Network configuration of UltraScan-in-a-Box for a single Optima AUC instrument:

The UltraScan-in-a-Box (USiaB) server is a Linux server that provides a complete data analysis and data management environment for AUC experiments conducted with the Beckman-Coulter Optima AUC instrument. The USiaB server is typically integrated into a high-end AMD Epyc server (128 compute cores and 256 GB of RAM recommended, preconfigured systems can be obtained from PSSC Labs in California, contact: alex@pssclabs.com):

1. Fully automated data acquisition, LIMS import, data analysis and refinement, and reporting workflow
2. Web-based LIMS server for data management and custom job submission
3. SLURM-based batch processing of supercomputing analysis jobs
4. MySQL relational database for data management
5. Apache web server for convenient web-based integration with the database
6. MPI-based parallel computing software for high-speed, high-resolution, high-throughput data fitting
7. GUI-based UltraScan desktop software for visualization, post-processing
8. GUI software for remote Optima AUC data acquisition monitoring
9. ssh-tunnel for VNC desktop sharing of user account workspace for remote access
10. openSSL encrypted remote network access for secure data transfers and remote access.
11. nightly push backups of critical server data to remote NAS or CIF mounted storage resource

The USiaB system is maintained and upgraded by AUC Solutions. It includes remote assistance with GMP experimental design, data analysis, and result interpretation, as well as regular software updates and security patches. The USiaB server requires network connectivity to the Internet and to the Optima AUC (on separate networks). To provide all necessary network services, the USiaB server has two ethernet network interfaces with a minimum of 1 Gbps transfer speed. Port 1 is typically connected to the corporate intranet, with outgoing ssh access to 142.66.17.9 enabled. The following basic network services are provided by the USiaB server on port 1:

1. a reverse ssh tunnel service on a specified port above 1000 to enable remote maintenance from 142.66.17.9
2. ssh access for client connections via ssh tunneled VNC service from the UsiaB server to access individual user accounts/desktop interfaces on the USiaB server.
3. SMTP mail service for account registrations, new/forgotten password updates, and job completion notifications (a corporate mail relay access is required).
4. Optional Services not enabled by default:
5. External Apache web service (ports 80 & 443) to allow user access to the LIMS management from the corporate network.
6. MySQL database service (port 3306, ssl-encrypted communications only) to allow remote UltraScan clients to access the LIMS database

On port 2, the USiaB server communicates exclusively with the Optima AUC. The Optima AUC is configured with an on-board Intel I7 server running an outdated Debian distribution (7.8 - wheezy, release date 1/10/2015). The Debian distribution is not patched with security updates, therefore, AUC Solutions strongly recommends to place the Optima on an isolated VLAN or private network to the USiaB server's port 2 network connection. The USiaB Server will firewall the insecure Optima network from the commodity internet. Services provided by the Optima AUC instrument to the USiaB server include:

1. ssh service for remote maintenance access from USiaB
2. PostgreSQL database service (port 5432)
3. UltraScan data acquisition service (port 8827, ssl-encrypted communications only)

4. Tomcat service for Beckman's data acquisition service (port 8888)

To assure data safety and maximum flexibility, we recommend one of three network configurations options shown in Figure 1. The most straight-forward configuration utilizes either a private VLAN or private network with a router/firewall to control access to the USiaB server, and the Optima AUC. Since security patches on the Optima AUC are not managed by Beckman, it is best to connect the Optima with a private, non-routable network to the USiaB server (192.168.x.x or 10.x.x.x). A private network can be configured by directly connecting a cross-over ethernet cable between the USiaB server and the Optima's ethernet port, or by placing both instruments behind a privately managed VLAN or behind a simple router that provides network address translation and its own internal firewall, that can be custom configured. To be clear, the USiaB server is configured with a secure, up-to-date Linux version that is continuously being patched for security updates. Therefore, it is not essential to place the USiaB server behind a separate firewall or into a private network. Depending on configuration chosen, either one or two ports will be required on the USiaB server.

