CAUDIT

Council of Australian University Directors of Information Technology

Policy on ARCS eResearch Services

Firewall Configuration Requests

(Endorsed by CAUDIT Executive 29 July 2009)

Introduction

ARCS and CAUDIT have together sought to arrive at an agreed set of firewall configurations that will facilitate the provision of ARCS services. The aim of this understanding is to help both ARCS and CAUDIT members be responsive to each other's needs when ARCS services are to be made available to a CAUDIT member.

This is a detailed list of firewall requirements for ARCS services, categorised by System Services, Data Services, Collaboration Services and Authorisation Services. The following requirements are identified:

- Port number or port range
- Protocol (TCP and/or UDP)
- Description of service
- Direction (inbound and outbound)

The direction is assumed to be from the client's (or institution's) perspective. It is important to note that outbound ports (ie. requests initiated from the institution to an ARCS service) are identified, as these are often overlooked.

ARCS Host List

ARCS will provide a list of IP addresses for each service. Institutions are recommended, wherever possible not to implement throttling on these ports.

Port Change Process

ARCS continuously works on developing new and on improving existing tools and services to provide a better experience and new possibilities to researchers. Infrequently, this requires a change in the ports used by ARCS tools and services.
In order to minimize the disruption for researchers, ARCS would like to establish a process which it can use to request a change in firewall settings ahead of time.

System Services

ARCS Systems Services provide the infrastructure to allow researchers to submit computational jobs to the grid, including the staging in and out of data.

Clients will use Grisu (http://www.arcs.org.au/products-services/systems-services/grisu) to access grid services. This limits the number of ports that need to be open. If this option is used, then the following ports are required:

Port	Protocol	Description	Direction
443	TCP	Grisu client communication with Grisu web service. All communication between the Grisu client and grid services occur on this port, including job submission and data transfers. MyProxy[1]. This is required for retrieval of user credentials stored on the MyProxy server.	Outbound
7512	TCP	MyProxy. This is necessary if a **direct** connection on port 443 is not possible.	Outbound

[1] MyProxy currently does not support http proxies, it requires a direct connection.

Data Services

The ARCS Data Services Team provides Australian researchers with tools and services that allow researchers to easily transfer, store, manage and share data (http://www.arcs.org.au/products-services/data-services/arcs-data-fabric-start-here). The two principal technologies are gridFTP for robust and high performance data transfers and iRODS for storing, managing and sharing data. To get best performance, clients are required to allow the following ports:

Port	Protocol	Description	Direction
80	TCP	WebDAV/OPeNDAP	Outbound
443	TCP	WebDAV/OPeNDAP (ssl)	Outbound
2811	TCP	gridFTP Control Channel. This port is used for control commands between the client and the gridFTP server.	Outbound
3306	TCP	MySQL	Outbound
5000	TCP	Alternate gridFTP Control Channel.	Outbound
5432	TCP	PostgreSQL	Outbound
1247	TCP	iRODS Server.	Outbound
ARCS will provide a list of ports in the range 40000-41000	TCP	Data Channels for both gridFTP and iRODS Agents. These ports are used for the actual data transfers between the client and the gridFTP server.	Outbound for passive transfers (possible) Inbound for active transfers (recommended)

Collaboration Services

The ARCS Collaboration Services Team support a wide range of tools and services that allow and promote the collaboration of researchers with inter-institutional, interstate and international colleagues. These tools and services support video, voice and web-based collaboration.

Port	Protocol	Description	Direction
80	TCP	Web collaboration tools – eg. Sakai, Wiki, Plone, etc	Outbound
46015	UDP	EVO – All video conferencing traffic, including video, audio, chat, etc. is tunnelled through this port. Due to the real-time nature of video conferencing, UDP performs better than TCP and is highly recommended over TCP. If UDP is not possible, then TCP is requested.	Outbound
Optional Ports			
4042, 4043, 4044, 10090, 60001, 60002, 60003	TCP	These ports enable EVO to detect the network conditions and connect the user to the best Panda server. They only need to be opened to a limited number of hosts.	Outbound
46012	TCP	This port is needed by EVO to allow file-sharing between users. If a TCP connection, initiated by the client, can not be made on this port, the file sharing plug-in will be disabled.	Outbound
25 (optional)	TCP	Sending EVO log files back to ARCS helpdesk for troubleshooting purposes. Limited to one host.	Outbound

Authorisation Services

Authorisation Services role includes implementing unified authorisation mechanisms for ARCS and research groups based on use of the AAF which uses Shibboleth. Ports required by Shibboleth are those associated with secure (i.e. https) browser-based interactions, secure back-channel SAML transactions using SOAP.
It is envisaged that Australian universities may perform roles of both Identity Provider (IdP) and Service Provider (SP). The requirements **for the machines hosting the IdP and SPs** are:

Port	**Protocol**	**Description**	**Direction**
443	TCP	HTTPS browser-based transactions	Inbound / Outbound
8443	TCP	HTTPS 'back channel' SAML transactions	Inbound (IdP)

Time synchronisation is a critical aspect of IdP-SP interactions, and use of NTP is recommended to ensure synchronisation of IdP or SP servers across the Federation. This requires servers to have access to UDP port 123 in both directions.

Port	**Protocol**	**Description**	**Direction**
123	UDP	Network Time Protocol	Inbound / Outbound