Zombie Host Finder

2020. 10

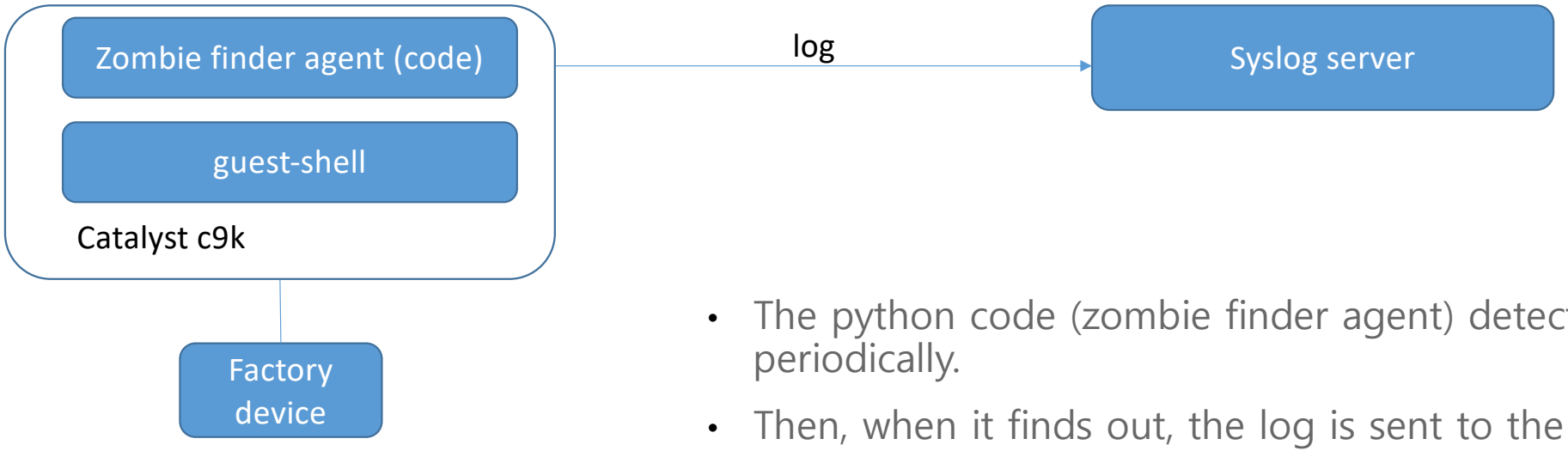
Wansoo Kim

Problem

- In the semi-conductor line or factory, the most import host is the manufacturing machine.
- However, it has the very poort networking fuction like printer and sometime very old.

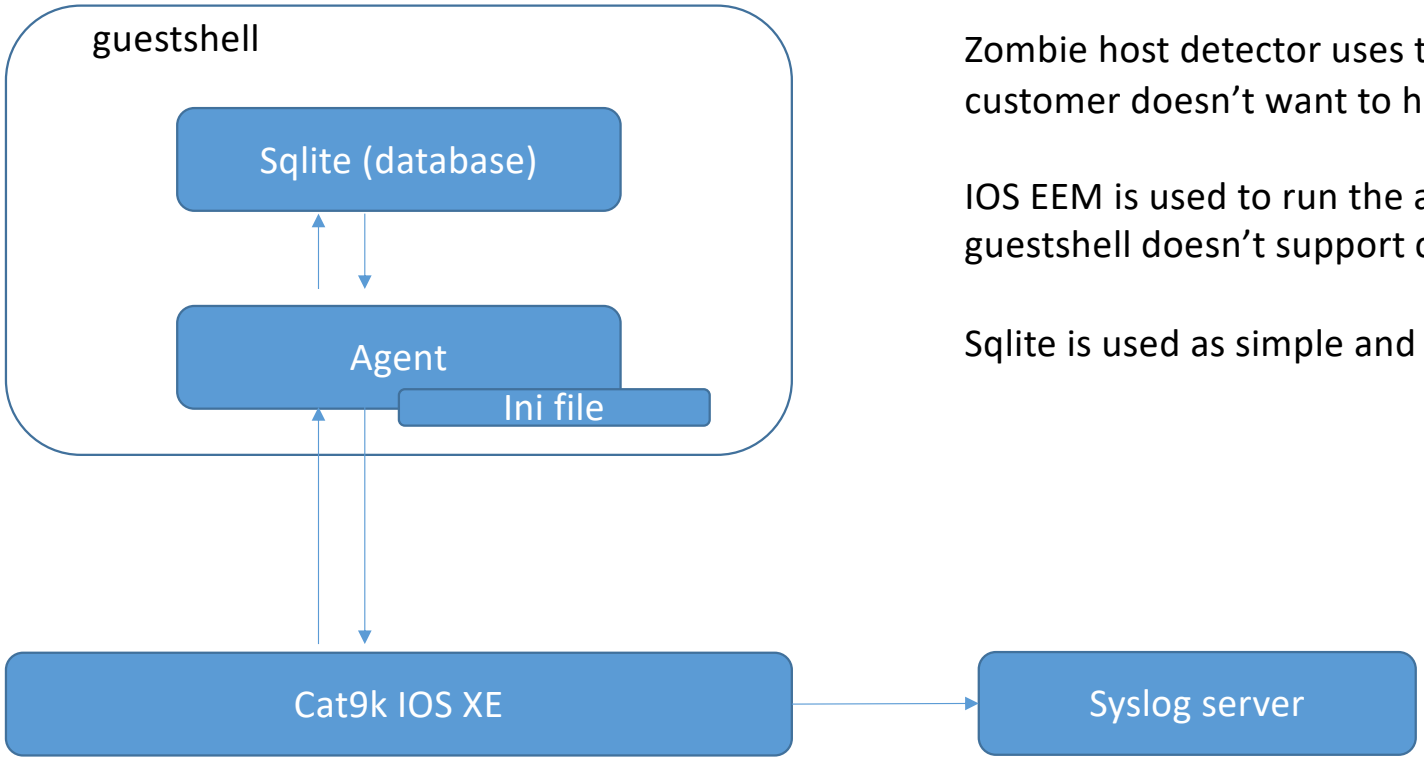
- Sometimes, the manufacturing machine interface is up but there is no traffic.
- If this “zombie host” can be detected, the factory effiency will be higher.
- If the catalyst can find out, it’s one of the unique feature of IOS XE.

Solution Diagram



- The python code (zombie finder agent) detects periodically.
- Then, when it finds out, the log is sent to the syslog server.

Software Architecture



Zombie host detector uses the guestshell because the customer doesn't want to have the separate server.

IOS EEM is used to run the agent periodically because the guestshell doesn't support cron.

Sqlite is used as simple and python embedded database.

How It Works

(1) IOS let the agent wake up the agent by EEM periocally.

(2) The Agent read the config file (interface.ini).
Config file has the interface which to monitor.

(3) The Agent queries the traffic of the interface (from config file).
And, write to the database and compare the value.

(4) If there is no traffic or uder the threadshold, the Agent makes the log.

(5) The log is sent to the syslog server.