XRAY Beamline Services

Computing and Network Resources for XSD Beamlines

David Wallis, David Leibfritz, Kenneth Sidorowicz

2/13/2024

The APS Engineering Support Division's Information Technology Group maintains and supports the APS computing infrastructure including the management of all APS enterprise networks and CAT backbone networks, tier 2 firewalls, servers, storage and printers in conjunction with supporting all DHS, DOE, and Argonne National Laboratory cyber security policies. This document provides an overview of the IT services available to the XSD beamlines. For additional information please see the IT home page https://www.aps.anl.gov/it.

Contents

1 Sector Liaison

A liaison from the IT group is assigned to each XSD sector. See https://inside.aps.anl.gov/Information-Technology/IT-Staff under "Liaison for" column for the current sector assignments.

The IT liaison serves as a conduit for information between the IT group and the sector staff. Sector liaisons should meet with their assigned sector groups to discuss IT needs in the sector, as well as to keep the sector up to date on short- and long-term IT plans. The sector liaison is also a resource for each sector and can help to expedite the resolution of urgent problems.

2 Networking Services

APS provides each sector with a public and private class C IPv4 subnet, which is shared between the beamline and LOM office computers. Each class C subnet provides 254 IP addresses for computers and other devices. All beamline network jacks are wired using CAT 6A-rated cabling supporting communications up to 10Gbps. The network cabling connects to a dedicated network switch/router on the beamline and a shared switch/router in the LOM for the offices. These network switches currently support 1Gbps connections to the desktops and multiple 10/40/100 Gbps connections to the APS backbone. Most beamlines provide connectivity for desktops and servers running at 10Gbps.

Each beamline is assigned a dedicated domain name server (DNS), DHCP server, NTP server and PV-Gateway interface. These services are local to the beamline so they will always be available in the event of an upstream network failure.

All computers and devices on the network must be registered with the Argonne Integrated Host Warehouse (IHW) database as required by the Argonne Cyber Security Office. Failure to register will create an automated network block. All computers will be subject to short network scans and monitoring when first attached to the network. Full network scanning only occurs for hosts that are connected to the beamline public networks.

To maintain the integrity of the network and to centrally manage every network port, mini-switches are strongly discouraged on the beamline networks. By having all devices connected directly to the beamline switch network administrators are able to monitor, diagnose and troubleshoot problems in a shorter amount of time and minimize downtime due to failed devices on the network. If sufficient network jacks are not available in a desired beamline location, please contact IT support so additional jacks can be installed.

2.1 Visitor Network/Wireless

APS provides a wireless 802.11g/n/ac network for visiting and APS wireless users. Visiting wireless computers must register before connecting to the network by starting a Web browser and filling out the automatically displayed form. See the "Wireless Networking" tab at https://inside.aps.anl.gov/Information-Technology/IT-Service-Catalog for additional information. Wired visitor network connections are also available. The visitor network is separated from the APS network through a firewall and has no access to the internal APS network or internet. Only access to the beamline subnet is permitted.

2.2 Firewall

APS manages a tier 2 firewall to provide security for our network users. All network protocols inbound and outbound are blocked by default. Inbound firewall access (conduits) requires approval from the Laboratory Cyber Security Program Office (CSPO). Contact IT Support if you have questions about firewall rules.

Argonne Business and Information Services (BIS) division manages the tier 1 firewall that connects the Lab to the Internet. The CSPO, BIS and APS network administrators manage the conduits between the tier 1 and 2 firewalls.

2.3 Spam Email

CSPO and BIS manage a pair of anti-spam appliances that quarantine email spam and permit users to manage their own spam filters. These devices are Cisco's IronPort appliances. They are integrated appliances that protect you from spam, viruses, phishing attacks, zombies, hackers and ransomware. Each user can view quarantined spam email with the options to release or delete emails and whitelist known good senders. If any of your incoming email is quarantined as spam, an email message will be sent to your email account at 6:00 am with the subject of "Argonne Anti-Spam Notification". This email will contain a listing of all your email quarantined for that day. See the Argonne Spam Quarantine Knowledge article Using the Argonne Spam Quarantine for additional information.

