Cyclotron computing

R. Burch, S. Wuenschel, and K. Hagel

Cyclotron Institute research programs require stable, fast, and secure computational and network resources. This past year we transitioned our users to the University authentication and dynamic name service systems and added infrastructure to accommodate the lab's growing need for cpu power, storage, and network throughput.

In order to comply with University computer policy with the least possible effort on our part, we migrated our identity management from our local Kerberos authentication system to the University authentication system which uses the TAMU NetID as the username. This allows us a single username/password combination for University services and our local computational services as well as local Window's PC authentication via the TAMU Open Access Continuum Domain systems. Importantly, all University requirements for identity management are satisfied with no intervention or effort from the computer group at the Cyclotron Institute. We are in the process of migrating administrative servers and identifying a methodology to migrate Macintosh users to use NetID authentication as well.

Given the ever increasing level of malicious attacks and software events of interest, we are implementing an ElasticSearch based log monitoring system which allows us to monitor, analyze, and display log data in real-time graphically and to drill down to view the events of interest. We collect log data from all Linux servers, sending them to the central log servers and we are investigating methodologies to send Macintosh and Windows logs to the central log servers. ElasticSearch has been instrumental in demonstrating the extent to which our ssh gateway is under a constant brute force ssh attack having 200 to 300 failed attempts per day. It illuminates the importance of protecting our servers with a hardened ssh gateway and firewall. To further strengthen our security posture, we are configuring and installing an additional firewall that performs deep packet inspection to run in series with our current firewall.

Infrastructure enhancements in the past year included replacing all our old 3COM 100 mega bit network switches in the server room with new 1 giga bit switches. We added 10 giga bit switches to each server rack, linking them with a 10 giga bit backbone and added 10 giga bit network cards to all file servers enhancing data analysis network reliability and throughput. For the lab's general usage, we added a data file server with 12 disk slots, 3 slots populated with 11 terabytes of capacity. For one group with large data volume requirements, we added a similar server for their data as well as another one for their backups. We added a messaging board system based on a Raspberry Pi and a large screen TV to show lab announcements. We replaced our aging Dell PowerEdge web server that had a power consumption of 450 Watts with a more powerful ODROID-XU4 credit card form factor Linux server that has a power consumption of 20 Watts for about $150 and added to it two high speed USB 3 Flash drives for web storage and local backups.

Several more waveform digitizers were added to our data acquisition system. The software for reading the digitizers was enhanced and made more flexible as we have learned to use them. The critical enhancements had to do with learning how to handle the large buffers that result from reading in multiple

long waveforms. In order to have the least impact on users with regards to backwards compatibility, we made the effort to implement the large buffers into our existing data analysis infrastructure. This was complicated by the fact that the raw data buffer had been designed long ago to have a maximum size of 64kB which is the maximum allowed for a 16 bit unsigned integer. It was therefore necessary to implement the option of splitting events across buffers. This was done with a very small impact on the users. The system was debugged and used extensively in a major run in the summer of 2016 in which the readout of the entire waveform was imperative. It was also used in a number of different experiments that, while the experiment could have been executed, would have had to severely curtail the information acquired from the important waveforms.

The preceding enhancements allowed us to utilize the capabilities of the waveform digitizers on an event by event basis. While we could handle the buffers from a software point of view, in fact various bandwidths made reading the long waveforms cause the data acquisition to become prohibitively slow. In fact, most of the events that were acquired did not require the information. We therefore developed software that allowed us to change both the triggering configuration as well as the length of the waveform "on the fly" when we detected an interesting event. Once the interesting information had been acquired, the triggering configuration as well as the length of the waveform read out was returned to the normal running status.

In summary, we have made changes in order to more fully comply with TAMU security policies, implemented an event monitoring system and made enhancements to our network bandwidth. We also implemented several changes to the data acquisition system to fully utilize the power to the waveform digitizers that are being deployed in more and more experiments.