PCN Self-supported Workstation Installation

CERN CentOS 7 (CC7) Installation

System Installation

Follow the instructions on http://linux.web.cern.ch/linux/centos7/docs/install.shtml

1. Create a boot image for a 64 bit system
2. Reboot your computer and press F2 (F12) at startup
3. In the BIOS setup add CD/DVD to boot devices; save BIOS setup and reboot
4. Select **http** as installation method
5. Installation server is: linuxsoft.cern.ch
6. Installation path is: /cern/centos/7/os//x86_64/
7. Keep default partition layout
8. Set host name to **xxx**.physics.purdue.edu: e.g. serret.physics.purdue.edu
9. Enable network time protocol (server: harbor.ecn.purdue.edu)
10. Set Time Zone to: America/Indianapolis
11. Router: 128.210.67.1
12. Name servers: 128.210.11.5, 128.210.11.57

Customize System

Download configuration file config.tar.

```
cd /
tar --list --file=config.tar
tar xvf /config.tar

sed -i.bak "s/xte/xxx/g" /etc/hosts
sed -i.bak "s/xte/xxx/g" /etc/sysconfig/network
```

1. Install services

```
cp /etc/yum.repos.d/*
cp /etc/pki/rpm-gpg/*
curl -o /etc/yum.repos.d/dperson-neovim-epel-7.repo
https://copr.fedorainfracloud.org/coprs/dperson/neovim/repo/epel-7/dp
erson-neovim-epel-7.repo

yum -y install nss-pam-ldapd
yum -y install iptables-services
yum -y install sudo authconfig ypbind autofs chkconfig nfs-utils
rpcbind dkms lcm yum-autoupdate epel-release
yum -y install dkms-openafs openafs openafs-client openafs-docs
openafs-krb5
yum repolist
```

2. Add /data and /project

```
mkdir /project
mkdir /data
chmod a+rwx /data

ln -s /bin/bash /usr/local/bin/bash
ln -s /usr/bin/bash /usr/local/bin/bash
ln -s /usr/share/purple/ca-certs/Thawte_Premium_Server_CA.pem
/etc/openldap/cacerts/.
```

All users should create their own directory in /data (e.g. mkdir /data/norbert) to store local data (no backup).

3. Copy /etc/ssl/certs/InCommonSHA2.pem (from config.tar)
4. Edit /etc/sysconfig/network

```
NETWORKING=yes
HOSTNAME=xxxx.physics.purdue.edu
NISDOMAIN=purdue-pcn
```

5. Edit /etc/hosts

```
127.0.0.1    localhost localhost.localdomain localhost4
xxx.physics.purdue.edu
::1             localhost localhost.localdomain localhost6
localhost6.localdomain6

128.210.67.227  aristotle.physics.purdue.edu aristotle
128.210.67.223  volta.physics.purdue.edu volta
128.210.67.83   fibonacci.physics.purdue.edu fibonacci
```

6. Edit /etc/group

```
zh:x:1399:
phys:x:1109:
wheel:x:10:nneumeis,cjorr
```

7. Install CUPS printers: Add the following line to the file /etc/cups/client.conf

```
ServerName spool.physics.purdue.edu
```

