Campus Cyberinfrastructure Plan for Research Support

Introduction

The Clarkson Cyberinfrastructure Plan is based on the OIT Strategic Plan document and the Clarkson@125 (University strategic plan) document and revised by input and needs identified in the 2017 Strategic Research Plan. This plan outlines specific steps that should be taken to effectively support the research computing needs at Clarkson. It is important for the strategy of the Office of Information Technology to be very closely aligned with the institutional and research goals and objectives. Not every item included in the OIT strategic plan document is relevant to cyberinfrastructure issues; instead specific goals, objectives and activities are addressed herein.

For the purposes of this document, we will consider the term cyberinfrastructure broadly, to include: *physical infrastructure* - like fiber optic cabling and datacenter space; *electronic infrastructure* - like servers, storage and networking hardware; *application infrastructure* - the software that runs on top of the electronic infrastructure; *personnel* - the expert faculty and staff who weave all of the underlying infrastructure layers together to produce usable systems; and *security* - the policies and practices that ensure the confidentiality, integrity and availability of each of the above categories of cyberinfrastructure.

Physical Infrastructure

Campus Fiber Optic Cabling

The majority of campus fiber optic cabling infrastructure has been updated between 2014 - 2019. With very few exceptions, all buildings are connected using single-mode fiber optic cabling. This cabling is sufficient to support the existing campus backbone and to provide for the growth necessary to support both consumers and producers of big data sources into the future.

Clarkson Green Data Center

The construction of the Clarkson Green Datacenter (CGDC) was completed in 2Q 2014. This new datacenter represents a generational improvement over the legacy facility, which was constructed in the 1970s. The GDC provides a modern, energy-efficient datacenter space via the adaptive reuse of Clarkson's original facility, Old Main. It was constructed and is managed according to current industry standard best-practices and incorporates a number of energy-efficiency measures, including: hot-aisle containment, passive free-cooling during winter months, and scalable emergency power generation. The facility has become the primary location for Clarkson's production IT equipment, large-scale research computing equipment and will also include leased space for tenants. This facility has adequate {power, cooling, rackspace} capacity to support the University's current and future growth needs for the foreseeable future.

Electronic Infrastructure

Servers — High Performance Computing (HPC)

In 2014, OIT launched the availability of a computational cluster for research computing, designed as a turnkey, professionally-administered high performance computing resource. Unlike many grant-funded clusters that limit access to members of the individual research team, this new cluster is available to any member of the campus community to use for free. The seed hardware for this cluster was graciously provided by IBM as part of a Shared University Research grant program. In addition to these shared nodes, Orion has the capability to be expanded with dedicated nodes funded by individual faculty members in a 'condominium' model. This combination of shared/dedicated resources represents a new model for providing HPC resources and is discussed in detail in the document "A Research Cyberinfrastructure Strategy for the CIC: Advice to the Provosts from the Chief Information Officers.[1]" It is recommended that a set of incentives should be implemented to encourage faculty to expand the hardware available in this resource, rather than pursuing local installations.

Additionally, it should be understood that an institution of Clarkson's size will not be able to provide access to an extremely large HPC facility internally. To ensure that faculty requiring this level of HPC access are adequately supported, it is recommended that Clarkson seek to develop relationships and agreements with national laboratories or other very large-scale facilities, to gain access to these facilities on an ad-hoc basis.

Network — Backbone

Academic buildings are connected to the campus network backbone uplinks with 80Gbps of capacity, which is sufficient to support the current needs of research faculty. However, the existing 100Mbps edge ports are no longer sufficient to meet growing demand for high-speed connectivity. Some locations on campus have received targeted deployment of 1G/10G edge ports in areas of high demand. To ensure equitable access to high-speed data transfer capability in support of research at Clarkson, it is recommended that edge ports in the academic buildings be upgraded to 1G across campus. This gigabit edge upgrade is currently scheduled to begin in Spring 2019.

Network — Pervasive Wireless

A major initiative to deploy campus-wide pervasive wireless was completed in 2017. This deployment provides secure, high-speed, latest-generation wireless capability to all indoor locations on campus, both academic and residential.

