zhmc-log-forwarder

A log forwarder for the IBM Z HMC

Andreas Maier
Juergen Leopold

2019-08-15

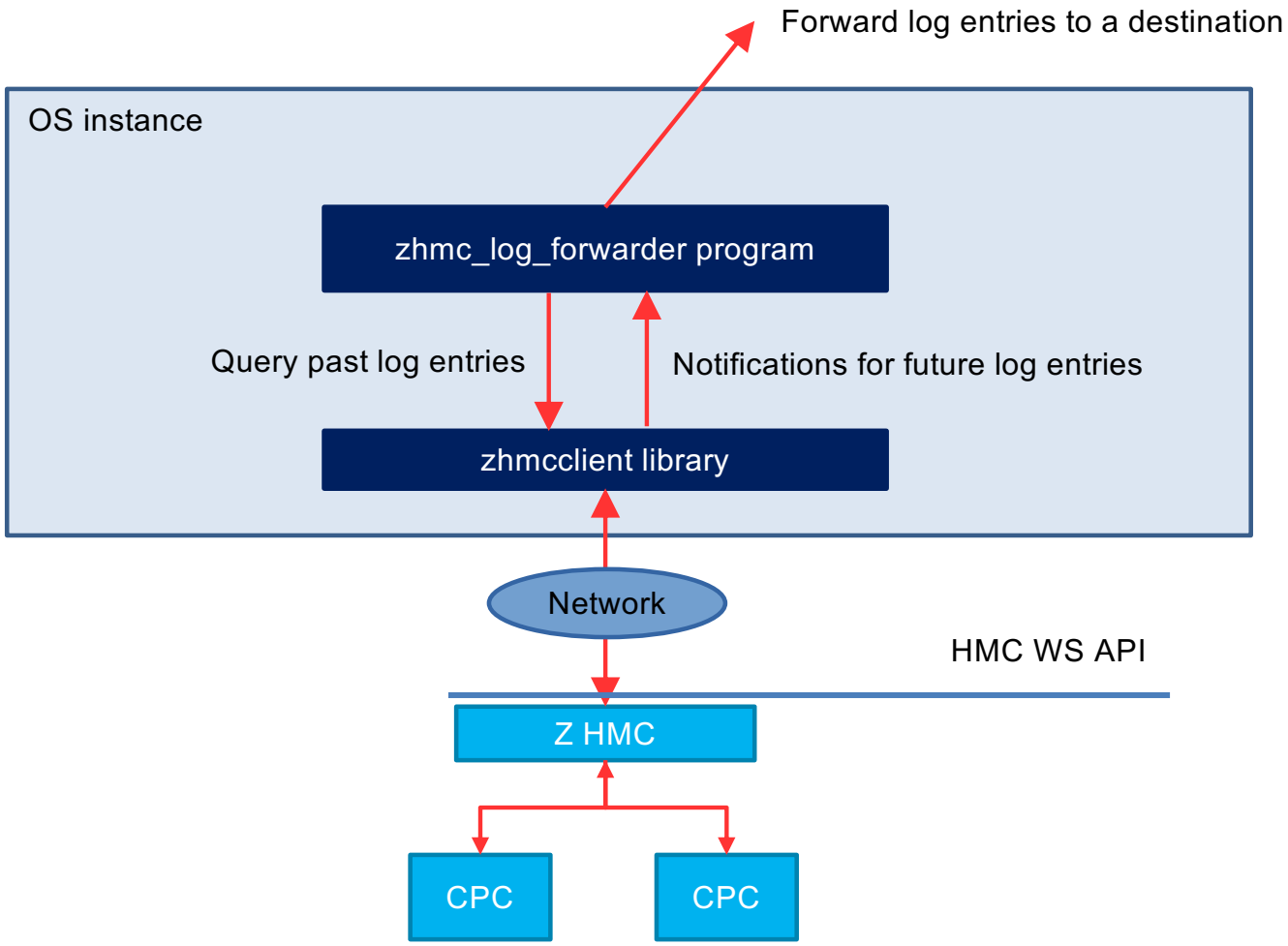
Problem Statement

- The Z HMC maintains an audit log and a security log
- Accessible in HMC GUI and HMC Web Services API
- However: The HMC does not support forwarding these logs to SIEM(1) services such as QRadar