8. Run:

```
authconfig --enablekrb5 --enableldap --enableldapauth --enablenis
--updateall
```

9. Firewall: Edit /etc/sysconfig/iptables

```
```

```
*filter

# Create a new chain that will accept tcp and udp.
-N ACCEPT_TCP_UDP
-A ACCEPT_TCP_UDP -p tcp -j ACCEPT
-A ACCEPT_TCP_UDP -p udp -j ACCEPT

# Allows all loopback (lo0) traffic and drop all traffic to 127/8 that
doesn't use lo0
-A INPUT -i lo -j ACCEPT
-A INPUT ! -i lo -d 127.0.0.0/8 -j REJECT

# Accepts all established inbound connections
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allows all outbound traffic
# You could modify this to only allow certain traffic
-A OUTPUT -j ACCEPT

# We trust the locals.
-A INPUT -m state --state NEW -s 10.164.17.128/25 -j ACCEPT_TCP_UDP
-A INPUT -m state --state NEW -s 10.164.18.0/24 -j ACCEPT_TCP_UDP
-A INPUT -m state --state NEW -s 10.164.19.0/25 -j ACCEPT_TCP_UDP
-A INPUT -m state --state NEW -s 10.164.26.128/25 -j ACCEPT_TCP_UDP
-A INPUT -m state --state NEW -s 10.164.81.128/25 -j ACCEPT_TCP_UDP
-A INPUT -m state --state NEW -s 10.164.82.0/24 -j ACCEPT_TCP_UDP
-A INPUT -m state --state NEW -s 10.164.83.0/25 -j ACCEPT_TCP_UDP
-A INPUT -m state --state NEW -s 128.210.146.0/24 -j ACCEPT_TCP_UDP
-A INPUT -m state --state NEW -s 128.210.67.0/24 -j ACCEPT_TCP_UDP
-A INPUT -m state --state NEW -s 128.210.68.0/24 -j ACCEPT_TCP_UDP
-A INPUT -m state --state NEW -s 128.210.69.0/24 -j ACCEPT_TCP_UDP

# Due to the way fortress.rcac's hsi/htar client works, we must
# do this. Reference:
https://www.rcac.purdue.edu/storage/fortress/faq/
# Best guess: The documentation is being generic and it's not
completely true.
# If someone compromises fortress, it would be a bad day. 9/17/2015
cjorr
-A INPUT -m state --state NEW -m iprange --src-range
128.210.251.141-128.210.251.148 -j ACCEPT_TCP_UDP

# Permit ssh from *
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

# ICMP is good. Probably. Some disagree.
-A INPUT -p icmp -j ACCEPT

# log iptables denied calls (access via 'dmesg' command)
-A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables denied:
" --log-level 7

# Reject all other inbound - default deny unless explicitly allowed
```

```
policy:
-A INPUT -j REJECT
```

```
-A FORWARD -j REJECT

COMMIT
```

10. Edit /usr/vice/etc/ThisCell

```
cern.ch
```

11. Edit /etc/krb5.conf

```
[libdefaults]
 default_realm = CERN.CH
 ticket_lifetime = 25h
 renew_lifetime = 120h
 forwardable = true
 proxiable = true
 default_tkt_enctypes = arcfour-hmac-md5 aes256-cts aes128-cts
des3-cbc-sha1 des-cbc-md5 des-cbc-crc
 chpw_prompt = true
 allow_weak_crypto = true

[realms]
 CERN.CH = {
  default_domain = cern.ch
  kpasswd_server = cerndc.cern.ch
  admin_server = cerndc.cern.ch
  kdc = cerndc.cern.ch
  v4_name_convert = {
     host = {
         rcmd = host
     }
  }
 }

 FNAL.GOV = {
  default_domain = fnal.gov
  admin_server = krb-fnal-admin.fnal.gov
  kdc = krb-fnal-1.fnal.gov:88
  kdc = krb-fnal-2.fnal.gov:88
  kdc = krb-fnal-3.fnal.gov:88
 }

 CENTRAL.PURDUE.LCL = {
  kdc = 128.210.63.203
  kdc = 1061cendc01.central.purdue.lcl
  admin_server = 1061cendc01.central.purdue.lcl
  default_domain = 1061cendc01.central.purdue.lcl
 }

[domain_realm]
```

```
 .cern.ch = CERN.CH
 .fnal.gov = FNAL.GOV
 .central.purdue.lcl = CENTRAL.PURDUE.LCL
 central.purdue.lcl = CENTRAL.PURDUE.LCL
[appdefaults]

 pam = {
   external = true
   krb4_convert = false
   krb4_convert_524 = false
```

```
    krb4_use_as_req = false
    ticket_lifetime = 25h
  }
```

12. /etc/ssh/ssh_config

```
GSSAPIAuthentication yes
GSSAPIDelegateCredentials yes
GSSAPIKeyExchange no
GSSAPITrustDNS yes
PubkeyAuthentication no
PasswordAuthentication yes
```

