Information Systems & Technology
2018 Mid-Year Assessment of Status and Opportunities

Introduction

This report identifies areas within the Information Technology environment at TRIUMF that are important to the ongoing operations of the organization. Current status, outstanding issues, and recommendations are described for each area. Items that were identified in the 2016 Mid-Year Review have been updated. A summary of major accomplishments since the last review is provided in Appendix A.

Agresso ERP

The Agresso ERP has been in production since January 1, 2016 and is generally meeting requirements.

First class application support for Agresso is critical to TRIUMF's success. Subsequent to the 2016 Mid-Year review a 3rd party organization (Agilyx) was engaged and provided support until early 2018. In addition internal staff continued to expand their understanding and expertise with Agresso.

Issue: Ongoing support for Agresso is a high priority for the ITS Team.

Recommendation: Agresso will be updated to Milestone 7 in the fall of 2018 which will bring the application to a current version and will resolve a number of existing issues. Due to a re-organization at Agilyx which resulted in key staff departures the external support for Agresso is now being provided by a new firm, Arribatec. The intent is to continue with a combination of internal and 3rd party support for Agresso for the foreseeable future.

Network Architecture

Although the core network switches and Firewall are state-of-the-art there are many peripheral devices that need to be upgraded. All devices (routers, switches) on the network need to centrally managed but there are some legacy devices that do not have that capability.

There are some applications (Work Permit, eLog, Faults) that Operations/Controls groups require even if there is a loss of access to the main TRIUMF network. User access to these systems had been through use of data replicated from the TRMAIL server including the copying of encrypted passwords. This has been replaced with a much more secure approach which involves having a Domain Controller on the controls network which effectively allows the use of TRIDENT authentication in a very secure manner. That was implemented in Q2 2018.

A new technology called GPON (Gigabit-capable Passive Optical Networks) is becoming mainstream in the networking world. GPON eliminates the need for “edge switches” and wiring closets with patch panels. Instead, small groups of connections are converted to an optical medium which communicates directly with the core router. The Sandia Laboratories in the U.S. have converted completely to GPON resulting in enhanced security, significant long-term cost savings, superior network performance and dramatic reductions in space required for networking equipment.

Issue: Some of the network equipment in use at TRIUMF is obsolete, expensive to maintain, and does not support modern network architectures.

Recommendation: Replace the existing VPN appliances with upgraded equipment (fall, 2018) and upgrade some edge switches in order to enhance network management capabilities. Undertake a pilot project with GPON technology to test its capabilities and, assuming a successful pilot project make GPON the standard technology architecture for all new facilities including IAMI as well as for all major renovation projects.

Cyber Security and Access to TRIUMF Computing Resources

External collaborators, experimenters and TRIUMF employees working offsite are able to access equipment inside the perimeter of the TRIUMF computing environment using Virtual Private Network (VPN), Secure Shell (SSH), Secure File Transfer Protocol (SFTP), VNC and other tools. In almost all cases proof of identity is established by the end user knowing a password. This is known as single factor authentication. It may be desirable to introduce a second form of authentication (possession of a physical device such as a registered computer or mobile device) to enable two factor authentication (SSH access already uses two factor authentication).

