

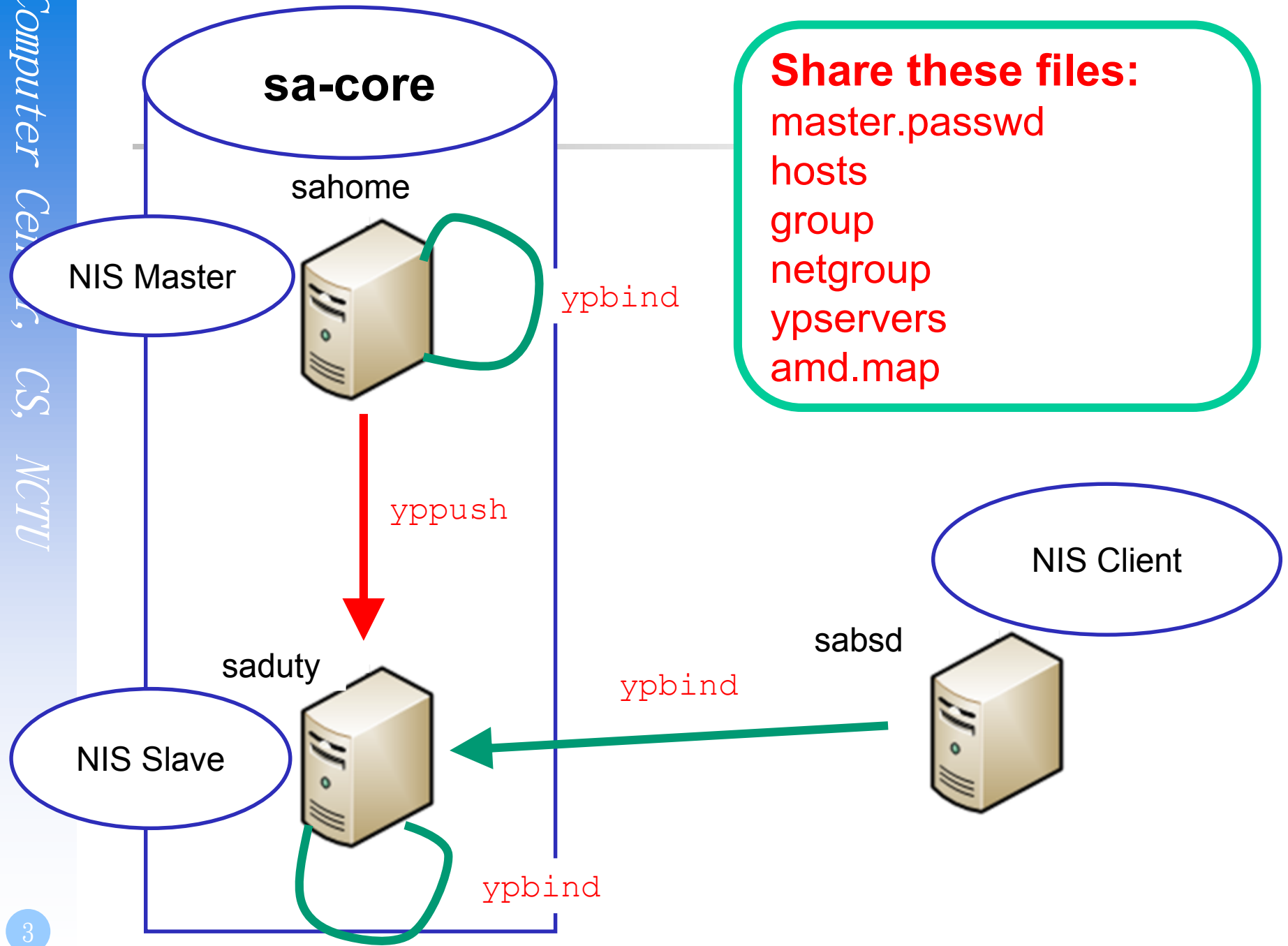


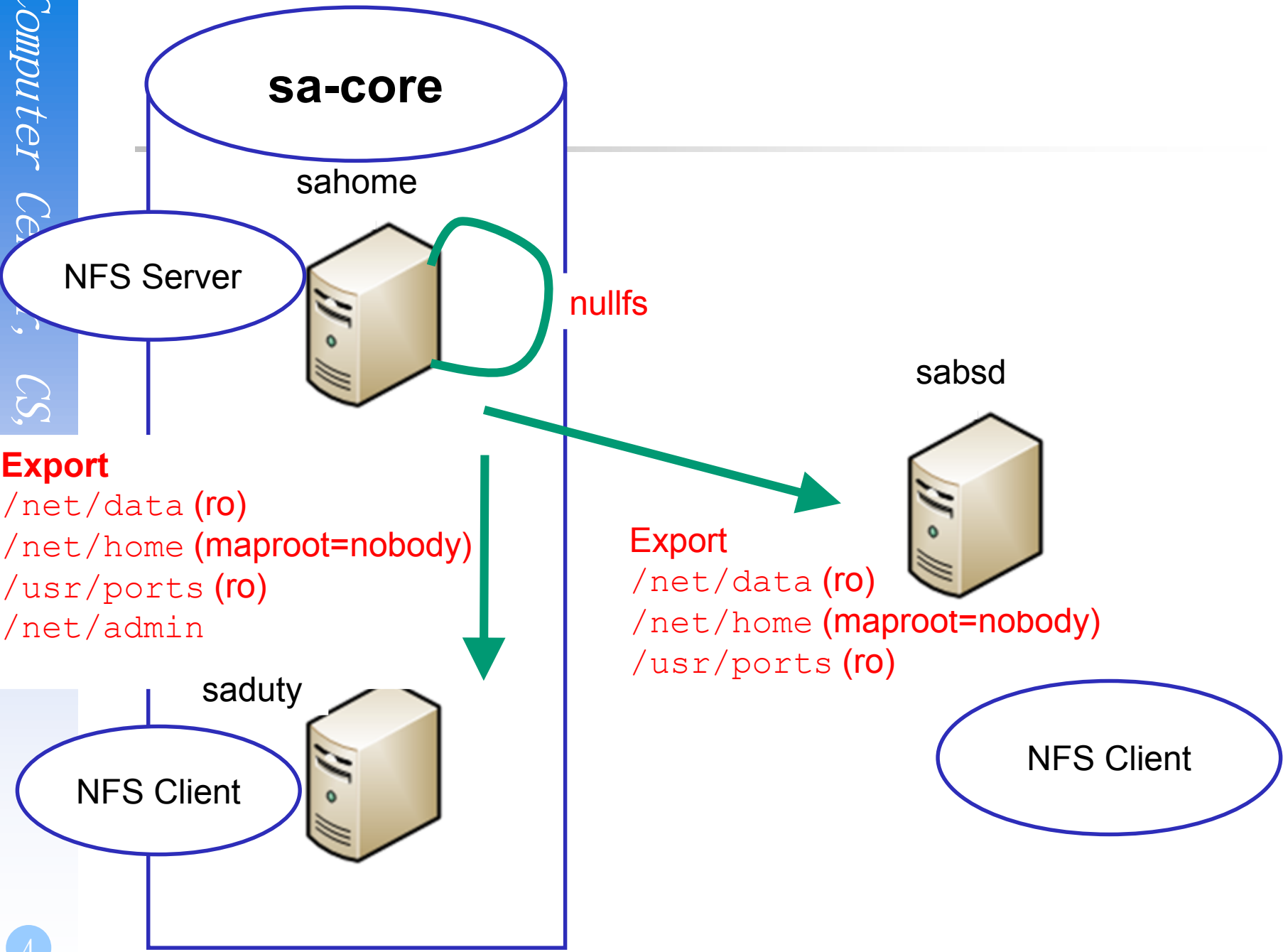
System Administration Homework 5 - Micro Computer Center