To provide remote maintenance, security patches, software upgrades, and scientific support, ssh port 22 must be open for a privileged user with sudo capabilities. If the hardware is ordered from our preferred vendor, all USiaB software will come pre-installed and turn-key for your network. See last page for required IP address information needed. If you purchase your server hardware through a different vendor, AUC Solutions will need to perform a remote install using Ansible. In order to perform the install, the latest version of Red Hat Enterprise 8 or Oracle Linux 8 need to be installed. See the following link for configuration requirements for the initial Linux installation:

https://docs.google.com/document/d/1tSgrHqFHGRDs7WgtXJp2tGUwJyiRlw4CSE6-ytgKsiA/edit

For the Ansible install it is required to provide ssh access (port 22) from 142.66.17.9 to install the USiaB framework on the compute hardware.

Data Backups: If regular scheduled backups of scientific data are requested, a networked storage device should be mounted on the USiaB server with a writeable partition containing sufficient storage (500 GB - 2 TB depending on user data size). USiaB will push backups to the server using rsync.

Local data access: In addition to direct terminal desktop use, the USiaB server facilitates remote access for an unlimited number of local users. There are two primary ways to access the server:

1. The recommended approach utilizes a ssh tunneled VNC connection from the user's device (which can be either a Windows, Macintosh, Linux, or Android OS) to remotely view a private USiaB GUI display (separate for each user) on the local device. The VNC display is tunneled through a secure ssh tunnel, where access rights are controlled through multi-factor authentication employing username verification by public/private openSSL key pairs installed on the USiaB server (public key) and the user's client computer (private key), and through source IP-based access authentication via the ssh daemon running on the USiaB server. A VNC server running on the USiaB server provides a separate desktop for each user under different display numbers, which are tunneled through the ssh connection to a local port on the user's computer. The user employs a VNC client to connect to the tunneled local port. This effectively exports a different display for each user on the USiaB server so all UltraScan desktop software can be executed directly from the USiaB server, and each VNC connection is encrypted by ssh.
2. The second approach additionally requires port 3306 for the MySQL database, and port 443 for the Apache web server to be open to the corporate network side. It also requires that each user installs and maintains a copy of the UltraScan desktop software on their own laptop or desktop. Although both MySQL and web service (over port 443) is openSSL encrypted, access control is more cumbersome and less flexible compared to managing a single ssh connection.

Option (1) is the recommended approach, because it has a number of key advantages:

1. Data acquisition from the Optima AUC requires a reliable network connection for all instrument related data transfers. A wired, private network between the Optima and the USiaB server is more reliable and secure than a wireless connection, or a mixture of connections from a user's home over VPN, and therefore preferred and highly recommended.
2. The user doesn't need to install and maintain an UltraScan desktop installation on their computer. All

software would be updated and maintained by AUC Solutions for any user.

3. Access control for ssh only is easier to manage than for additional ports needed in option (2).
4. Performance for the desktop UltraScan software running on the Linux-based USiaB server will be much better than on a Windows laptop.
5. Using the UltraScan desktop GUI software on the USiaB server guarantees that the version of the software for GUI operation, the database structures, and the MPI backend for remote batch analysis processing are synchronized across all UltraScan components, avoiding database corruption and failed supercomputer submissions.

Remote LIMS setup (for academic use): For academic installations where the local USiaB server is not suitable for high-performance computing, the USiaB server can be configured to utilize a remote LIMS server and remote HPC resources that are available only for academic use through a XSEDE community allocation grant from Dr. Demeler. This will reduce the cost for the required hardware for the USiaB server (any PC 5 years old or newer, or a virtual machine on the local cloud service can be used). It also requires a compatible Linux installation. In that case all data will be stored on a remote cloud server on the AUC Solution's LIMS server and can be accessed remotely through port 3306, which must be open for outgoing traffic only (in addition to standard ports 80 and 443 for http/https web traffic).

Multiple AUC Instruments: For older instruments like the XLA/XLI Proteomelab, a private network installation is highly recommended (see Figure 2). Since the Windows XP computers are not suitable to be on an open network, a private, non-routable 192.168.x.x network is recommended. The USiaB server will be able to serve all instruments over the network and network shares set up on the XP computers can be mounted on the USiaB server for transparent network access to the XLA/XLI data.