2.4 Web URL Filtering

The Laboratory's Cyber Security Program Office (CSPO) in conjunction with BIS manage a "web washer" that filters content and detects malicious code. The product uses a worldwide community approach to build a categorized database of hostile web sites and servers that will be checked when web traffic requests from external providers occur from within the Laboratory.

For a full list of the Security Protection Technologies available from the CSPO click on this link:

CSPO Security Protection Technologies

2.5 Private Networks

To improve overall cyber security on the XSD beamlines, the IT group is working closely with beamline staff and the BC and SDM groups in setting up private networks on all BL sectors. This configuration keeps critical equipment that needs to be isolated from public networks and adds an additional layer of protection. In addition, APS IT is working with the BCDA group on private networks for all beamline controls.

2.6 Visiting Computers

Normally, only APS computers connect to APS internal networks. In cases where visiting scientists need to bring their own computer equipment to operate their experiment, the IT group can assist the beamline to support such an arrangement.

3 Computer Accounts

Computer accounts are required for authentication and resource authorization at Argonne and the APS.

3.1 ANL Domain Account

An ANL Domain account is required for authentication to Windows, Mac, and Linux computers in the CLO and XSD LOMs and beamlines, access to the APS Citrix server and APS Oracle applications.

3.2 XRAY Domain Account

An XRAY Domain account is required by beamline service/group accounts for authentication to XSD Windows computers on the Experiment Floor and XSD LOM offices. In addition, the account provides authorization to access beamline resources.

3.3 APS Operations Account

A web link is available on the IT home page https://inside.aps.anl.gov/Information-Technology "Register for an APS Operations Account" to request an APS computer account. The APS Operations Account is utilized in the assigning and authorization of computing resources within the APS environment. You will continue to use your ANL domain account username and password for authentication.

3.4 Local Administration

APS IT recognizes that Windows-based PC workstations are an integral and important part of many beamlines and experiments, and those PCs, by nature, require certain operations to be performed by a user with administrator privileges. This section documents the policies and procedures required for beamline personnel to have local administrator access to their PCs.

1. Who can be a local PC administrator?
    a. Each sector may designate staff members as local PC Window, Linux, and Mac administrators.
    b. Request a local admin account via the Xink ANL-990 form.
2. What workstations are eligible for local administration privileges
   Windows Computers running experiments on the beamline floor may have local administrator accounts if they fall under certain criteria outlined below:
    a. The PC must be connected to, and users authenticated to the XRAY domain.
    b. The PC must be used expressly for the purpose of facilitating an experiment.
    c. The PC is not used at any time as a regular desktop workstation.
3. Local PC administration Best Practices
   If the computer fulfills the requirements detailed above, the designated sector administrator may request a local administrator account for that computer.

   Argonne Cyber Security Rules for local administrator accounts:

    - Never give out the local admin account. As the sector administrator, you are responsible for ALL activity performed on that computer under the local administrator account.
    - DO NOT treat the local admin account as a regular user account. Use a normal user account for all activities, log in as local admin ONLY when an action requires administrative privileges.

- For Windows use the RUN AS command for most of your administrative needs. Software installation, driver installation, and other common admin tasks can be performed in a regular user account, elevated to admin by the RUN AS command.
- Local administration privileges are to be used only for emergencies that affect beamline operations when IT staff is not available to fix the problem.
- Changes made to a PC by a local admin must be documented in an email to IT Support within a reasonable time frame. APS uses automated configuration management tools, and the tools could delete undocumented changes.

4 Beamline Services

4.1 Local Data Storage (Tier 1)

The disk storage attached to the beamline detectors and computers is considered tier 1 storage. Many beamlines find it useful or necessary to store data collected from experiments on local disks or high-performance disk arrays. The IT group can assist in setup and configuration of local storage as required by the beamline experiments**. Please notify IT when user data on local disks needs to be backed up. While the system disks are automatically backed up, additional drives and arrays must be entered into the backup system configuration.**

4.2 NFS – Network File System (Tier 2)

The primary method of accessing files in XSD is via NFS from Linux and Mac workstations. The primary file servers are the NetApp storage appliances. The IT group currently manages multiple petabytes of disk storage for XSD beamlines. This includes shared/general purpose storage (user home directories, software distribution, etc.), as well as disk storage dedicated to beamline data and backup disk arrays.