13. Automount /project, /home, /cvmfs:
    /etc/auto.master:

```
#
/misc    /etc/auto.misc
/project /etc/auto.project
/home    /etc/auto.home
/cvmfs   /etc/auto.cvmfs
/net    -hosts
+auto.master
```

    /etc/auto.home:

```
* -fstype=nfs,rw,soft,intr,rsize=32768,wsize=32768,nolock
aristotle.physics.purdue.edu:/net/aristotle/home/&
```

    /etc/auto.project:

```
cmsphys
-fstype=nfs,rw,grpid,soft,intr,nosuid,nodev,rsize=16384,wsize=16384,t
imeo=8,retrans=4,proto=tcp kepler:/net/kepler/project0/cmsphys
*
-fstype=nfs,rw,grpid,soft,intr,nosuid,nodev,rsize=16384,wsize=16384,t
imeo=9,retrans=4,proto=tcp kepler:/net/kepler/project0/&
```

14. Edit /etc/nslcd.conf

```
# /etc/nslcd.conf
# nslcd configuration file. See nslcd.conf(5)
# for details.

# The user and group nslcd should run as.
uid nslcd
gid ldap

# The location at which the LDAP server(s) should be reachable.
uri ldaps://fibonacci.physics.purdue.edu

# The search base that will be used for all queries.
base dc=physics,dc=purdue,dc=edu

# The LDAP protocol version to use.
#ldap_version 3

# The DN to bind with for normal lookups.
binddn cn=unsupported,dc=physics,dc=purdue,dc=edu
bindpw 1WyLrtUhTBSWw

# The DN used for password modifications by root.
#rootpwmoddn cn=admin,dc=example,dc=com

# SSL options
#ssl off
tls_reqcert allow

# The search scope.
#scope sub

#ssl start_tls
#ssl on
#tls_cacertfile /etc/ssl/certs/Thawte_Premium_Server_CA.pem
tls_cacertfile /etc/ssl/certs/InCommonSHA2.pem
ssl start_tls
ssl on
```

15. Edit /etc/yp.conf

```
# /etc/yp.conf - ypbind configuration file
# Valid entries are
#
# domain NISDOMAIN server HOSTNAME
#       Use server HOSTNAME for the domain NISDOMAIN.
#
# domain NISDOMAIN broadcast
#       Use  broadcast  on  the local net for domain NISDOMAIN
#
# domain NISDOMAIN slp
#       Query local SLP server for ypserver supporting NISDOMAIN
#
# ypserver HOSTNAME
#       Use server HOSTNAME for the  local  domain.  The
#       IP-address of server must be listed in /etc/hosts.
#
# broadcast
#       If no server for the default domain is specified or
#       none of them is rechable, try a broadcast call to
#       find a server.
#
domain purdue-pcn broadcast
```

16. Edit /etc/nsswitch.conf

```
#       [NOTFOUND=return]       Stop searching if not found so far
#

# To use db, put the "db" in front of "files" for entries you want to
be
# looked up first in the databases

#
# Example:

#passwd:    db files nisplus nis
#shadow:    db files nisplus nis
#group:     db files nisplus nis

passwd:     files ldap
shadow:     files ldap
group:      files nis

#initgroups: files

#hosts:     db files nisplus nis dns
hosts:      files dns myhostname

# Example - obey only what nisplus tells us...

#services:   nisplus [NOTFOUND=return] files
#networks:   nisplus [NOTFOUND=return] files
#protocols:  nisplus [NOTFOUND=return] files
#rpc:        nisplus [NOTFOUND=return] files
#ethers:     nisplus [NOTFOUND=return] files
#netmasks:   nisplus [NOTFOUND=return] files

bootparams: nisplus [NOTFOUND=return] files

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files sss

netgroup:   files sss ldap

publickey:  nisplus

automount:  files sss ldap
aliases:    files nisplus
```

