SMS and EPM log integration using SmartLog

Derek O'Flynn
SE Louisiana
Rev. 1

For customers that are utilizing a SMS for gateways and SmartLog/SmartEvent integration adding Endpoint requires connecting to multiple consoles to view and respond to log data. This paper allows configuration of the primary SMS to read logs from EPM for less complexity. Information below references sk35288 (Step1) but this paper focuses on EPM integration specifically.

Architecture

- Primary Management and SmartEvent Server for Perimeter
  - Name - gw-00434b
  - IP - 192.168.1.8
- Endpoint Management Server
  - Name - gw-00434c
  - IP – 192.168.1.9

Setup LEA connection on EPM using SmartConsole

- Create a new host
  - New Object -> Host
  - Name - SmartEvent_host
  - IPv4 - 192.168.1.8
  - Publish
- Add a new OPSEC application
  - New Object -> More -> Server -> OPSEC -> Application
    - Name - SmartEvent_server
    - Host – Select SmartEvent_host
    - Client Entities - LEA
    - Click on Communication
    - Enter activation key and initialize
    - Under LEA Permissions
      - Show all log fields
    - Install Database

Setup SmartLog to index EPM logs

- SSH into the SmartEvent Server (eg. 192.168.1.8)
- cd $INDEXERDIR
- Run the opsec pull command
  - ./opsec_pull_cert -h <IP_address_of_Host> -n <OPSec-Application-Name> -p <Activation-Key> -o <Name-of-Certificate-File>
  - ./opsec_pull_cert -h 192.168.1.9 -n SmartEvent_server -p admin123 -o SmartEvent_cert.p12
- Edit the log_indexer_custom_settings.conf file

©2019 Check Point Software Technologies Ltd. All rights reserved

- Find “log_servers” and modify it to look like the following

```
:log_servers (
        : (
        :name (127.0.0.1)
        :uuid ()
        :log_files (all)
        :folder ("/opt/CPsuite-R80/fw1/log")
        :is_local (true)
        :read_mode (FILES)
        )

        : (
        :name (192.168.1.9)
        :log_files (all)
        :is_local (false)
        :certificate_file (SmartEvent_cert.p12)
        :sic_name_client ("CN=SmartEvent_server,O=gw-00434c..2ka3tf")
        :sic_name_server ("CN=cp_mgmt,O=gw-00434c..2ka3tf")
        :read_mode (LEA)
        )
```

- Run stopIndexer;startIndexer

Notes

- If you have errors in your logs such as cannot read LEA error, most likely your sic_name_client or sic_name_server is incorrect. Make sure that sic_name_client matches the OPSEC DN on the EPM. Then sic_name_server only CN=cp_mgmt is modified. O=should match on both as this is the internal_ca of the EPM.
- If you have to adjust this after an initial run, you will need to reset the trust on the OPSEC object, and then opsec_pull a new cert.