4.3 CIFS – Common Internet File System (Tier 2)

Access to XSD file systems on the NetApp storage appliances via the CIFS protocol allows Windows users to browse the XSD file systems as if they were on a Windows server. Users can browse to the primary XSD file servers, or can access them directly (e.g., "\\<server name>\<share name>" from the "Start/Run" option).

4.4 Backups

4.4.1 Linux

IT provides a centralized file backup and restore system. All data on the XSD servers (user home directories, scientific data shares, etc.) are backed up as follows:

Small file systems (less than 2 TB):

- Full backups: Mondays starting at 8:00 am
- Incremental backups: Sunday – Saturday, starting at 8:00 am

Large file systems (greater than 2 TB):

- Full backups: once per file system each 30-day maintenance period

- Incremental backups: Sunday – Saturday, scheduled throughout the day to minimize impact on system performance.

In general, data on individual Linux workstations are not backed up – files should be copied from a workstation's local disk to space on a primary file server. Contact IT for backups of Linux systems.

Snapshots

IT takes a weekly snapshot of Linux workstation boot disks. The snapshot can be uses to restore systems from bare metal. The snapshot also serves as a backup of the system configuration and the installed applications.

- Weekly snapshots: Mondays starting at 8:00 am

Code42

Linux laptops are installed with the Code42 client. The client software runs in the background to back up the user's local home directory from the laptop to our Code42 cloud service (Fedramp Moderate). The user may also customize the backup schedule, CPU usage, and add additional directories or files to the backup.

4.4.2 Windows and Macs

The XRAY Beamline computers are backed up to a Code42 cloud service (Fedramp Moderate). This backup system will allow XSD staff the ability to initiate backups for selected data on beamline computers when the systems are not engaged in operating an experiment. This allows beamline computers to be backed up in a way that doesn't impact beamline data acquisition or experiment operation.

4.5 Web Servers

There are several web server options for beamlines at the APS. For a public web presence, the preferred standard is to use the primary APS web server, with a URL such as "https://www.aps.anl.gov/Sectors/SectorN". For non-public, experiment specific or operational information and control, IT maintains an Apache web server that provides a virtual domain for each sector or station, with URLs similar to "https://sectorN.xray.aps.anl.gov" or "https://Nid.xray.aps.anl.gov".

Each beamline that desires one can have a virtual domain created on the XSD web server. Each sector's virtual server is self-contained, and provides a private cgi-bin directory, database support, and more. Each sector has full control over their server and can manage their documents and web applications as they see fit.

The XSD web server provides a rich web environment, including the following features:

PHP

MySQL

Private CGI-BIN directory

Perl

Python

Elog electronic logbook

Elog read-only mirror sites

Contact IT Support if you are interested in setting up a web presence for your beamline or station.

4.6 Distributed Network Services

IT provides servers, known as “dserv” (distributed services) servers for each of the sectors. These servers are dedicated to APS beamlines (both XSD and CAT) and provide the following network services:

- DNS (name service)
- DHCP (dynamic host configuration protocol)
- NTP (network time protocol)
- FTP (file transfer protocol) for booting IOCs
- NFS (for accessing home filesystems, APSshare and IOC-specific file systems)
- CIFS (for Windows access to the same file systems)

The dserv servers and NetApp appliances have network interfaces directly connected to each beamline subnet, so that their services will be available even in the event of a central network failure. For XSD sectors, the dserv provides the boot and operational data for IOCs, storing the IOC configurations as well as automatically saved operational data.

4.7 Data Management Service (DMS)

The APS IT group maintains a cluster of highly available servers that provide the Data Management Service, which is a software system developed and managed by the XSD Scientific Software Engineering and Data Management (XSD-SDM) group. The DMS provides management and movement of beamline data between beamline systems and larger storage systems, XSD Linux clusters, and other Argonne computing and storage resources. It also provides a Globus Online portal allowing outside user groups to transfer data from APS to their home institution over a high-performance Internet connection. Contact the XSD-SDM group for more information.

4.8 Subversion

IT provides a Subversion software version control server (https://subversion.xray.aps.anl.gov). Contact APS IT Support if you would like to have a Subversion repository set up.