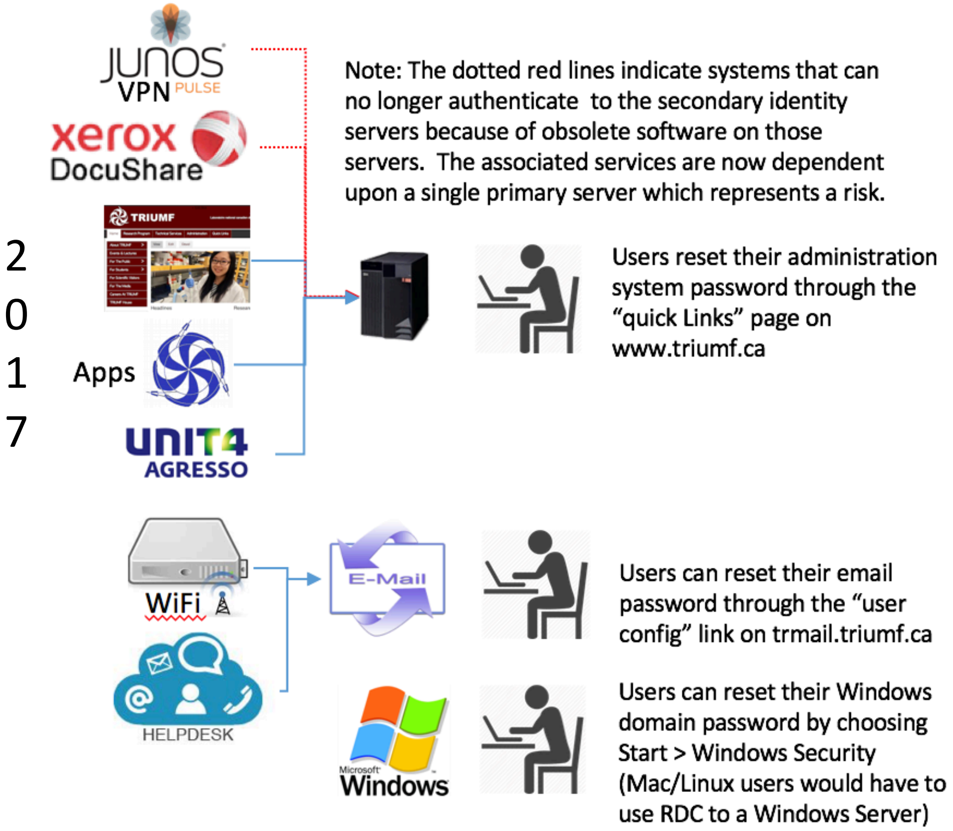
The culture at TRIUMF has traditionally been very open to external collaboration and the restrictions on access to TRIUMF systems have had to been minimized in order to support this. As a result, the compute resources (servers, files, email, etc.) have been protected against attack by “hardening” access through the use of personal certificates and through other measures. Given the state of the world today it would be useful to obtain external validation of that approach.

Issues: the evolving nature and sophistication of computer network attacks is difficult to assess and demands a very highly skilled and focused approach.

Recommendations: Trustwave, a Managed Security Services Provider has been engaged to assess the current state of cyber security at TRIUMF and make recommendations regarding measures that can improve security practices and better protect TRIUMF assets. This assessment will be started in October, 2018 and will be completed early in 2019. It is anticipated that a number of recommendations will emerge from that assessment which will be implemented in fiscal 2019/20.

Identity Management

The management of access to various TRIUMF systems was historically very fragmented and was suffering from obsolete versions of software which was limiting the ability to integrate systems. Most TRIUMF users had at least 4 identities and passwords (administrative systems, email, Windows environment, Google Calendar) which made it impossible to manage access and roles in a consistent and centralized fashion.



Note: The dotted red lines indicate systems that can no longer authenticate to the secondary identity servers because of obsolete software on those servers. The associated services are now dependent upon a single primary server which represents a risk.

Users reset their administration system password through the "quick Links" page on www.triumf.ca

Users can reset their email password through the "user config" link on trmail.triumf.ca

Users can reset their Windows domain password by choosing Start > Windows Security (Mac/Linux users would have to use RDC to a Windows Server)

TRIDENT

In October, 2017 a new, secure Identity was established at TRIUMF allowing users to set up security questions and self-serve password resets using a web-based tool. This TRIDENT will be used to access all major systems at TRIUMF by the end of 2018. The implementation of TRIDENT also allowed TRIUMF to join the EDUROAM Federated Identity consortium.

The establishment of TRIDENT will eliminate most of the issues associated with Identity Management by the end of 2018.

Associated Issue: The annual on-boarding and off-boarding of hundreds of co-ops, undergraduate and graduate students, regular employees and researchers makes provisioning of computer services very challenging.