yml / shunyi / chihhsin / hlku / shhu

2014-12-11

Briefly View





sa-core

sahome

NFS Server

nullfs

sabsd

Export

- /net/data (ro)
- /net/home (maproot=nobody)
- /usr/ports (ro)
- /net/admin

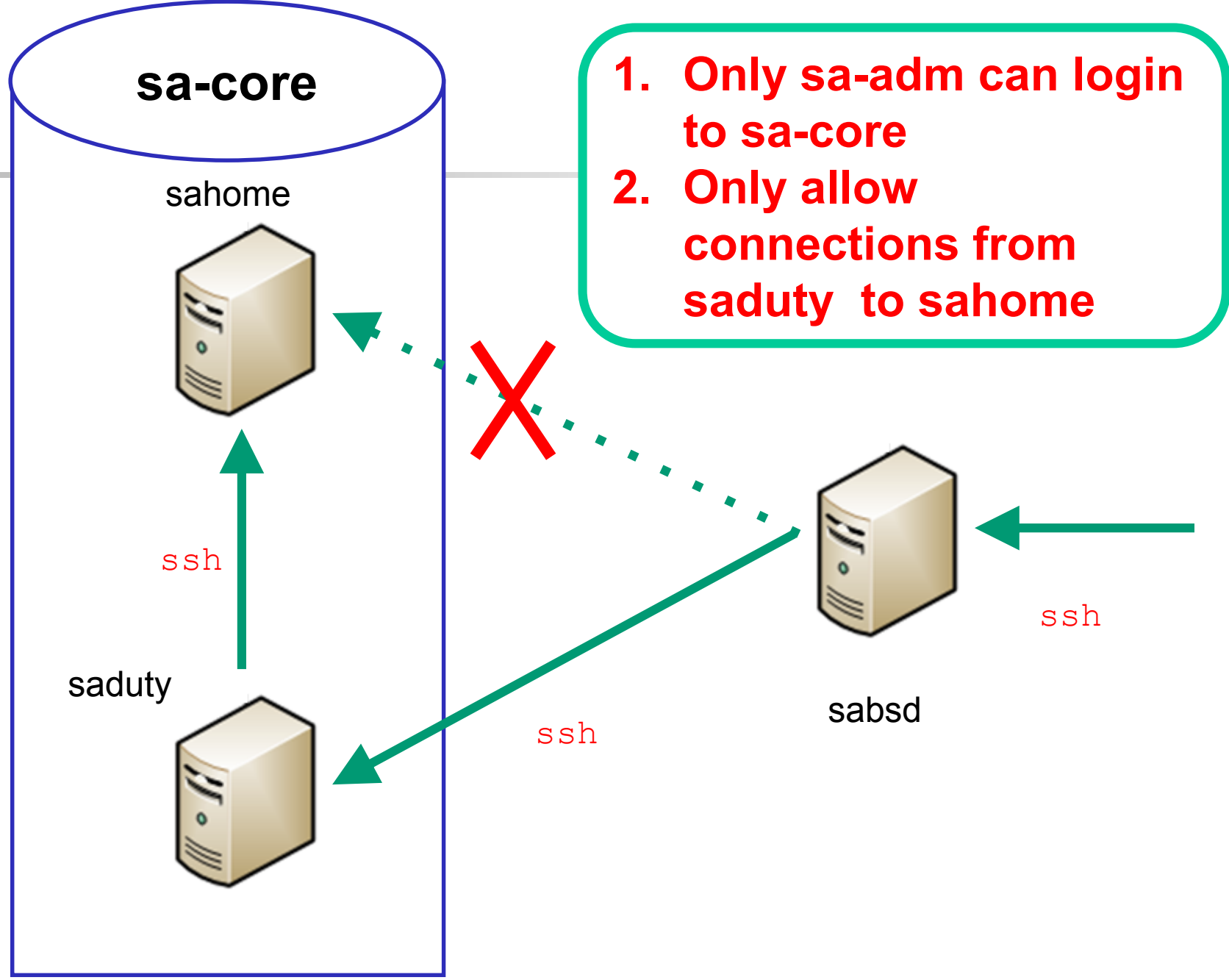
Export

- /net/data (ro)
- /net/home (maproot=nobody)
- /usr/ports (ro)

saduty

NFS Client

NFS Client



Grading

- ❑ Base requirement (80%)
- ❑ Advanced requirement (20%)
- ❑ Bonus (15%)

Base Requirement

Base requirement (1/5) - Overview

❑ Machines

- sahome: NFS **server**, NIS **master**
- saduty: NFS client, NIS **slave**
- sabsd: both NFS / NIS client

❑ Groups

- sysadm: can access `/net/data/sata`
- nctucs: normal user
- samaster: god

❑ Netgroups

- sa-adm: admin **users**, can login **sa-core**
- sa-core: core **machines** (sahome and saduty)
- sa-bsd: all freebsd **machines** (sahome, saduty, sabsd)

