zhmc-log-forwarder

A log forwarder for the IBM Z HMC

Andreas Maier
Juergen Leopold

2019-08-07

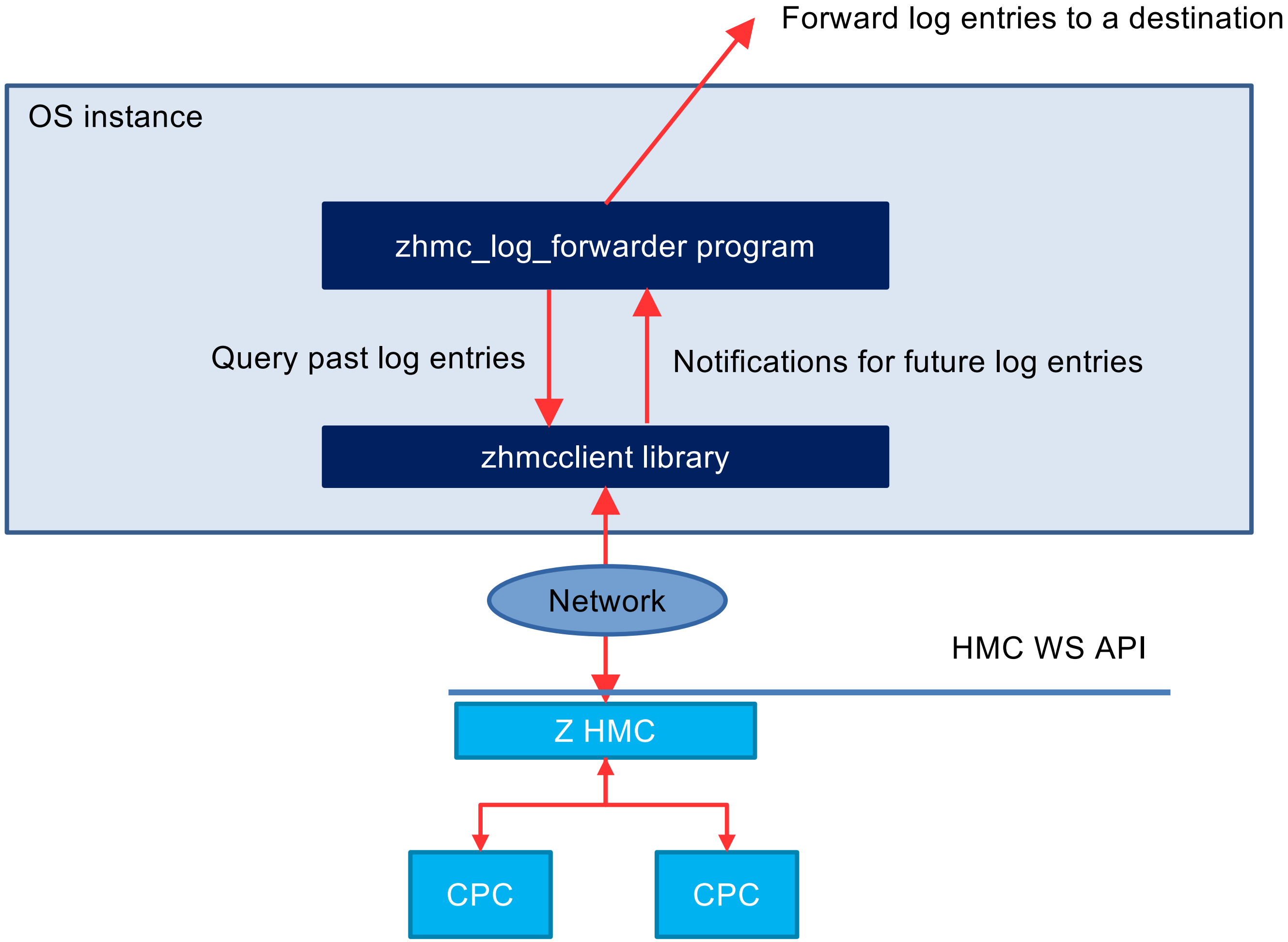
Problem Statement

- 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


Forward log entries to a destination
OS instance
zhmc_log_forwarder program
Query past log entries
Notifications for future log entries
zhmcclient library
Network
HMC WS API
Z HMC
CPC
CPC

zhmc_log_forwarder program

- Pure Python program, running on any OS and on Python 2.7 and 3.4 or higher
- 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 a destination: stdout, syslog (local and remote)
  - Note: The remote syslog destination is used for QRadar

zhmc_log_forwarder help

```
Usage:

  zhmc_log_forwarder [options]

General options:

  -h, --help              Show this help message and exit.
  --help-config           Show a help message about the config parameters
                          (including optionality and defaults) and exit.
  --help-config-file      Show a help message about the config file format and
                          exit.
  --help-output-format    Show a help message about the output formatting and
                          exit.
  --version               Show the version number of this program and exit.
  --verbose               Show additional information.

Config options:

  -c CONFIGFILE, --config-file CONFIGFILE
                          File path of the config file to use. Default: No
                          config file.

  . . . More options for overriding config parms in config file
```

Config file

YAML format:

```
---

# Which Z HMC to talk to:

hmc_host: 10.11.12.13.     # IP address or hostname of the HMC
hmc_user: myuser           # HMC userid
hmc_password: mypassword   # HMC password

# Which log entries to collect:

logs: [security, audit]    # List of log types to include
since: now                 # Include past log entries since when: all, now, date&time string
future: true               # Wait for future log entries

# What to do with the log entries:

dest: stdout               # Destination for the log entries: stdout, syslog
# TBD: parameters for syslog / remote syslog
format: '{time:32}  {type:8}  {name:12}  {id:>4}  {user:20}  {msg}'  # Output format
```

Output fields

Example (config file syntax):

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

Supported fields:

`time`: The time stamp of the log entry, e.g. 2019-08-07 05:56:37.177189+02:00.
`type`: The log type: Security, Audit.
`name`: The name of the log entry.
`id`: The ID of the log entry.
`user`: The HMC userid associated with the log entry.

`msg`: The fully formatted log message, in English.
`msg_vars`: The substitution variables used in the log message

`detail_msgs`: The list of fully formatted detail log messages, in English.
`detail_msgs_vars`: The substitution variables used in the detail log messages.

Example output

```
$ zhmc_log_forwarder -c wdc04-05.config.yml

zhmc_log_forwarder - a log forwarder for the IBM Z HMC.

HMC address:                     172.16.192.15
HMC userid:                      zbcInstall
Log destination:                 stdout
Gathering these HMC logs:        security, audit
Include log entries since:       now (2019-08-08 08:52:05.399237+02:00)
Wait for future log entries:     yes (use keyboard interrupt to stop, e.g. Ctrl-C)

Time                              Type      Name         ID  Userid      Message
----------------------------------------------------------------------------------------------------------------…
2019-08-08 08:52:16.340000+02:00  Security  WSA Logon  1941  zbcInstall  User zbcInstall has logged on to Web Se…
Starting to wait for future log entries
2019-08-08 08:52:37.050000+02:00  Audit     WSAPI      6055  zbcInstall  A web services client on 10.183.204.141…
2019-08-08 08:52:37.530000+02:00  Audit     WSAPI      6055              A web services client on 10.183.204.141…
^C--------------------------------------------------------------------------------------------------------------…
Stopping to wait for future log entries
Closing notification receiver
Logging off
```