SOC-Connector Quickstart-Anleitung

DFN-CERT

Inhaltsverzeichnis

1 SOC-Connector Quickstart-Anleitung

Dieses Dokument listet die wichtigsten Schritte in sehr knapper Form auf, mit denen der SOC-Connector in Betrieb genommen werden kann.

Eine ausführliche Anleitung ist zusätzlich verfügbar.

1.1 Inbetriebnahme des SOC-Connectors

- Benötigt wird ein Linux-Host (oder VM) mit vorinstalliertem Container-Manager Podman 4.x
- Installation als User `soc` in leerem Verzeichnis `/home/soc/soc-connector/`
- Das Script `soc-connector.sh` Download sowie das erhaltene SOC-Access-Zertifikat mit Schlüssel in dieses Verzeichnis kopieren.
- SOC-Connector einrichten:
  - `./soc-connector.sh setup`
  - Der Setup muss ohne Fehler durchlaufen!
- Status prüfen:
  - `./soc-connector.sh status`
  - SOC-Connector ist jetzt im Modus `stage`!
- SOC-Connector für Tests starten:
  - `./soc-connector.sh start`
  - Der SOC-Connector erwartet nun auf Port `1514` per TCP übertragene Meldungen in Syslog-Format/Protokoll.
  - Im Modus `stage` werden diese Daten nur an den SOC-Incubator übertragen, nicht analysiert und nur kurzzeitig gespeichert!
- Einfachen, automatischen Test starten:
  - `./soc-connector.sh test`
  - Ein paar automatisch erzeugte Logzeilen werden an den SOC-Incubator übertragen und es wird auf eine Eingangsbestätigung gewartet.
  - Dieser Test sollte erfolgreich durchlaufen. Beim ersten Start kann es zu Timeouts kommen, dann bitte nochmals ausführen.
- Umfassenden Test mit eigenen Log-Meldungen starten:
  - `./soc-connector.sh sample` - jederzeit mit `<Ctrl-C>` beenden.
  - Eingehende Meldungen werden an den SOC-Incubator übertragen und in JSON-Format zurück an den SOC-Connector geschickt, um prüfen zu können, ob und in welcher Struktur die Meldungen ankommen.
  - Bitte genau prüfen, ob die Felder der bestätigten Meldung korrekt erkannt wurden.
  - Insbesondere Zeitstempel (`timestamp`) und eigentlicher Meldungstext (`body`) müssen korrekt sein.
- SOC-Connector stoppen:
  - `./soc-connector.sh stop`

1.2 Betrieb des SOC-Connectors

- Wenn Setup und Tests erfolgreich waren, kann der Produktiv-Modus aktiviert werden:
  - `./soc-connector.sh deploy`
  - Der SOC-Connector wechselt dadurch in den Produktiv-Modus.
- Status prüfen:
  - `./soc-connector.sh status`
  - SOC-Connector ist jetzt im Modus `production`!
- SOC-Connector für den Produktivbetrieb starten:
  - `./soc-connector.sh start`
  - Der SOC-Connector erwartet nun auf Port `1514` per TCP übertragene Meldungen in Syslog-Format/Protokoll.
  - Im Produktiv-Modus werden die eingehenden Meldungen an die DFN.Security SOC-Infrastruktur gesendet. Dort werden die Daten gemäSS Datenschutzbestimmungen und vertraglichen Vereinbarungen verarbeitet und temporär gespeichert.
- SOC-Connector stoppen:
  - `./soc-connector.sh stop`

1.3 Wartung des SOC-Connectors

- Konfiguration erneuern oder ändern:
  - `./soc-connector.sh setup`
  - Das Setup-Kommando kann jederzeit ausgeführt werden, wenn der SOC-Connector gestoppt ist, um die Grundkonfiguration zu ändern. Zu beachten ist, dass der SOC-Connector nach dem Setup grundsätzlich im `stage`-Modus ist und erneut manuell in den Produktiv-Modus versetzt werden muss. Nach erfolgreicher Durchführung aller Tests.
- Container-Image aktualisieren:
  - `./soc-connector.sh update`
  - Auch nach einem Update befindet sich der SOC-Connector grundsätzlich im `stage`-Modus.
- SOC-Connector entfernen:
  - `./soc-connector.sh stop` - Stop des SOC-Connectors
  - `./soc-connector.sh delete` - Löschen des Containers
  - `./soc-connector.sh purge` - Löschen des Container-Images
  - `rm -rf setup conf logs` - Löschen aller Unterverzeichnisse