4.9 Git

IT provides an APS Git software version control server (https://git.aps.anl.gov). Contact APS IT Support if you would like to access the Git service.

4.10 Commercial/Licensed Software

The following commercial/licensed software is available for XSD Linux, Windows and Mac clients:

- IDL

- IGOR
- Mathematica
- Matlab
- Spec

4.11 Open Source and Other Software

IT supports a wide variety of commercial, third party and open-source software for use by XSD personnel and beamline users. Enter a ServiceNow ticket to request the installation of additional scientific or engineering software.

4.12 Detector Pool

The XSD division maintains a set of detectors that are available for loan to beamlines. The detectors are registered in the Argonne Integrated Host Warehouse (IHW) and will automatically receive an IP number on any XSD beamline network.

4.13 Email List Service

APS maintains a Mailman email list server to facilitate communication and collaboration among APS users. Access the list server via the web at: https://mailman.aps.anl.gov/mailman/listinfo. The main list server page describes the currently available email lists. Note that some lists have a closed membership, and some are "broadcast only" lists, rather than discussion lists. Contact IT support if you would like to create additional lists.

4.14 IOC Console Access

APS-IT and XSD-BC groups maintain a service that provides uniform and controlled access to the consoles of XSD beamline IOCs. Network terminal servers are installed in each XSD sector and provide serial connections to the console port of each IOC at the beamlines in that sector. The program, “iocConsole” allows beamline users to connect remotely to any of the consoles. The iocConsole program also provides history of the output of each IOC console, even when you are not connected to it. The XSD-BC group maintains access controls for the iocConsole software that allows users to access only those IOCs they are authorized to access.

5 Outside Access to XSD Networks

5.1 VPN

VPN (Virtual Private Network) access to XSD computers is available via the ANL VPN appliance. VPN access requires an ANL domain account and Microsoft Authenticator application installed on your smartphone. VPN access cannot be enabled for service/group (shared password) accounts per Argonne’s Cyber Office. The main VPN appliance for the Argonne employees is https://vpn.anl.gov. Submit a Service Desk ticket to request a VPN account. VPN is only permitted from Argonne owned and managed computers that are running Crowdstrike.

5.2 SSH

IT provides multiple SSH servers for accessing XSD beamline computers from the Internet. The domain name for the servers is “https://xgate.xray.aps.anl.gov”.

SSH access requires the Microsoft Authenticator application be installed on your smartphone. You must submit a support ticket for external XSD SSH access. Accounts that have had external SSH enabled, but don't use it for 12 months, will have that access removed from their account per Lab cyber policy. External SSH access for group (shared password) accounts is not allowed per CSPO.

5.3 Data File Download Via FTP

Note: due to DOE cyber guidelines, the ftp service is deprecated. For new requests for data access, please see the “SFTP” section below.

5.4 Data File Download via SFTP

It provides an authenticated SFTP (Secure File Transfer Protocol) server to allow non-APS users to transfer experiment data from the APS to their home institution. SFTP is based on the SSH protocol, and so provides both encryption and compression of transmitted data. XSD beamline staff can create and manage accounts (usernames and passwords) that provide only SFTP access for outside users via the sftpAdmin web-based application (https://ftp.xray.aps.anl.gov/sftpAdmin). A PowerPoint presentation on how to use the application is at https://ftp.xray.aps.anl.gov/sftpAdmin.pptx.

5.5 Globus Online

Globus Online is a high-performance, reliable data transfer protocol optimized for high-bandwidth wide area networks. It is based on the Globus FTP protocol and defines extensions for high-performance operation and security. It is available at https://www.globus.org

Globus-url-copy is the most used client for GridFTP. It's syntax is as follows: globus-url-copy [options] srcURL dstURL The URL rules are: protocol://[user:pass@][host]/path
host can be anything resolvable - IP address,localhost, DNS name

For additional information see https://docs.globus.org

The two GridFTP servers available at the APS are:

Wolf.xray.aps.anl.gov	Internal transfers to/from Orthros
Wolfa.xray.aps.anl.gov	Internal transfers to/from Orthros
Clutchs1.aps.anl.gov	External transfers to/from Orthros
Clutchs2.aps.anl.gov	External transfers to/from/Othros

6 Supporting Beamline Users

6.1 Data transfer

Data transfer to storage systems such as memory sticks and USB-hard drives is often necessary to move large volumes of data offsite. Please contact the IT group if there are any problems during the process.

