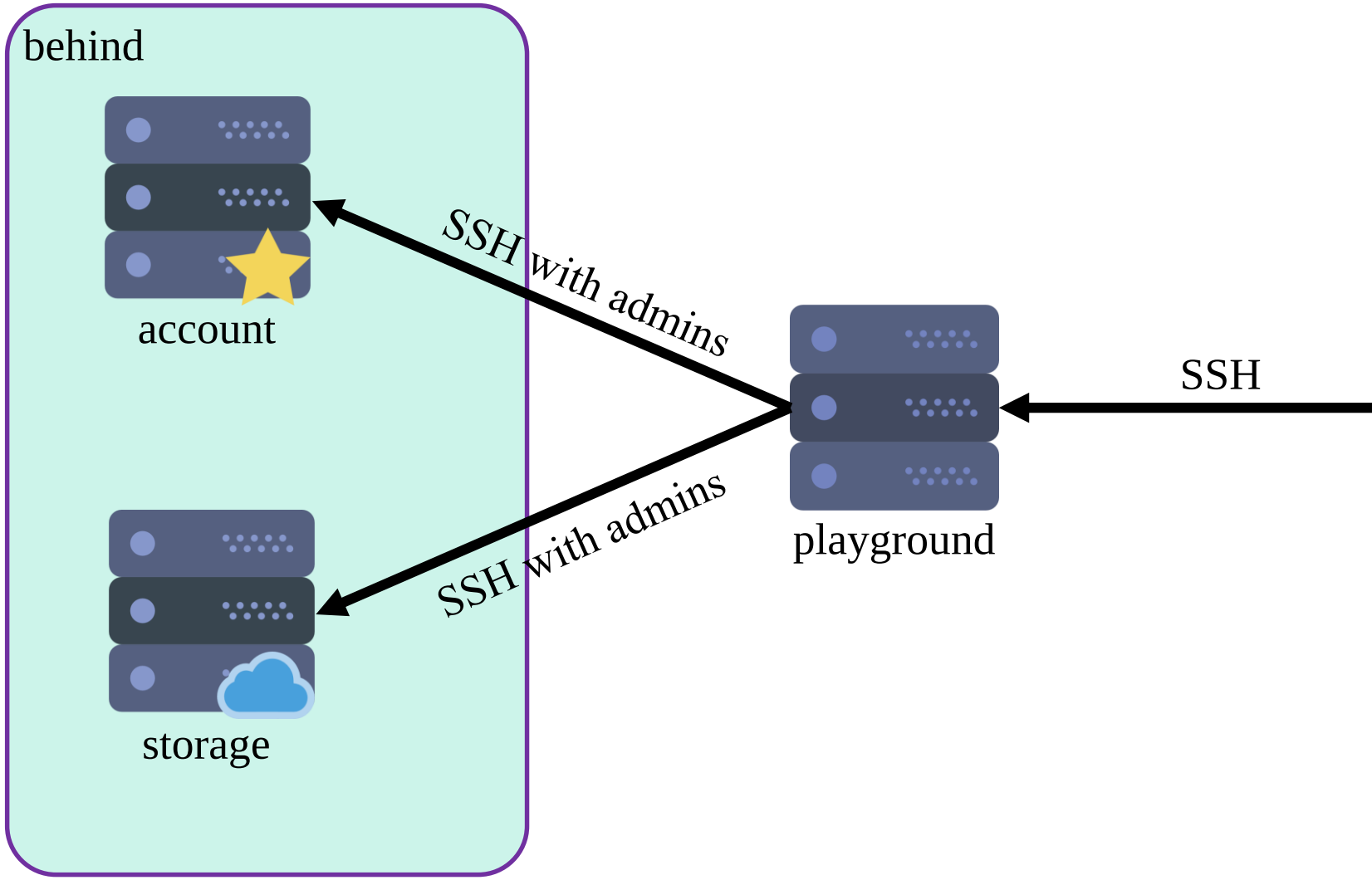
System Administration HW5

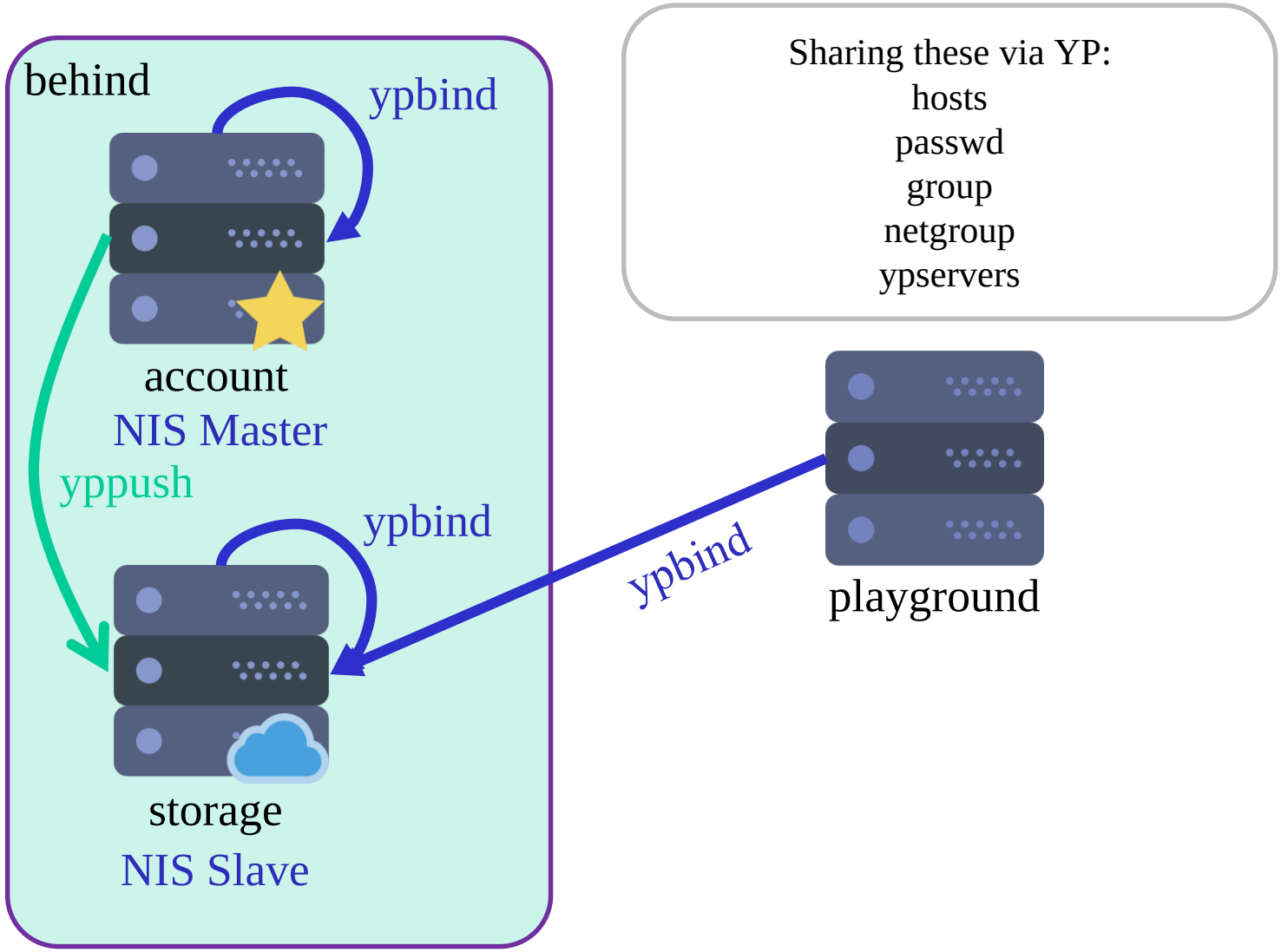
- Mini Private Lab

tzute

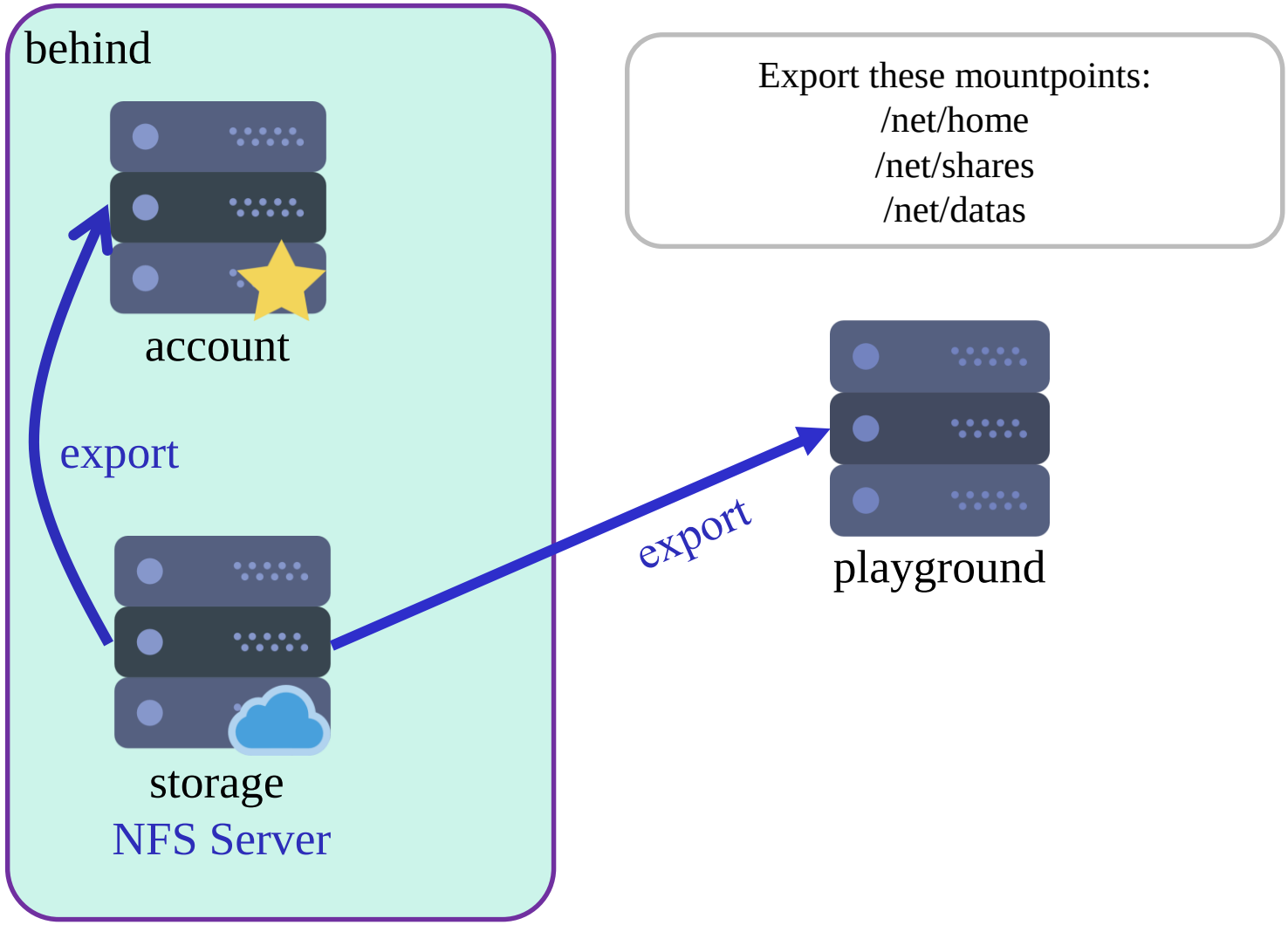
Architecture Overview (1/3)



Architecture Overview (2/3)



Architecture Overview (3/3)



Requirements (1/7) - Overview

- Machines
  - account: NIS Master Server, (NIS/NFSv4 Client)
  - storage: NFS Server, NIS Slave Server, (NIS/NFSv4 Client)
  - playground: NIS/NFSv4 Client
- Groups
  - acctadm: can sudo inside "account"
  - storadm: can sudo inside "storage"
  - users: can access /net/shares
- Netgroups
  - admins: admin users, can login behind
  - behind: machine "account" and "storage"
  - front: machine "playground"

Requirements (2/7) - Overview

- Users
  - god
    - ✓ Group: acctadm, storadm, users
    - ✓ Netgroup: admins
  - <student-id-A>
    - ✓ Group: acctadm, users
    - ✓ Netgroup: admins
  - <student-id-B>
    - ✓ Group: storadm, users
    - ✓ Netgroup: admins
  - user
    - ✓ Group: users

Requirements (3/7) - Account

- NFSv4
  - storage:/net/home (maproot=nobody)
  - storage:/net/shares (all_squash, anonuid=user, anongid=users)
  - storage:/net/datas (rw)
- NIS
  - Bind priority: account > storage
- login
  - ssh from playground only
  - ssh by admins only
  - sudo with acctadm only