Base requirement (2/5) - sahome

❑ NFS (server)

- nullfs
 - /net/home -> /vol/home
 - /net/data -> /vol/data
 - /net/admin -> /vol/admin (only share to saduty)
- share /usr/ports

❑ NIS (master)

- Bind priority: sahome > saduty (bind itself first)

❑ login

- sa-adm only
- only from saduty

Base requirement (3/5) - saduty

❑ NFS (client)

- `/net/home` -> `sahome:/vol/home` (`maproot=nobody`)
- `/net/data` -> `sahome:/vol/data` (`ro`)
- `/net/admin` -> `sahome:/vol/admin` (`ro`)
- `/usr/ports` -> `sahome:/usr/ports`

❑ NIS (slave)

- Bind priority: `saduty` > `sahome` (also bind itself first)

❑ login

- `sa-adm` only

Base requirement (4/5) - sabsd

❑ NFS (client)

- `/net/home` -> `sahome:/vol/home` (`maproot=nobody`)
- `/net/data` -> `sahome:/vol/data` (`ro`)
- `/usr/ports` -> `sahome:/usr/ports`

❑ NIS (client)

- Bind priority: `saduty>sahome`

❑ login

- All

Base requirement (5/5)

- 1** member as a team (build 3 VMs yourself)
- All machines share `/net/data/sudoers`
- All user's home directory must be in `/net/home/`
- Auto-start all services
- Auto-mount all folders
- Users can change their passwords on NIS clients
- You can run `rup` command on all servers
- Export `sahome`'s ports tree and automatically update that
- Logging at `sahome`

Advanced Requirement

Advanced requirement (1/6) - Overview

- sudo
- FTP service
- web server
- backup service
- build kernel

Advanced requirement (2/6) - sudo

- ❑ share the sudoer file via NFS
 - `/net/data/sudoers`
- ❑ different permissions
 - **sysadm**
 - `ls, cat, top, renice, kill`
 - `reboot, shutdown`
 - `sudoedit`
 - **samaster**
 - ALL commands on any machine
 - **nctucs**
 - not a sudoer

Advanced requirement (3/6) - ftp

- ❑ Provide FTP service
 - FTP over TLS
 - Chrooted in users' home directories

Advanced requirement (4/6) - web

- ❑ Let saduty provide web service (Apache or Nginx)
 - Make the UserDIR work
 - UserDIR location is `$HOME/public_html`
 - Note the `$HOME` directory is shared by NFS

Advanced requirement (5/6) - backup

- ❑ Use rsync to archive users' home directories on sahome
- ❑ Write a script to backup users' home directories every 4 hours
- ❑ The backup files should be put in `/net/data/backup/`
- ❑ We only maintain 10 copies
 - hourly.0 (latest backup)
 - hourly.1
 - ...
 - hourly.9

Advanced requirement (6/6) - kernel

- ❑ Build your own kernel!
 - Compete with your classmates!
 - The smaller, the better!
 - Make sure everything is still okay

```
chcbsd :) ~
starbops $ ls -l /boot/kernel/kernel
-r-xr-xr-x  1 root  wheel  14646999 Dec 10 19:59 /boot/kernel/kernel*
chcbsd :) ~
starbops $ ls -l /boot/kernel.old/kernel
-r-xr-xr-x  1 root  wheel  20524796 Dec 10 19:20 /boot/kernel.old/kernel*
```

Reference Steps

Step 1 - Setup sahome as NIS Master Server

❑ Edit `/etc/rc.conf`

- `nis_server, nisdomainname, yppasswdd`

❑ Edit `/var/yp/Makefile`

- `#NOPUSH = "True"`
- `HOSTS = $(YPPDIR)/hosts`
- `GROUP = $(YPPDIR)/group`
- `AMDHOST = $(YPPDIR)/amd.map`

❑ Create `/var/yp/hosts, /var/yp/group...etc`

- **Edit `/var/yp/master.passwd` & `/var/yp/group` to create your accounts**
- **Edit `/var/yp/hosts` to fit your environment**

