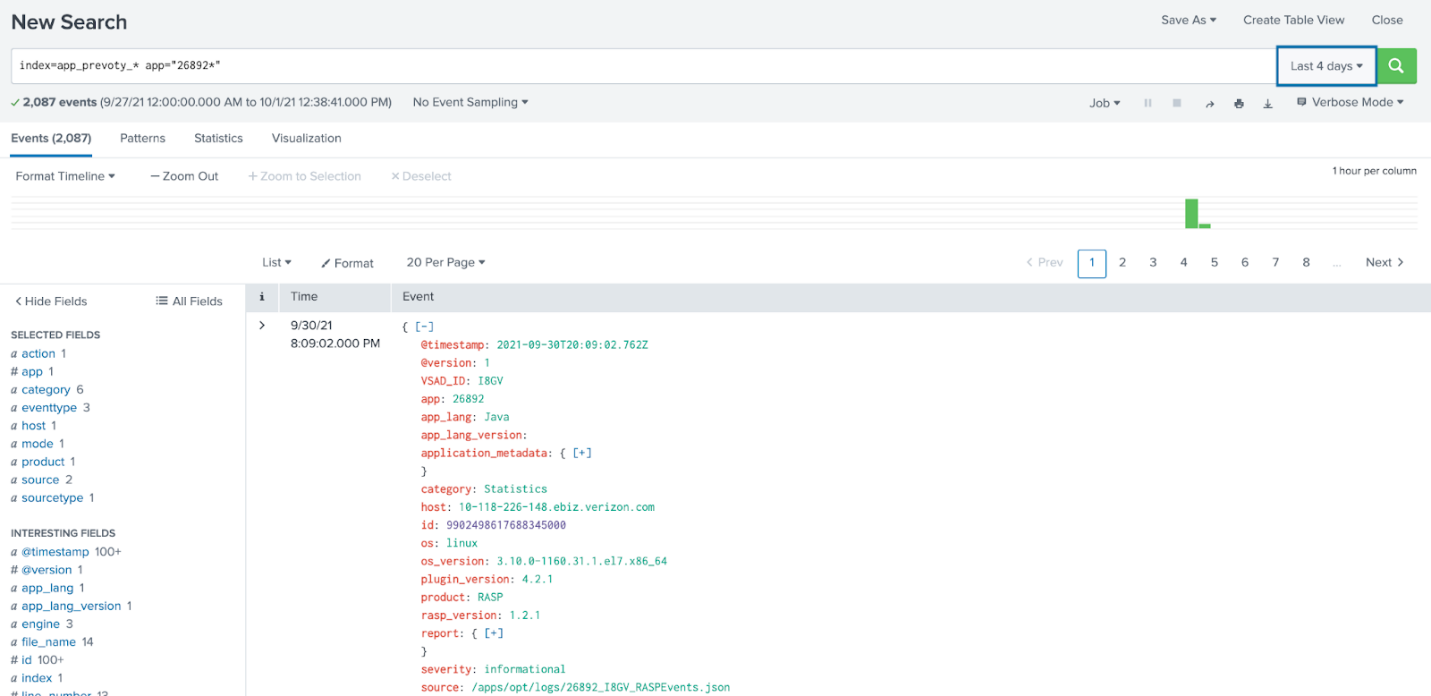
 #cd /apps/opt/logstash-7.1.1/bin

 # ./logstash -f /usr/share/imperva/rasp/rasp\_logship\_aws\_np/rasp\_logship\_aws\_np.conf --path.data=data/prevoty

Logs in Splunk dashboard

<https://awsnplogsearch1.ebiz.verizon.com:8000/>

Search string  - index=i8gv\_pr sourcetype="Prevoty-JSON" app="26892"



**Error Scenario**

If the logs are not shipping to splunk dashboard

Follow the following steps

* First,  run your Logstash stop script,
* Then take the last line from the RASPEvents.json log and put it by itself in the same directory, name it something like "test.json"
* then go back into your logstash config, and change from "RASPEvents.json" to "test.json"
* Then run your Logstash start script
* Check to see if it made it to Splunk, if yes, you stop Logstash again and change it back from "test.json" to "RASPEvents.json" (or whatever yours is named)

[10:35](https://vz-gnt.slack.com/archives/D02B5GYF064/p1635258920014600)

* Switching it to another file and back seems to "unstick" the flow of logs in some instances

Once RASP configuration in production is up, the application will be taken down in non-prod.

<https://awslogsearch1.vpc.verizon.com:8000/en-US/account/login?return_to=%2Fen-US%2F>

Above url is for accessing splunk

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_