Requirements (4/7) - Storage

- NFSv4
  - exports
    - ✓ /net/home
    - ✓ /net/shares
    - ✓ /net/datas
- NIS
  - Bind priority: storage > account
  - Slave of account
- login
  - ssh from playground only
  - ssh by admins only
  - sudo with storadm only

Requirements (5/7) - Playground

- NFSv4
  - storage:/net/home (maproot=nobody)
  - storage:/net/shares (all_squash, anonuid=user, anongid=users)
  - storage:/net/datas (ro)
- NIS
  - Bind priority: storage > account
- login
  - ALL

Requirement (6/7)

- All machines share /net/datas/sudoers
- All user's home directory must be in /net/home except root
- Auto-start all services
- Auto-mount all folders with autofs

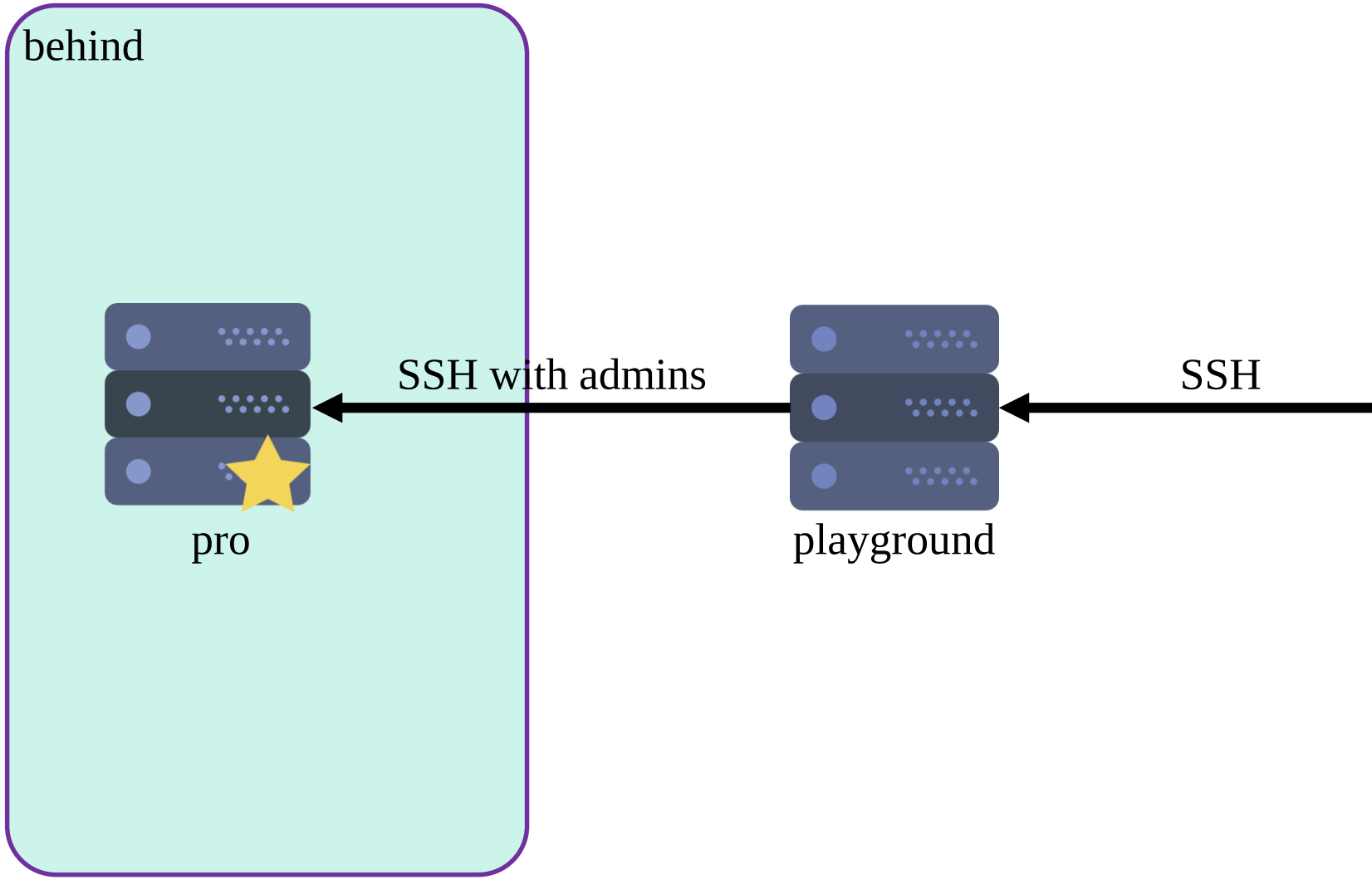
Requirement (7/7)

