

IDS – Intrusion Detection System

For tracking and analyzing network statistics and application logs

Executive Summary

IDS is a software system designed and implemented as a dashboard application to gather system status, network statistics and application logs of different systems and analyze them. It works inside a LAN or over the internet. Basically it gathers data from client systems and stores them at a centralized server. At server side, backend scripts parse the stored data and save it in the database.

Other features include a **notification system** and a **rule processor**. The notification system is meant to send notifications in the form of mail or SMS whenever some client-system (asset) goes down or is about to go down. Using rule processor we can design rules. The system logs and application logs are then tested based on these rules and the responsible users are notified accordingly.

All the logs saved at the server are represented nicely using graphs and tables. The system also generates reports based on the analyzed data.

Business Situation:

The client asked for a software-system to monitor connected systems. We used **collectd** to gather system statistics like disk space, memory usage and CPU stats and generate notifications. A **cron** script also keeps checking if the given system can be pinged or not.

The client also asked for monitoring applications on the client system. We implemented this using **rsyslog** through which we monitor application log files and store them at server where they are analyzed using rule processor.

The main functionality for the system as follows:

- Gather system statistics of different host machines.
- Store system statistics in a centralized place
- Analyze system statistics and Logs
- Notify users if something goes Wrong
- Detect network attacks, **DdoS**, Brute-force attack

About our Client

Client Custom Software Development Company | **Location** Tortola, Virgin Islands, British | **Industry** Custom Software Development

