Managed Platform Unit 2012 T2 report

1 Effort

Development work accounted for 49% (1.06 FTE) of this trimester; 29% for specific projects and 20% for misc development. Although a small rise on T1, it is still not as high as for previous periods. It is perhaps concerning that more effort was spent on misc development than on any one prioritised project.

Effort expended on operational work rose again to 27% (0.59 FTE). Much of this effort was related to managing the virtualisation servers. We will look at creating a bucket for this activity.

Effort expended on overhead and meetings was roughly similar to previous periods.

Personal development effort shrunk back to 8% (0.17 FTE).

2 Development

2.1 System security enhancements (224))

14% 0.31 FTE 196 hrs

During this period a number of separate parts of this project have been completed.

The Linux auditing framework is now used to generate daily reports regarding events of interest on the SSH servers. There is also a test deployment of a system to do more frequent monitoring for critical events, such as attempts to load kernel modules, on a separate central host which collects the audit logs.

There is now also a locally-developed suite of tools, named BuzzSaw, which can parse and filter system log files stored on a central host to discover events of interest. Associated with this is a report generation tool which is now used to generate daily reports on events related to the Linux kernel (e.g. kernel panics, oops, invocations of the Out-Of-Memory killer).

A facility to sweep for rootkits using the rkhunter tool has also been developed. This is much more capable and flexible than the chkrootkit tool upon which we had previously been reliant. There is a new LCFG component to configure and run the tool. A suitable configuration for the SSH servers has been created.

The developments of this project have already proved themselves to be very useful when we had to deal with another compromise of an SSH server in July 2012. In particular, the configuration of the Linux auditing framework made it possible for us to quickly and confidently identify the compromised user account and the method used to gain root privileges.

2.2 SL6 Server upgrades (203)

6% 0.13 FTE 82 hrs

This project involves upgrading all the MPU servers to SL6.

The following services were upgraded :-

- pkgforge master
- DR server

- pkgs sites (AFS)
- pkg export

Work has begun on upgrading to the most recent version of bugzilla for bugs.lcfg.org.

2.3 Improved server hardware interaction (171)

6% 0.12 FTE 77 hrs

A final attempt at making sense of and deploying Dell's OMSA software, which can in theory be of considerable help with firmware management. The OMSA software is hugely improved but certain fundamental assumptions seem to have been made by its designers and packagers:

- That the server will be running a standard commercial operating system such as RedHat Enterprise Linux
- That the server's OS configuration will be done by an operator rather than by automated configuration software such as LCFG
- That all Linux sites have handy Windows PCs lying about ready to be used as server monitoring stations.

None of these assumptions is true for Informatics.

A start was made on a home grown system which lists recommended server firmware updates and compares them to the firmware versions which servers already have installed. A script called 'firmwarereport' was developed which detects the firmware details of most major hardware components used in our servers and stores the data in a database. This work took a while thanks to two factors. The first was the complication involved in detecting firmware details in different types of hardware; for instance the several types of RAID controller in use are queried using several distinct software tools, all of which the firmwarereport script had to be told how to drive. The second factor was the need to learn DBI and SQL programming to manage the database interaction. However the script was completed and installed in T2, and since then data on firmware versions has been collected daily from our servers.

2.4 Inventory Improvement (146)

2% 0.05 FTE 29 hrs

This project is looking at improving the inventory system.

In this period, further discussions were held and a report was written describing the existing system.

2.5 Simple KVM service (202)

1% 0.02 FTE 11 hrs

This project aims to deliver a simple KVM service on DICE.

Further enhancements were made to kvmtool. Documentation (for managing KVM hosts) was expanded.

2.6 Misc Development

20% 0.43 FTE 269 hrs

This category covers all minor development work which is too small to be a full project. This quarter this has included :-

- Support for SL6.3
- Benchmarking of LCFG server to identify best hardware config
- New lcfg-auditd component
- Improvements to the lcfg-boot, lcfg-subversion and lcfg-logserver components
- Improvements to the installroot and hardware monitoring scripts

3 Plan for T3 2012

- Complete the MPU server SL6 upgrade project
- Complete the System Security enhancements project
- Complete the Improve Server Hardware interaction project
- Propose a follow-on project for Inventory Improvement
- Start user accessible login logs project
- Start LCFG client component code cleanup project
- Maintain effort spent on targeted personal development by tracking activity at weekly MPU meetings