❑ Initial and start services

Step 2 - Setup NIS Clients

- ❑ Add NIS Servers' IP to `/etc/hosts`
- ❑ Edit `/etc/master.passwd` & `/etc/group`
 - `vipw`
- ❑ Edit `/etc/nsswitch.conf`
 - `hosts : files nis dns`
- ❑ Edit `/etc/rc.conf`
 - `nis_client, nisdomainname, ypbind`

- ❑ Testing tools
 - `ypcat`
 - `ypwhich`

Step 3 - Setup NFS environment

❑ nullfs (NFS Server)

- `$ mount_nullfs /vol/home /net/home`
- **Edit `/etc/fstab`:** `/vol/home /net/home nullfs rw 2 2`

❑ Edit `/etc/exports` (NFS Server)

❑ Edit `/etc/rc.conf`

- `amd` (NFS Client)
- `nfs_server`, `mountd` (NFS Server)

❑ Edit `amd.map` (NIS Server)

❑ Testing tools

- `showmount`

Step 4 - Setup saduty as a NIS Slave Server

- Edit** `/etc/rc.conf`
 - `nis_server, nisdomainname, ypxfrd`
 - **Modify ypbind priority (on every clients)**
- Edit** `/var/yp/ypservers` (on sahome)
- Initial and (re)start services**

Step 5 - Finishing

- ❑ `sudoers (/usr/local/etc/sudoers)`
 - Include shared sudoers file from `/net/data/sudoers`
 - `man sudoers` to see more about “include”
- ❑ `sahome:/etc/hosts.allow`
 - `sa-adm` only can login `sahome` from `saduty`
- ❑ `/net/data/sata`
 - `sysadm` only
- ❑ Login permissions
 - only `sa-adm` can login `sa-core`

After NIS & NFS Servers

After NIS & NFS servers

- Rup
- Ports tree
- Log server

Rup

- ❑ You can run `rup` on all servers
- ❑ `rup (1)`

```
16:25 hwchiu@sahome [~] >rup
saduty      4:25pm  up           1:13,  load average: 0.00 0.00 0.00
sabsd       4:25pm  up           33 mins, load average: 0.00 0.00 0.00
sahome      4:25pm  up           4 mins,  load average: 0.04 0.26 0.16
```

Ports tree

- ❑ `sahome`: exports its `/usr/ports`
 - write a script to update the ports tree automatically
 - It must be executed at 1:30 A.M everyday

- ❑ `sa{duty,bsd}`: mount or link the shared ports tree to `/usr/ports`
 - `/etc/make.conf`
 - `DISTDIR`
 - `WRKDIRPREFIX`
 - able to install stuffs with the shared ports tree

Log server

- ❑ sahome as a Log server
- ❑ write a script to parse ssh logs automatically
 - When
 - Who
 - Where
 - E.g.: Dec 14 17:26:10 hwchiu login saduty fail from 192.168.157.139
 - It must be executed at 11:30 P.M everyday on sahome