- NFSv4 with nfsuserd for mapping uid and username
- /etc/exports must be NFSv4 format
- User can change password on NIS Clients
- NIS share file must be in /var/yp/src
  - configure /var/yp/Makefile

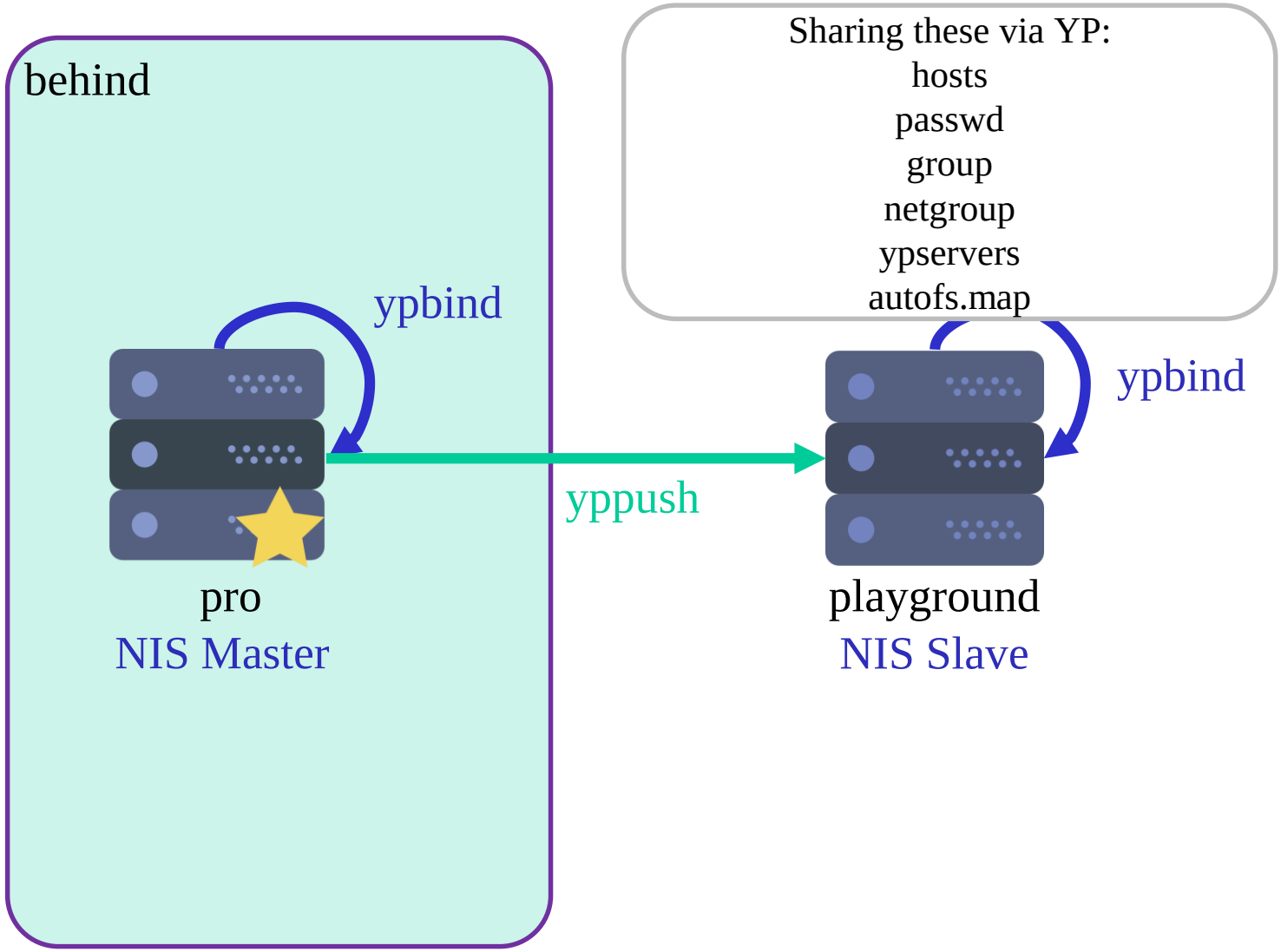
Single Player Team

- If you are in a single player team, here are some boost for you
  - Combine account and storage as machine named "pro"
  - Make playground as NIS Slave like the original storage