→ zhmc-log-forwarder can be used for that purpose

(1) SIEM = Security Information and Event Management

Architecture



Availability and Functionality

- Pure Python program, running on any OS and on Python 2.7 and 3.4 or higher
- Future: Available as ‘zhmc-log-forwarder’ package on Pypi:

```
$ pip install zhmc-log-forwarder
```

- Supports selecting audit log, security log, or both
- Supports selecting a time since when log entries are collected
  - keywords ‘now’, ‘all’, or a specified date & time string
- Supports selecting whether to wait for future log entries
- Supports selecting one or more destinations: stdout, stderr, syslog
  - Note: A remote syslog server is used for Qradar
- Supports custom formatting the output for log entries

zhmc_log_forwarder command

```
Usage:

  zhmc_log_forwarder [options]

General options:

  -h, --help            Show this help message and exit.
  --help-config-file    Show help about the config file format and exit.
  --help-log-format     Show help about the log message formatting and exit.
  --help-time-format    Show help about the time field formatting and exit.
  --version             Show the version number of this program and exit.
  --debug               Show debug self-logged messages (if any).

Config options:

  -c,--config-file CONFIGFILE    File path of the config file to use.
```

Config file (1)

YAML format:

```
---
# Which Z HMC to collect the log entries from:

hmc_host: 10.11.12.13.      # IP address or hostname of the HMC
hmc_user: myuser            # HMC userid
hmc_password: mypassword    # HMC password
label: region1-zone2-hmc1   # Label for use in log output to identify the source

# Time range for log entries to collect:

since: now                  # Include past log entries since when: all, now, date&time string
future: true                # Wait for future log entries

# Logging for the program itself:

selflog_dest: stdout                            # Destination (stdout, stderr)
selflog_format: '%(levelname)s: %(message)s'    # Log message format (Python logging placeholders)
selflog_time_format: '%Y-%m-%d %H:%M:%S'        # Format of 'asctime' field in log message
```

Config file (2)

```
# List of log forwardings.
# A log forwarding defines a set of logs to collect and a destination to forward them to.

forwardings:

- name: Example forwarding   # Name of the forwarding
  logs: [security, audit]    # List of log types to include
  dest: syslog               # Destination for the log entries: stdout, stderr, syslog

  syslog_host: 10.11.12.14   # IP address or hostname of remote syslog server
  syslog_port: 514           # Port number of remote syslog server
  syslog_porttype: udp       # Port type of remote syslog server
  syslog_facility: user      # Syslog facility name

  format: '{time:32} {label} {log:8} {name:12} {id:>4} {user:20} {msg}'  # Log message format
  time_format: '%Y-%m-%d %H:%M:%S.%f%z'                                  # Format for 'time' field
```

Log message format

Example:

```
format: '{time:32} {label} {log:8} {name:12} {id:>4} {user:20} {msg}'
```

Supported fields:

`time`: Time stamp of the log entry. Format can be customized.
`label`: Label identifying the HMC the logs came from.
`log`: HMC Log: security, audit.
`name`: Name of the log entry.
`id`: ID of the log entry.
`user`: HMC userid associated with the log entry.

`msg`: Fully formatted log message, in English.
`msg_vars`: Substitution variables used in the log message

`detail_msgs`: List of fully formatted detail log messages, in English.
`detail_msgs_vars`: Substitution variables used in the detail log messages.