Recommendation: Leverage the TRIDENT identity management system and available workflow software to automatically provision and de-provision services based upon changes in the HR and Visitor databases with automated approvals from supervisors and TRIUMF staff members responsible for visiting scientists and other stakeholders. Opportunities for providing more federated identity services (similar to EDUROAM) for authorized staff from TRIUMF member institutions and collaborators will be investigated (for example, access to "internal" pages on the Intranet, access to Docushare, etc.)

Telephone System

There have been numerous problems and some extended outages with the legacy telephone system in use at TRIUMF due to the age of the equipment and the very limited number of technicians who know how to maintain and configure the system. The lengthy amount of time it took to install and configure the Code Blue telephone was primarily due to difficulties integrating a new device with the legacy telephone switch.

In the fall of 2017 a new telephone architecture based upon the use of a virtual PBX running on servers in a private cloud at UBC (EDUCLOUD) was implemented. There have been a number of internal network issues that were identified as more telephones were deployed but most if not all of the issues have now been resolved. It is expected that this system will be fully functional by the end of 2018 resulting in significant long-term cost savings and much improved unified communications capabilities.

Issue: The existing telephone equipment in use at TRIUMF is obsolete, expensive to maintain, and does not support modern unified communications capabilities.

Recommendation: Complete rollout of VOIP/SIP telephone system.

TRIUMF Internally Developed Applications

A number of internally developed applications are used at TRIUMF. These include the Work Request System, the Work Permit System, the Visitor Application, the Dosimeter Application, Administrative and Human Resource components of the ERP, a conference booking application, and the new NCR application (currently nearing completion after a long delay due to changing requirements and rebuilding the development team).

Some internally developed applications should probably be replaced by third party Commercial Off the Shelf (COTS) applications. In particular, the continued development and support of a custom HR application may not be warranted when a module could be added to the existing Agresso ERP or HR functionality could be handled through the UBC system (UBC already handles employee payroll).

Issue: the applications developed at TRIUMF use a variety of technologies and databases which represent a barrier to integration and complicate maintenance and support.

Recommendation: A review of all existing applications is being undertaken and a plan for migration to a common set of underlying technologies will be developed. A new, robust and highly automated deployment infrastructure based upon modern technologies such as Gitlab and Docker is being implemented. Third party COTS applications will be implemented if appropriate.

AS400/iSeries

The IBM AS400/iSeries server used for many administration functions at TRIUMF is essentially obsolete and obtaining support services for it, even from IBM, is very problematic. The DB2 database used to store HR data and tables for TRIUMF custom software is difficult to access with modern reporting and visualization tools.

During 2018 many key database tables have been cloned from DB2 to SQL Server using real time replication. This will allow TRIUMF custom applications to start using SQL Server as the primary database so that DB2 can be decommissioned towards the end of 2019.

The room booking application on the AS400 was retired in the fall of 2018, replaced by Outlook.

Issue: AS400 support is hard to find and the DB2 database is difficult to work with

Recommendation: All TRIUMF custom applications will be modified to use SQL Server for data storage. A decommissioning project for the AS400 will be initiated with anticipated end date of December 31, 2019.

High Performance Computing for the Theory Group

Through a partnership with the Advanced Research Computing (ARC) centre at UBC a new, high performance computing environment was established for the TRIUMF Theory Group in 2017. This facility took advantage of very heavily discounted pricing for equipment that was available as a result of the Compute Canada data centre RFP. Because of its location at ARC there is no hardware or operating system maintenance required by TRIUMF staff.

Issue: Managing access to this resource for international collaborators is challenging.

Recommendation: Implement EDUROAM style federated identity to allow international collaborators to use the Theory cluster with TRIUMF controlling access rights but not having to be concerned with user ID/password maintenance.

Servers, Storage and Backup

During 2017 a new backup architecture was implemented which uses dedicated hardware appliances that incorporate data de-duplication to reduce the amount of backup required. Most of the important file systems used at TRIUMF are now maintained on upgraded network attached storage and are backed up on these appliances.