Additional Notes:

For installation at the preferred hardware vendor, the following network information is needed before the hardware can be shipped:

USiaB server: IP address, netmask, gateway, DNS server address for one or more DNS servers, fully qualified domain name/hostname, IP address under which the server will be reachable per ssh from 142.66.17.9, and name and IP address for the SMTP mail relay server.

Optima AUC: IP address reachable from the USiaB server.

Alternatives to external ssh access: After installation, it is possible to close the external ssh port access to the USiaB server, and instead use a reverse ssh tunnel from USiaB to a secure server in Canada to perform any maintenance or customer support. Once installed, the reverse ssh tunnel can be established or shut down as needed by the customer at the remote site.

Multiple AUC instruments: The USiaB platform is able to support data acquisition from multiple instruments simultaneously, and integration of older Proteomelab XLA or XLI analytical ultracentrifuges is also possible. In that case, it makes sense to install all laboratory instruments on a private network and supply one connection from the private network to the second network port on the USiaB server. An example configuration is shown in Figure 2.

Operation on a DMZ network: If remote access, either via direct ssh or reverse ssh tunnel, cannot be established within the corporate network infrastructure due to other corporate network equipment present on the same network segment, an external and separate network connection should be provided that lies in or beyond the corporate DMZ. If network infrastructure cannot accommodate such a network, a wireless 5G service can also be used directly from the USiaB server.

Webserver https certificates: If the customer has the ability to issue certificates, that is preferred. If not, we will setup a self-signed certificate which requires the following information (note the self-signed certificate will present a warning in the user's web browser, an inconvenience, but does not impact functionality)

NTP time server: For the system to maintain a stable time clock, an ntp daemon (chronyd) is used and needs access to an ntp server. If a corporate time server is not available, all UDP ports greater than 1023 will need to be publicly open (so that an external time server can respond). If neither of the above options

are possible, the time will drift and will need to be manually adjusted on a regular basis.

Email / SMTP server: USiaB registration and various server status messages, including job notifications to users, use email. If a corporate SMTP server is not available, mail will be restricted to localhost only, requiring users to find emails on the USiaB server.

Fail2ban: Fail2ban is a utility to scan login attempts and block ip addresses upon failed logins. This can be optionally installed.

The requirement for external ssh access, either directly or with a reverse ssh tunnel, is essential and is an absolute requirement, and cannot be eliminated under the terms of the service provided by AUC Solutions.

On-Site Network Preparation Form

(to be filled out by customer prior to delivery of USiaB server)

Server Operating System:

RHEL 8 or Oracle Linux 8_____

PLEASE NOTE: customers will be required to obtain licenses from RedHat if RHEL is chosen.

USiaB Server Network Configuration:

PLEASE NOTE: The Optima ↔ USiaB network addresses and the USiaB ↔ Corporate network connections should be on separate networks, and the Optima ↔ USiaB network should be on an isolated private VLAN

Fully qualified domain name of host, or local network name: _____

IPv4 address (USiaB – to Optima AUC): _____

IPv4 address (USiaB – to corporate network): _____

Netmask: _____

Gateway: _____

DNS 1, 2: _____

SMTP Server/Mail relay (example: smtp.office365.com): _____

SMTP Port (example: 587): _____

SMTP encryption (example: STARTTLS, SSL/TLS): _____

SMTP credentials username: _____

SMTP credentials password: _____

Internal NTP Time Server IP address: _____

Optima AUC network IP address: _____

IPMI IP address (for remote system management): _____

Webserver certificate information if a self-signed certificate is needed:

Country Name (2 letter code, e.g., US): _____

State or Province Name (e.g., Colorado): _____

Locality Name (eg, Denver): _____

Organization Name (eg, Company name): _____

Organizational Unit Name (eg, AUC Facility): _____

Optional services

Install Fail2ban (yes/no): _____

Configure PAM Authentication (yes/no/need more info) _____

Are you planning to use LDAP or AD authentication (yes/no): _____

Install Advanced Intrusion Detection Environment (AIDE) (yes/no): _____

Install MySQL audit plugin (yes/no, provide plugin configuration – PAM authentication is required): _____

(https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/security_guide/sec-using-aide#sec-Using-AIDE)