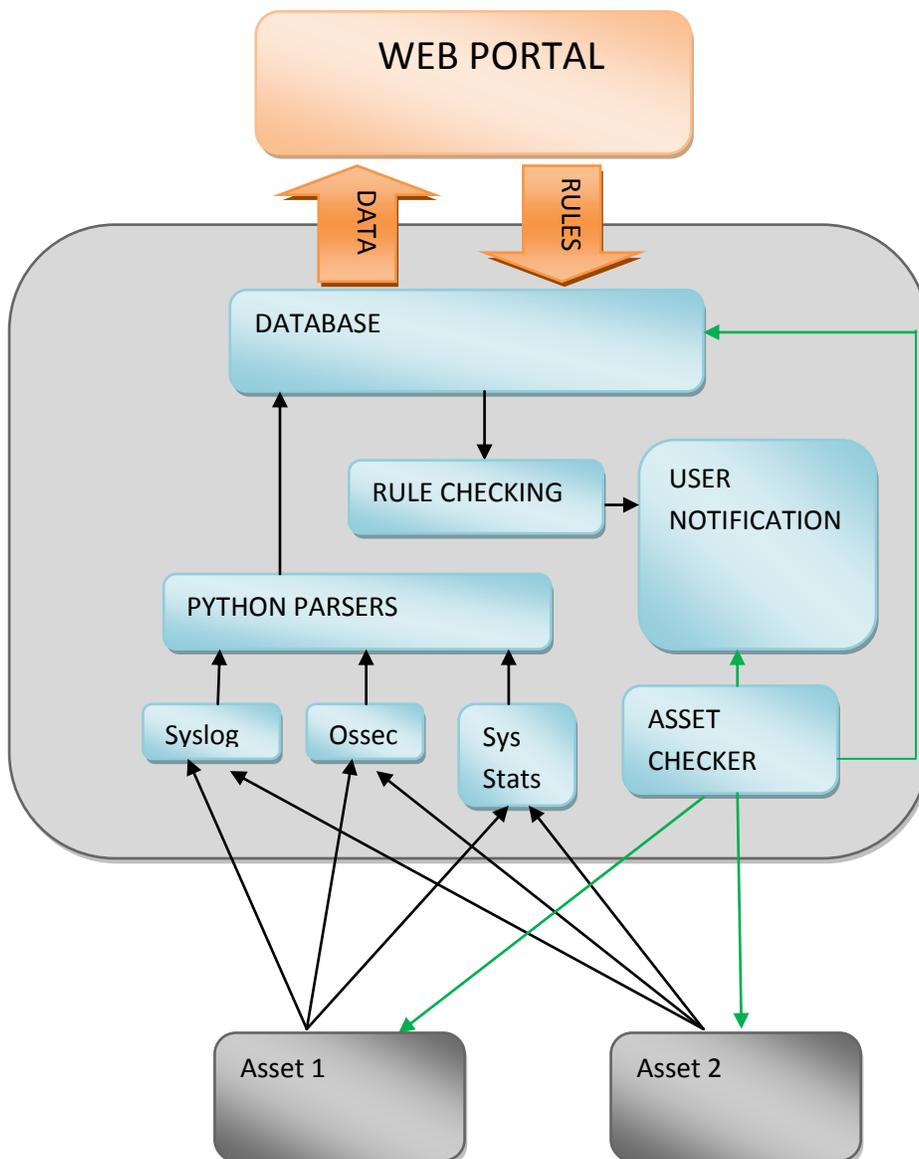
Technologies

Server Side: Python, Django, collectd, rsyslog, pyparsing, reportlabs, pyExcelerator,

Database : Mysql

Client Side : jQuery, Google charts API.

Architecture Diagram



Sample images of the actual application

Monitoring Charts

Home > Log Chart Recent Activity: 2012-02-03 14:05:59 low [] child_rip+0xa0x12

Dashboard

- [Home Page](#)
- [Asset Reports](#)
- [Log Reports](#)
- [System Overview](#)
- [Log Chart](#)
- [Notification Chart](#)

Logs

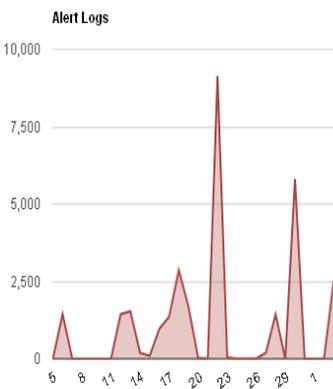
Settings

Users

Help

Chart

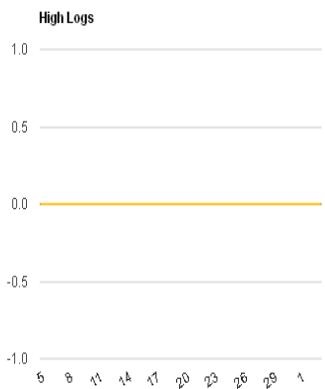
Alert Logs



Day

Daily Weekly Monthly

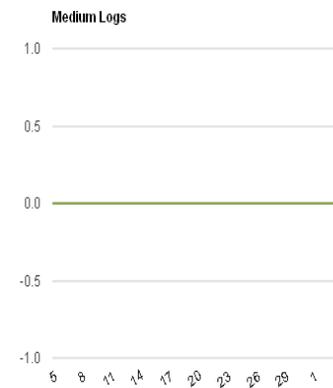
High Logs



Day

Daily Weekly Monthly

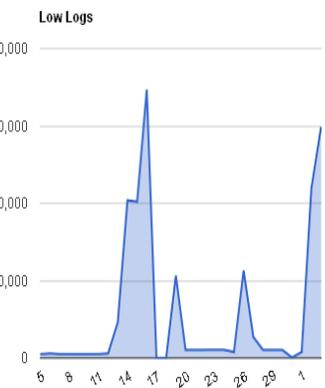
Medium Logs



Day

Daily Weekly Monthly

Low Logs



Day

Daily Weekly Monthly

Future relationship

The client was pleased with Mindfire's effort and reckoned that they were happy to have discovered a professional offshore IT unit. We shall continue to be the service provider for the next versions of the client's product. They have not only allocated the support and maintenance work of the current system to Mindfire but have also chosen us for future customization work.