Cyclotron Computing

R. Burch, K. Hagel, D. Rosenfeld and J. Utley

The infrastructure of the labs computing facility is changing to reflect the availability of cheap Intel processors and the demise of Digital's computing platforms and operation systems. We have over the past year continued the installation [1] of a base of Linux servers which will replace the various VMS systems. We intend to migrate the VMS user base to Linux. To do so we have identified four classes of servers: Computational Servers, Access Control Servers, File/Backup Servers and Data Acquisition Servers.

The Computational Servers (currently sleeper and ccomp) are intended to be used as the VMS systems were, to run computationally intense jobs. They each currently have large scratch disks (40 Giga Byte) which the user can use for temporary storage of data analysis results or computational results.

They are available to the lab for general remote (ssh suite) use: checking mail, editing files, for submitting batch jobs, and as an X window server. The Computational Servers are also available for incidental use by local users (discouraged) and visitors as a graphical workstation.

The Access Control Servers primary purpose is to authenticate the user's request and allow his usage of one or more of the labs computing services. There are two Access Control Servers, the main server and a fail-over server. This will help insure continuous access to the labs computing services if one of the access control servers (or part of the network) fails or must be taken down for maintenance.

The File/Backup Server (currently CyclotronMail) maintains the users personal directory on local disks and make these available to the other servers as required. It also is the primary Mail Hub to-be for the lab. We have installed a WebMail service, in addition to pop and imap servers. IMP (Internet Mail Protocol) is the version of WebMail we chose. IMP can be accesses throughout the world using a web browser. It is secure since communication between the browser and the server is over SSL which is the webs De facto encryption technology. We built IMP, the WebMail application from the source code to insure we could maintain control over the security of the application and it's configuration files and to prove to ourselves that we could build it in house. The File/Backup Server is also available for incidental use by local users (discouraged) and visitors as a graphical workstation.

The fourth class of servers is the Data Acquisition Server. A Data Acquisition Server (acq) has been added to the labs Linux base and has demonstrated the feasibility of acting as the primary back-end of the labs data acquisition system.

A toolkit based on the data analysis program ROOT[2] has continued development [1] and was successfully used as a data handler for data coming from the frontend, as run-control and as the spectra display manager for data acquired by the data handler in several NIMROD[3] experiments as well as a number of other experiments. Data from these experiments is saved directly on a combination of 50Gb and 70 Gb disk cache. For permanent storage the

user can choose between two different media types: DDS4 tape and DVDRAM, for later analysis.

Considerable effort in learning Linux has been expended in the last six months to insure a secure and relatively painless user base migration from VMS to Linux. A concerted effort is still required. Linux is inherently more susceptible to security breaches than was VMS. To reduce our exposure, we have implemented the strong authentication system, Kerberos, which exchanges "tickets" encrypted with the user password for authentication rather then exchanging the users password itself in clear text which can be "sniffed". The kerberos service is running on two dedicated servers (Access Control Servers) to minimize its exposure and to insure availability. We are also deprecating the r-tools, telnet and FTP for the ssh suite which encrypts all transactions. We have upgraded the version of Linux run on the server to RedHat 6.2. This fixes some security holes found in the earlier the versions of RedHat we were running.

To help insure data integrity and availability, the power for the File Server, Computational Servers, and the Access Control Servers are supplied by uninterruptible power supplies (American Power Company Smart-UPS 1400's) with at lease 40 minutes of continuous runtime. We are developing a script which will shutdown non-critical machines early to extend the up-time of critical machines. A the end of the UPS's battery life, the critical machines will be shutdown before the UPS shuts down it outputs. In addition, full monthly backup are performed on the user directories and the system disks using a commercial backup program, BRU by Enhanced Software Technologies. Weekly differential backups are performed on the user directories.

References

[1] K. Hagel *et. al., Progress in Research*, Cyclotron Institute, Texas A&M University (1999-2000), p V-9.

[2] Rene Brun and Fons Rademakers, ROOT - An Object Oriented Data Analysis Framework, Proceedings AIHENP'96 Workshop, Lausanne, Sep. 1996, Nucl. Instr. & Meth. **A389**, 81 (1997). See also http://root.cern.ch/.

[3] R. Wada *et. al., Progress in Research*, Cyclotron Institute, Texas A&M University (2000-2001), p. V-28.