Issue: Some file systems, especially those used by experimental groups, are not yet using the enterprise backup system.

Recommendation: Expand the capacity of the existing backup appliances to support backup of all experimental data. Move the secondary appliance to UBC Okanagan for disaster recovery purposes.

Email, Chat, Calendar, Presence

The email system used at TRIUMF was based upon technology that did not provide Unified Communcations capabilities (the integration of email, voicemail, chat, calendaring, audio and video conferencing). The technology was also no longer widely used and there was only one staff member at TRIUMF knowledgeable in the configuration and administration of the system.

During 2017/2018 Office 365 was implemented at TRIUMF providing cloud-based Email, Calendar, Room booking, and chat capabilities as well as access to advanced collaboration tools such as Sharepoint, One Drive, Teams, and others. The full Microsoft Office suite is now available to all employees with real-time updates so that everyone has the same version of software.

This was a very challenging project due to the very heterogenous computing environment at TRIUMF with hundreds of Mac and Linux users and various vintages of windows computers and Office Suite versions.

Issue: Additional training and support will be required to fully take advantage of the many tools available in Office 365.

Recommendation: Provide support and training using internal and 3rd party resources.

Better Access to Docushare

The search capabilities of Docushare are somewhat limited and cannot produce lists of documents that are in various stages of routing. Work undertaken by a Co-op student produced a proof-of-concept that would allow for search capabilities designed specifically to meet the needs of the TRIUMF community. These can be integrated into the TRIUMF Intranet.

It may also be possible using a different technology (Java interface) to provide summaries of documents at different stages of routing.

Issue: Search capabilities customized to meet the needs of the TRIUMF community would be beneficial and would enhance the value of the Docushare system.

Recommendation: Xerox has been contracted to customize some of the Docushare interfaces to allow for easier and more reliable document searching. Delivery of these customizations is expected before the end of November, 2018. Further investigation of ways to improve the effectiveness of Docushare will be ongoing.

Improvements to Cell Phone Coverage

The cell phone coverage on the TRIUMF campus is generally poor even in some outdoor open paces between buildings. Because TRIUMF employs a "bring your own device" strategy multiple carriers are involved which makes enhancements to cell coverage problematic.

The recent installation of additional cell towers in the Westbrook Village area has improved coverage for Telus/Bell customers.

Issue: Cell phone coverage is unreliable in many areas of the TRIUMF campus

Recommendation: Rogers/Fido has requested permission to install transceivers on a building on the TRIUMF campus. Technical and administrative ramifications are being evaluated. A review of the current state of cell coverage will be undertaken and further measures will be taken to improve coverage if warranted and cost effective.

Replacement of the Physical Access Security System

The system used to control building access at TRIUMF is Facilities Commander, originally purchased through Chubb Edwards. The maintenance for this system in now provided by Tyco. The ownership of the Facilities Commander software application has changed several times over the last few years. The current owner is Lenel (A United Technologies Company). Lenel has announced that there will be no further development of the Facilities Commander software and has provided an upgrade path to their "On Guard" product.

Modern Security and Event Management (SIEM) systems provide a web-based interface so that there is no need to install software. Enhanced features such as visual information on the location of alarms presented on accurate building plans and role-based access would significantly improve the ability of TRIUMF Safety and Security staff to monitor and respond to access incidents.

Issue: The system used to control building access at TRIUMF has reached end-of-life.

Recommendation: Alternative systems to provide this functionality need to be investigated with the goal of replacing the existing system within 6-18 months. Any new system will require installation of new hardware so that a phased approach will be necessary.

Note: *This item has been carried over from the 2016 assessment because no action has been taken to address it.*

Resource Constraints and the Complexity of Decentralized IT Support

Support for different components of the Information Technology environment at TRIUMF have evolved over the 40+ years that the organization has been in existence. Responsibility for different aspects of the computing environment such as ERP/Enterprise applications, server and storage management, and Windows computing had their origins in different parts of the organization.