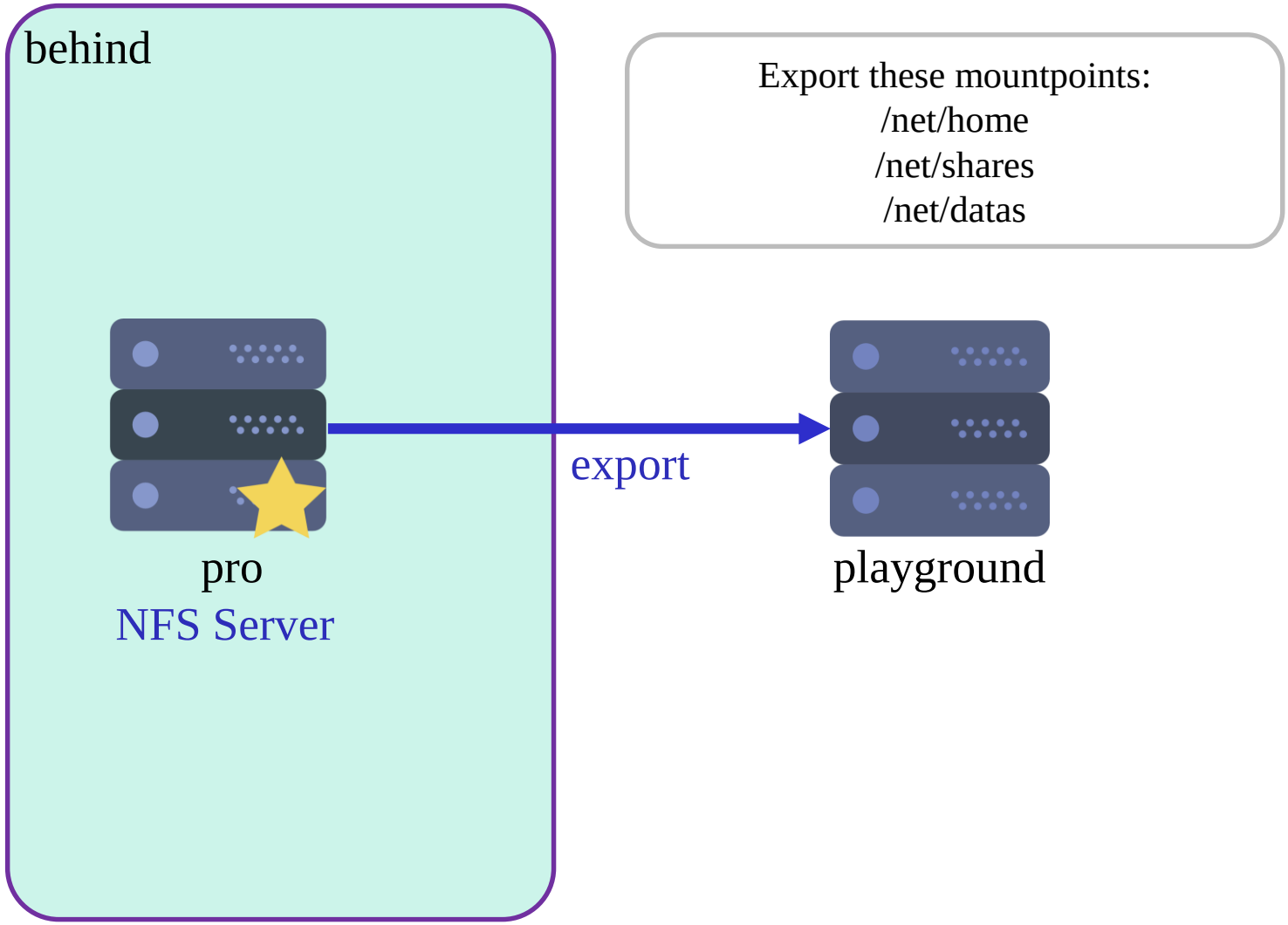
Architecture Overview (1/3)



Architecture Overview (2/3)



Architecture Overview (3/3)



Step 1 - Setup NIS Master Server

- Edit /etc/rc.conf
  - nis_server, nisdomainname, yppasswdd
- Edit /var/yp/Makefile
  - #NOPUSH = "True"
  - $(YPSRCDIR) = < to be modified >
  - TARGETS = < to be modified >
- Create /var/yp/src/hosts, /var/yp/src/group…etc
  - Edit /var/yp/src/master.passwd & /var/yp/src/group to create your accounts
- Initial and start services
  - ypinit
  - service [ypserv | ypbind | rpcbind] [start | restart | stop]
  - services started order is important!