Example output

```
$ zhmc_log_forwarder -c dal13-01.config.yml
2019-08-13 09:28:37 zhmc_log_forwarder INFO zhmc_log_forwarder starting
2019-08-13 09:28:37 zhmc_log_forwarder INFO zhmc_log_forwarder version: 0.5.1.dev7
2019-08-13 09:28:37 zhmc_log_forwarder INFO HMC: 172.18.0.15, Userid: zbcInstall, Label: dal13-01-hmc1
2019-08-13 09:28:37 zhmc_log_forwarder INFO Since: now (2019-08-13 …), Future: True
2019-08-13 09:28:37 zhmc_log_forwarder INFO Forwarding: 'Testing RFC5424 format'; Logs: security, audit;
                                            Destination: syslog (server 10.74.145.195, port 514/tcp, facility user)
2019-08-13 09:28:37 zhmc_log_forwarder INFO Collecting these logs altogether: audit, security
2019-08-13 09:28:39 zhmc_log_forwarder INFO Starting to wait for future log entries
^C
2019-08-13 09:29:11 zhmc_log_forwarder INFO Keyboard interrupt - stopping to wait for future log entries
2019-08-13 09:29:11 zhmc_log_forwarder INFO Closing notification receiver
2019-08-13 09:29:11 zhmc_log_forwarder INFO Logging off from HMC
2019-08-13 09:29:11 zhmc_log_forwarder INFO zhmc_log_forwarder stopped
```

Log entries in destination (e.g. RFC5424 syslog format):

```
Aug 13 09:28:37 dal13-01-hmc1 [id="1941" type="Security" user="zbcInstall"] User zbcInstall has logged on to W…
Aug 13 09:28:46 dal13-01-hmc1 [id="6055" type="Audit" user=""] A web services client on 10.74.103.97 attempted…
Aug 13 09:28:54 dal13-01-hmc1 [id="1691" type="Security" user=""] User zbcInstall has attempted to log on from…
Aug 13 09:28:56 dal13-01-hmc1 [id="6055" type="Audit" user=""] A web services client on 10.74.103.97 attempted…
Aug 13 09:29:04 dal13-01-hmc1 [id="1941" type="Security" user="zbcInstall"] User zbcInstall has logged on to W…
```

Log message formats

- **RFC3164 format (aka BSD style syslog):**

  Config:

```
format: '<14>{time} {label} {log}: {id} {user} {msg}'
time_format: '%b %d %H:%M:%S'
```

  Example log message:

```
<14>Aug 15 10:23:04 dal13-01-hmc1 security: 1942 zaasmoni User zaasmoni has logged off from Web …
```

- **RFC5424 format:**

  Config:

```
format: '<14> 1 {time} {label} HMC - {id} [cat="{log}" usrName="{user}"] {msg}'
time_format: '%b %d %H:%M:%S'
```

  Example log message:

```
<14> 1 Aug 15 10:23:04 dal13-01-hmc1 HMC - 1942 [cat="security" usrName="zaasmoni"] User zaasmoni
  has logged off from Web …
```

- **QRadar LEEF format:**

  Config:

```
format: '{time} {label} LEEF:1.0|IBM|HMC|2.14.1|{id}|cat={log}\tdevTime={time}\t
         devTimeFormat=MMM dd yyyy HH:mm:ss\tusrName={user}\t{msg}'
time_format: '%b %d %Y %H:%M:%S'
```

  Example log message:

```
2019-08-15 10:23:04 dal13-01-hmc1 LEF:1.0|IBM|HMC|2.14.1|1942|cat=security\t
  devTime=Aug 15 2018 10:23:04\tdevTimeFormat=MMM dd yyyy HH:mm:ss\t
  usrName=zaasmoni\tUser zaasmoni has logged off from Web …
```

IBM QRadar service

- Supported formats of incoming log messages:
  - RFC3164, RFC5424 syslog formats (with deviations)
  - QRadar LEEF format
- QRadar needs a DSM parser for the log source
  - Without a DSM parser, the log message is handled by the generic DSM parser, which treats the entire log message as text
- Possible staging:
  - Stage 0: Generic DSM parser
  - Stage 1: XML defined parsing rules for generic DSM parser
  - Stage 2: Specific DSM parser for HMC, and HMC messages in QRadar message inventory
  - Only stage 2 allows recognizing specific messages and their parameters, e.g. alerting based on invalid login attempt.