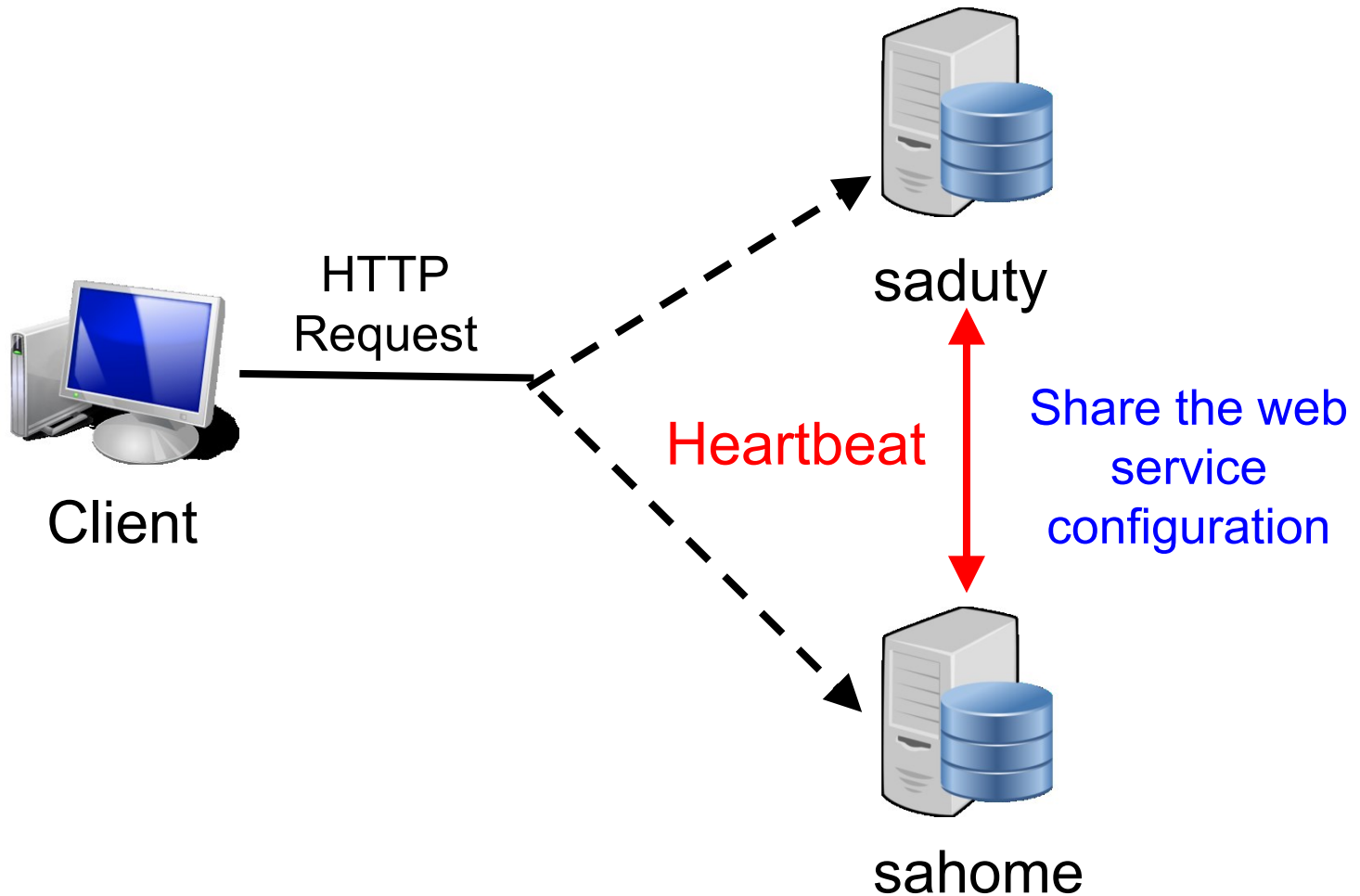
Log server (cont.)

- ❑ Your script should record the result to `/net/data/ssh/`
- ❑ The filename should be the format as following
 - Year_Month_Day
 - Example: 2014_Dec_13

```
/net/data/ssh/  
├── 2013_Dec_13  
├── 2013_Dec_14  
└── 2013_Dec_15
```

Bonus & Appendix

Bonus: web server HA



Appendix A – mount_nullfs

❑ \$ man exports

A host may be specified only once for each local file system on the server and there may be only one default entry for each server file system that applies to all other hosts.

❑ The command

- `mount_nullfs <origin> <new_path>`
- For example
 - `% mkdir /home/allhome` make a directory for Real NFS Home
 - `% mkdir /home/for_nis` make a directory for NFS Home exports
 - `% mount_nullfs /home/allhome /home/for_nis` mount it

❑ Use it in /etc/fstab

- Change the fstype to nullfs
- For example
 - `/home/allhome /home/for_nis nullfs rw 2`

Demo

- Demo sheet will be available next week.
- Demo before **2015/01/09 (Fri.)**

 Will have another homework due by 2015/01/19

Help

- ❑ Go to bsd*.cs.nctu.edu.tw

- ❑ IRC channel #nctuNASA on freenode
- ❑ BBS bs2.to board CS-SysAdmin
- ❑ Email ta@nasa.cs.nctu.edu.tw
- ❑ Goto CSCC to ask professional 3F!

- ❑ Read this article before you asking a question:
 - <https://code.google.com/p/smartquestions/> (Traditional Chinese)
 - <http://www.catb.org/~esr/faqs/smart-questions.html> (English)

Q & A