Step 2 - Setup NIS Clients

- Add NIS Servers' IP to /etc/hosts
- Edit /etc/master.passwd & /etc/group
  - vipw
  - vigr
- Edit /etc/nsswitch.conf
  - hosts : files nis dns
- Edit /etc/rc.conf
  - nis_client, nis_client_flags, nisdomainname
  - Modify ypbind sequence (on every clients)
- Testing tools
  - ypcat
  - ypwhich

Step 3 - Setup NIS Slave Server

- Edit /etc/rc.conf
  - nis_server, nisdomainname
- Edit /var/yp/ypservers (on cshome)
- Initial and (re)start services
  - ypinit

Step 4 - Setup NFSv4 environment

- Edit /etc/rc.conf
  - autofs (NFS Client)
  - nfs_server, mountd, nfsv4_server, nfsuserd, nfsuserd_flags (NFS Server)
- Edit /etc/exports (NFSv4 Server)
  - Must be NFSv4 format
- Edit autofs.map / amd.map

Step 4 - Setup NFSv4 environment (Cont.)

- Initial and start services
  - service [rpcbind | nfsd | nfsuserd | mountd] [start | restart | stop]
- Do something for mapping uid/gid and user/group
  - nfsuserd

Step 5 - Finishing

- sudoers (/usr/local/etc/sudoers)
  - Including other sudoers file from /net/data/sudoers
  - man sudoers to see more about “include”
- Login permissions
  - only admins (netgroup) can login behind
- /etc/hosts.allow
  - only can login behind from playground
- /net/shares
  - Squash all as user:users
- If you restart rpcbind, all of service based on rpc also need to restart

Bonus - Share autofs.map

- Share autofs.map via yp with automountd
  - yp key map name
    - ✓ auto_behind for account
    - ✓ auto_front for playground
  - ypcat -k auto_behind
  - auto_master
    - ✓ +auto_behind
- Hint
  - man auto_master

Bonus - Script to create account

- Write a script to create accounts on NIS
  - random password
  - read from <account_info> file only contain username, fullname
    - e.g. bigwang, Da-Chui Wang
  - define group by args
    - e.g. ./autocreate users <account-list.txt>
  - user home directory must be created on NFS
  - you can use any language to implement

Deadline

- 2019/1/15
- You do not need to submit anything

Checklist (1/2)

- Service auto start (5%)
- SSH limitation (10%)
  - Only can login behind from playground (5%)
  - Only admins can login behind (5%)
- Sudo (15%)
  - acctadm can sudo in account (5%)
  - storadm can sudo in storage (5%)
  - Sharing and including /net/datas/sudoers (5%)
- NIS (30%)
  - Bind priority (5%)
  - Slave configured (5%)
  - passwd on client (10%)
  - File sharing (10%)

Checklist (2/2)

- NFS (40%)
  - Export using NFSv4 (5%)
  - Mount storage:/net/home as nobody (5%)
  - Mount storage:/net/shares and squash all as user:users (5%)
  - Mount storage:/net/datas with rw on behind (5%)
  - Mount storage:/net/datas with ro on playground (5%)
  - Auto mount all folders (10%)
  - Mapping uid and username (5%)
- Bonus (20%)
  - Sharing autofs.map via yp with automountd (10%)
  - Account creating script (10%)

Help

- E-mail ta@nasa.cs.nctu.edu.tw
- New E3 https://e3new.nctu.edu.tw/
- Office hour: 3GH at EC320

Appendix

❑ Virtualbox Network Type Comparison

	VM ↔ Host	VM1 ↔ VM2	VM → Internet	VM ← Internet
Host-only	+	+	–	–
Internal	–	+	–	–
Bridged	+	+	+	+
NAT	–	–	+	Port forwarding
NAT Network	–	+	+	Port forwarding