Although there has been a significant consolidation of support staff into the ITS Department there are still resources distributed throughout the organization to handle DAQ equipment, Controls and Operations networks and computers and some custom applications.

This distributed approach to both system support as well as the purchasing of computer equipment represents a significant challenge to the optimization of operations and makes it difficult to obtain the best value for the financial and human resources dedicated to computing at TRIUMF.

The use of dedicated staff to support different parts of the organization has some advantages and has worked well in the past. These advantages must be balanced against the operational complexities associated with this approach. As a minimum, better communication between groups and coordination of activities should be implemented.

Although TRIUMF is a unique organization which makes cost comparisons difficult, it seems clear that resource constraints continue to impact the ability of the ITS Department to deliver world class computing resources to TRIUMF stakeholders.   The need to replace retiring and departing employees has also been a constant issue (5 out of 12 staff members have changed in the last 2 years) and that will continue for at least the rest of 2018.

Issue: Although much has been accomplished in the last two years through the dedicated efforts of the ITS staff many important items have received little or no attention..

Recommendation: Recruitment to maintain or expand the current staff complement of the ITS Department must remain a high priority. The use of external consultants and contractors with specific expertise will be used to supplement internal resources.

APPENDIX A: Major Accomplishments since the 2016 Review

Agresso/ERP

- A new staff member has become familiar with many functions of Agresso.
- An external contract organization with expertise with Agresso has been engaged to provide additional support particularly in niche areas such as Planner and Workflow
- In the fall of 2018 Agresso will be upgraded to Milestone 7 which will bring to a current software release eliminating a number of defects and simplifying support.

Network Architecture

- Core router and Firewall upgrades
- EDUROAM was made available on the TRIUMF site and for TRIUMF employees off site
- A secondary Domain Controller was implemented on the Controls network allowing custom applications to make use of TRIDENT for user ID/password.

Identity Management

- TRIDENT was implemented providing web based security question setup and self-serve password reset. This was essential because of the many Mac and Linux users at TRIUMF that are not part of the Windows Domain.
- By mid-2018 Office 365 (Microsoft Office Suite, Email, Calendar), VPN, TRIUMF Secure Wi-Fi, Helpdesk, eLog, Faults, Calibration and Inspection Index, Work Permit and Docushare all required TRIDENT authentication. Other systems will be implemented by the end of 2018.

Telephone System

- A Mitel virtual PBX was implemented in a private cloud at UBC (EDUCLOUD) using VOIP/SIP technology. More than 100 handsets have been deployed and network issues resolved.
- This project should be completed by the end of fiscal 2018/19.
- Existing contracts for telecommunications services have been renegotiated resulting in significant cost savings for TRIUMF.

High Performance Computing for the Theory Group

- A partnership with the Advanced Research Computing centre at UBC was developed to provide a new high performance computing cluster for the TRIUMF Theory Group. This facility is maintained by UBC personnel.

Servers, Storage and Backup

- A new state-of-the-art Network Attached Storage (NAS) environment was set up and all existing files systems transferred to that system.
- A new backup system was put in place for all critical TRIUMF file systems. Using dedicated appliances that employ data-duplication this provides a scalable and future-proof backup solution that will be expanded to support experimental groups, DAQ, and others.

Email, Chat, Calendar, Presence

- Office 365 was implemented using Canadian data centres providing cloud-based email, calendar, office booking, and chat capabilities. All employees also have access to the full Microsoft Office suite resulting in all employees having the same productivity and collaboration tools.
- Google Calendar has been decommissioned.
- The TRIUMF developed custom room-booking application is being decommissioned.

Resource Constraints and the Complexity of Decentralized IT Support

- Five new staff members have been hired to replace retiring or departing members of the ITS team.
- Outside consultants have been hired to assist with implementation of Office 365, support for the AS400, and implementation of TRIDENT.