

May 9, 2006

Computer Resources Policies at the Center for functional MRI

Highlights of the policies, for more information please check each attachment.

1. Computer resources (attachment 1),
 - a. Online resources are expensive and limited.
 - b. Each internal PI/Scientific Staff has 30G limit on one of the servers (cfmri or fmriserver),
 - c. Outside PI has a 10G limit on one of the servers (cfmri or fmriserver).

2. Data backup (attachment 2)
 - a. Backup is mainly provided for disaster recovery. We strongly recommend that internal and external PIs always back up their raw data.

3. Security (attachment 3)
 - a. Remote access to our server is only available to UCSD domain and strongly affiliated recharge institutions (such as SDSU, and SALK), Access from home has to be through the UCSD VPN connections.
 - b. No one should be given access to CFMRI computers without first consulting with Eman Ghobrial the Center System Administrator. All the servers have very critical information and there is nothing worse than a physical breach.
 - c. All servers have a virus scan and firewall software, PIs are responsible to make sure that their workstation is compliant with the minimum UCSD security requirements.

May 9, 2006

Attachment 1

File Servers at the center of fMRI

1. The center currently has 4 main servers
 - a. fmrserver (new replacement for oldfmrserver, with accounts for half of the internal + external users and the mirror website)
 - b. cfmri (one and half year old server, with accounts for the other half of the users)
 - c. fMRIwebapp (server for the webapps)
 - d. cfmriweb (the main website)
 - e. Our experience shows that average life time for any server (with the center load) is around three years. The current server prices allow us to keep two relatively new servers at any given time and retire the older servers

2. fmrserver and cfmri each have a guest account that can be used in case one of the servers is down.

3. Data storage allocation:
 - a. Online resources are expensive and limited.
 - b. Each internal PI/Scientific Staff has 30G limit on one of the servers (cfmri or fmrserver),
 - c. Outside PI has a 10G limit on one of the servers (cfmri or fmrserver).

 - d. PIs who need more space allocation should try to use their own funds, and if no other funds are available they should talk to the center director.

4. Non active accounts will be deleted one month after the PI's affiliation ends. PI will be notified one week before deleting the account.

May 19, 2005

Attachment 2

General Data Backup Guidelines at the Center

1. Data backup is provided at the center every night for the three servers (cfmri (/mnt/raid3, fmriserver /mnt/raid6 and fmriwebapp /mnt/raid5).
2. We recycle the tapes and our retention period varies from one month to six month according to how much data we have on the server we backup.
3. Backup is mainly provided for disaster recovery, so we strongly recommend that internal and external PIs always back up their raw data.
4. Instructions for how to backup will be available on the web site for different Operating Systems.

May 9, 2006

Attachment 3

Computer Security at the center

As of 1 January 2005, all devices attached to the UCSD network must meet the minimum standards for security, basically OS updates, virus scan protection and personnel firewall for more information check the following site:

<http://www-no.ucsd.edu/security/minstds/index.html>

All Machines at the center now have some type or another of a firewall.

Windows Symantec AntiVirus **Macs** Build in firewall.

Linux/Unix servers and workstations IP Chains/tcpwrappers.

Allowed traffic for only ssh port (22) for ucsd.edu domain, and strongly affiliated recharge group (such as sdsu, and salk).

To get remote access from home use the VPN client, information can be found at:

<http://www-no.ucsd.edu/documentation/vpn/>

What is /Why firewalls?

A host-based firewall is software that runs directly on a networked device and protects that device against attack from the network by controlling incoming and/or outgoing network traffic. Host-based firewalls work by monitoring, passing, or blocking incoming and outgoing network packets. Rules govern what to look for and what to block or pass. Typical firewalls block based on source and destination address and port, packet type, etc.

Note that as of March 2006 the ports (6000-6010) for X-forwarding does ****not**** need to be open and not secure to be open.

Please use the ssh command with the `-X` options which tunnel the X-windows traffic over port 22 ex:

```
ssh -X <username>@<servername>.ucsd.edu
```

Mac users please use ssh `-Y` <username>@<servername>.ucsd.edu