Network — IPv6

The University has received an allocation of IPv6 addresses and this address space is advertised via all three of the University's upstream ISPs. Both campus datacenters fully support IPv6 and new equipment purchases are being made with IPv6 support as a requirement. While deployment of IPv6-services beyond the core and experimental networks has been limited, as the use of IPv6 "in-the-wild" continues to grow, Clarkson will continue to monitor the state of IPv6 adoption and will evaluate deployment of IPv6-based services on an ongoing basis.

---

[1] http://www.cic.net/docs/default-source/technology/2010report_-_6_21reduced.pdf

Storage — Long-term Archival and Dissemination

Beginning January 2011, funding proposals submitted to NSF must include a data management plan outlining steps that will be taken to preserve and disseminate research results. The consensus within the higher education research community is that ultimately research universities will be held responsible for the ongoing storage and maintenance of data generated by sponsored research. It is recommended that funds be committed to supporting the creation of large-scale centralized storage to support this demand.

Application Infrastructure

Site-Licensed Software for Research

In 2014 the academic technology advisory committee identified several software packages which are used extensively by faculty for both teaching and research. At the time, these software packages were licensed for limited classroom usage, but it was recognized that broader availability would greatly benefit the campus community for both teaching and research. These software packages included: MATLAB, SPSS, Adobe Acrobat, Labview, and ESRI. Between 2014 - 2018, site licenses were purchased for MATLAB, SPSS, ESRI. Funding continues to be sought to purchase the remainder of these software licenses.

Identity Management and Global Federation

LDAP and Active Directory identity sources are provisioned by custom feeds from our ERP system (PeopleSoft). Single sign-on authentication and authorization services are provided by the Central Authentication Service (CAS) supporting intra-campus access to web resources, and the Shibboleth federated identity service. In the past, due to the limitations of our campus backbone network, opportunities to share large volumes of research data had been limited. As a result, there had not been sufficient demand from the research community to warrant the implementation of a global federated identity management solution. However, as the capabilities of the network have improved and as technology in this space has developed, we have observed a growing demand for the availability of Shibboleth authentication (via inCommon) and for ‘eduroam’ authenticated wireless. These two items will be pursued in the future.

Personnel

Research Computing Staff

To effectively build and maintain a world-class research computing infrastructure requires dedicated staff with specialized skills. Traditionally this support was absorbed by the Network Services group in the Office of Information Technology. But as the number of services and the complexity of needs grows, it will become necessary to add dedicated staff with specialized skills in the area of high-performance computing, visualization, and mathematical modeling to provide this support. The cost of these computational/application/domain scientists could be partially recovered via grants and contracts, through a University commitment would also be needed to jumpstart the effort and to ensure continuity of staff levels in the event that grant funds cannot be secured.

Information Security

Applying NIST SP800-171 to Research and Education Infrastructure

In 2018 the Chief Information Officer led an initiative to conduct a comprehensive Information Security Risk Assessment for the campus community, which included academic, administrative, and research foci. This risk assessment led to the creation of a plan of action and milestones that describes a three-year initiative to roll out critical information security controls to the campus community. The ultimate goal of this initiative is to create a NIST SP800-171 compliant environment for all research activities on campus.

Approach to Data and Privacy

Clarkson University respects the diversity of values and perspectives inherent in an academic institution and is therefore respectful of intellectual freedom and freedom of expression. The University does not condone censorship, nor does it endorse the routine inspection of electronic files or monitoring of network activities related to individual use. Users of University information systems may expect privacy in their individual files and data, electronic mail, and voicemail as long as they are using University information technology resources in a manner consistent with the purposes, objectives, and mission of the University and in accordance with law and University policy. Clarkson University has adopted a comprehensive set of policies governing Data and Privacy which are incorporated in the University's Operations Manual, Section IX.

Routing Security

At the urging of the NSF, the Office of Information Technology has begun assessing the recommendations expressed in the Mutually Agreed Norms for Routing Security (MANRS). Many of the recommended controls have been in-place on the University network for decades, including: bogon filtering, route filtering, anti-spoofing protections, etc. The additional recommendations included in MANRS will be evaluated and implemented in the future.

Sustainability

Sustainability and Responsibility for Maintaining Federal Investments

Clarkson University's CI strategy relies on leveraging federal research opportunities to enhance the infrastructure and services available to the local research community. In recognition of the stewardship responsibilities of these investments, Clarkson commits to use central investment and personnel available in the Office of Information Technology to support bringing and maintaining these assets in the campus production environment for the use of the academic community.