CA Spectrum Modsecurity update.

Correcting high number of log-entries and enable Heartbeat/alive-logic for OC-Console.

The following adjustments are done in CA Spectrum OC-webserver – here to the enabled ApacheModSecurity webfirewall service. The file edits/modification needs to be adjusted/edited while Apache Service is stopped. So clearly first ensure: Stop down the Apache and OC-Tomcat service – and find reconfiguration info per below advise.

Editing the file:

`./apache/modsecurity-crs/activated_rules/`**`whitelist.conf`**

Modify the file to cover entries as follows (full file content):

```
<LocationMatch /spectrum/restful/.*>
        <IfModule mod_security2.c>
                SecRuleRemoveById 960032
                SecRuleRemoveById 981260
                SecRuleRemoveById 981173
                SecRuleRemoveById 981205
                SecRuleRemoveById 970901
                SecRuleRemoveById 950006
        </IfModule>
</LocationMatch>

<LocationMatch /spectrum/webclient/tsperspectives/.*>
        <IfModule mod_security2.c>
                SecRuleRemoveById 960010
        </IfModule>
</LocationMatch>
```

ENABLE HeartBeat for OC-Console:

The following file edits/modification needs to be adjusted/edited for an active Heartbeat. Clearly first ensure: Stop down the Apache and the OC-Tomcat service – and find files per below advise.

Now - editing the file:

`./apache/modsecurity-crs/`**`modsecurity_crs_10_setup.conf`**

and **add to the end one single line** containing: `SecDataDir /spectrum/apache/tmp`

This then looks like:

```
.....
..
SecRule &TX:REAL_IP "@eq 0" \
  "id:'900021', \
  phase:1, \
  t:none, \
  initcol:global=global, \
  initcol:ip=%{remote_addr}_%{tx.ua_hash}, \
  setvar:tx.real_ip=%{remote_addr}, \
  nolog, \
  pass"

SecDataDir /spectrum/apache/tmp
```

Next - editing the file:

`./apache/modsecurity-crs/base_rules/`**`modsecurity_crs_50_outbound.conf`**

Here to comment out SecRule in dir/file: ./apache/modsecurity-crs/base_rules/modsecurity_crs_50_outbound.conf

Find and edit:

```
# The application is not available
SecRule RESPONSE_STATUS "^5\d{2}$" "phase:4,rev:'2',ver:'OWASP_CRS/2.2.9',maturity:'9',..
SecRule RESPONSE_BODY "(?:Microsoft OLE DB Provider for SQL Server(?:<\/font>.{1,20} ..
```

.. and modify to:

```
# The application is not available
# SecRule RESPONSE_STATUS "^5\d{2}$" "phase:4,rev:'2',ver:'OWASP_CRS/2.2.9',maturity:'9',..
SecRule RESPONSE_BODY "(?:Microsoft OLE DB Provider for SQL Server(?:<\/font>.{1,20} ..
```

Next - editing the file:

`./apache/modsecurity-crs/base_rules/`**`modsecurity_crs_60_correlation.conf`**

Here to comment out SecRule in dir/file: /apache/modsecurity-crs/base_rules/modsecurity_crs_60_correlation..conf

Here find and edit:

```
SecRule TX:INBOUND_ANOMALY_SCORE "@ge %{tx.inbound_anomaly_score_level}" \
"phase:5,id:'981204',t:none,log,noauditlog,pass,msg:'Inbound Anomaly Score Exceeded ..

SecRule TX:OUTBOUND_ANOMALY_SCORE "@ge %{tx.outbound_anomaly_score_level}" \
"phase:5,id:'981205',t:none,log,noauditlog,pass,msg:'Outbound Anomaly Score Exceeded ..

SecMarker END_CORRELATION
```

Comment out line:

```
# SecRule TX:OUTBOUND_ANOMALY_SCORE "@ge %{tx.outbound_anomaly_score_level}" \
"phase:5,id:'981205',t:none,log,noauditlog,pass,msg:'Outbound Anomaly Score Exceeded ..
```

Avoiding error messages reported to ./apache/logs/error.log claiming about IP or Global database missing:

Create missing directory and create files:

By default install the `$SPECROOT/apache/tmp` directory (and subdirectory) is maybe missing. Create this directories and add some files.

So once `./apache/tmp` and `./apache/tmp/global` plus `./apache/tmp/ip` is created and fine for access – create the following files by using the “`touch`” tool (native Linux in a shell / or for Windows using “bash -login” shell) . The files are created “empty” with "0" bytes. Filenames are as follows – these are case-sensitive (see sample below):

```
touch ./global/global.dir
touch ./global/global.pag
touch ./ip/ip.dir
touch ./ip/ip.pag
```

```
[specadm@spectro101 tmp]$ ls -laRt
.:
drwxrwxr-x.  2 specadm specadm 4096 May 11 21:12 ip
drwxrwxr-x.  2 specadm specadm 4096 May 11 21:12 global

./ip:
-rw-rw-r--. 1 specadm specadm    0 May 11 21:14 ip.dir
-rw-rw-r--. 1 specadm specadm    0 May 11 21:14 ip.pag

./global:
-rw-rw-r--. 1 specadm specadm    0 May 11 21:15 global.dir
-rw-rw-r--. 1 specadm specadm    0 May 11 21:14 global.pag
```

Once this config is done - start the Apache and the Tomcat - wait for service startup is completed.