Data transfers to home institutions are possible via sftp through https://ftp.xray.aps.anl.gov/sftpAdmin

or via GridFTP through clutchs1.aps.anl.gov or clutchs2.aps.anl.gov. The recommended solution for GridFTP is to use Globus Online. See Globus Online documentation https://www.globus.org/data-transfer

7 PC/Workstation/Laptop Configurations

The IT Support group maintains a list of supported hardware configurations for PCs and Workstations at the APS:

https://inside.aps.anl.gov/Information-Technology/Supported-Hardware/PC

Supported desktops, workstations, and laptops are from the business catalogs at Hewlett-Packard and Dell. In addition, SuperMicro computers are supported for specific beamline requirements only, not as a general use computer.

As part of Argonne configuration management requirements, the APS requires that you purchase from the recommended platform list unless you have a specific requirement due to vendor hardware limitations for beamline equipment, which the recommended systems do not provide. In that case, you must contact the IT group leader to have your hardware requirements reviewed.

You can contact the IT group if you would like assistance choosing PC/workstation/laptop hardware configurations.

8 Getting Help

8.1 Service Desk

APS IT utilizes the Argonne Service Desk for requests from all APS users. Please create a ticket whenever you need IT Support. Using the Argonne Service Desk helps ensures requests are tracked from start to finish and allows IT Support personnel to monitor response time, discover trends, and prioritize work. Using the Argonne Service Desk also helps ensure that requests are quickly seen by the proper support personnel, even if the IT staff the user normally works with is sick or on vacation. This system also allows the user or requester to monitor their cases, view who the case is assigned to and view the work log.

The Argonne Service Desk can be accessed from any platform using a web browser at: https://vector.anl.gov. Please login with your ANL domain account username and password. If this fails, call 2-9999 anytime or the Main Control Room (2-9424) after hours or on weekends. In addition, a help request can be emailed to help@anl.gov.

8.2 Out-of-hours support

IT Support provides support for critical applications outside of normal work hours. Out-of-hours support is limited to emergencies that affect the operation of beamline experiments.

Non-APS beamline users should contact their beamline contact person for any problems they experience. Your beamline contact may be able to resolve the problem directly or escalate the problem to APS IT if necessary.

APS beamline users or staff should contact the on-duty Floor Coordinator (x2-0101) for out-of-hours problems. If a Floor Coordinator is not available, they should contact the Main Control Room (x2-

9424) directly.

The Floor Coordinator or MCR operator will evaluate the problem, and let the user know if their problem is related to a known issue (such as a network outage). Otherwise, they will contact the proper on-call IT staff member. The IT staff member will contact you via phone to further evaluate the problem.

8.3 Critical Problems

Whenever a critical problem occurs – one that affects the operation of a beamline or experiment, create an Incident ticket. During normal business hours (Monday through Friday, 8:30 am to 5 pm), you may call the Argonne Service Desk at 2-9999. If outside normal business hours, the procedure for out-of-hours support listed above should be followed.

9 Communication to Beamlines

9.1 System Status Information

The IT Support Group maintains a web page that displays a summary of current network and server operational status. The URL of the page is https://status.aps.anl.gov. IT updates the web page to inform users of current network or computer resource issues that may affect them. This page can also be seen on the APS site-wide TV system.

9.2 Email Notifications

The IT Group will periodically send out broadcast email message to alert users to ongoing problems, or to issue advanced notification of scheduled downtime or maintenance. Messages are sent to every computer account on APS and/or XSD beamline systems.

9.3 Monthly XSD/IT/BCDA/SDM Meetings

Monthly meetings with XSD and the IT, BCDA and SDM groups are held the fourth Monday of each month at 3:30 pm via Teams. Alec Sandy oversees these meetings and the agenda. If you are interested in specific topics, contact Alec to have your topic added to the agenda.

9.4 IT Workshops

Members of the IT group will give workshops on specific topics such as remote access to the APS throughout the year. Notices of upcoming workshops are sent to the email notification lists.