17. Edit /etc/pam_ldap.conf

```
# @(#)$Id: ldap.conf,v 1.38 2006/05/15 08:13:31 lukeh Exp $
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.
#
# The man page for this file is pam_ldap(5)
#
# PADL Software
# http://www.padl.com
#
# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
#host 127.0.0.1

# The distinguished name of the search base.
base dc=physics,dc=purdue,dc=edu

# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
#ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
#binddn cn=proxyuser,dc=example,dc=com

# The credentials to bind with.
# Optional: default is no credential.
#bindpw secret

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
#rootbinddn cn=manager,dc=example,dc=com

# The port.
# Optional: default is 389.
#port 389

# The search scope.
#scope sub
#scope one
#scope base
```

```
# Search timelimit
#timelimit 30

# Bind/connect timelimit
#bind_timelimit 30

# Reconnect policy: hard (default) will retry connecting to
# the software with exponential backoff, soft will fail
# immediately.
#bind_policy hard

# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
#idle_timelimit 3600

# Filter to AND with uid=%s
#pam_filter objectclass=account

# The user ID attribute (defaults to uid)
#pam_login_attribute uid

# Search the root DSE for the password policy (works
# with Netscape Directory Server)
#pam_lookup_policy yes

# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
#pam_check_host_attr yes

# Check the 'authorizedService' attribute for access
# control
# Default is no; if set to yes, and the user has no
# value for the authorizedService attribute, and
# pam_ldap is configured for account management
# (authorization) then the user will not be allowed
# to login.
#pam_check_service_attr yes

# Group to enforce membership of
#pam_groupdn cn=PAM,ou=Groups,dc=example,dc=com

# Group member attribute
#pam_member_attribute uniquemember

# Specify a minium or maximum UID number allowed
#pam_min_uid 0
#pam_max_uid 0
```

```
# Template login attribute, default template user
# (can be overriden by value of former attribute
# in user's entry)
#pam_login_attribute userPrincipalName
#pam_template_login_attribute uid
#pam_template_login nobody

# HEADS UP: the pam_crypt, pam_nds_passwd,
# and pam_ad_passwd options are no
# longer supported.
#
# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
#pam_password clear

# Hash password locally; required for University of
# Michigan LDAP server, and works with Netscape
# Directory Server if you're using the UNIX-Crypt
# hash mechanism and not using the NT Synchronization
# service.
#pam_password crypt

# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
#pam_password clear_remove_old
#pam_password nds

# RACF is an alias for the above. For use with
# IBM RACF
#pam_password racf

# Update Active Directory password, by
# creating Unicode password and updating
# unicodePwd attribute.
#pam_password ad

# Use the OpenLDAP password change
# extended operation to update the password.
#pam_password exop

# Redirect users to a URL or somesuch on password
# changes.
#pam_password_prohibit_message Please visit http://internal to change
your password.

# RFC2307bis naming contexts
# Syntax:
# nss_base_XXX          base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
```

```
# You can omit the suffix eg:
# nss_base_passwd       ou=People,
# to append the default base DN but this
# may incur a small performance impact.
#nss_base_passwd        ou=People,dc=example,dc=com?one
#nss_base_shadow        ou=People,dc=example,dc=com?one
#nss_base_group         ou=Group,dc=example,dc=com?one
#nss_base_hosts         ou=Hosts,dc=example,dc=com?one
#nss_base_services      ou=Services,dc=example,dc=com?one
#nss_base_networks      ou=Networks,dc=example,dc=com?one
#nss_base_bootparams    ou=Ethers,dc=example,dc=com?one
#nss_base_aliases       ou=Aliases,dc=example,dc=com?one
#nss_base_netgroup      ou=Netgroup,dc=example,dc=com?one

# attribute/objectclass mapping
# Syntax:
#nss_map_attribute      rfc2307attribute        mapped_attribute
#nss_map_objectclass    rfc2307objectclass      mapped_objectclass

# configure --enable-nds is no longer supported.
# NDS mappings
#nss_map_attribute uniqueMember member

# Services for UNIX 3.5 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount User
#nss_map_attribute uid msSFU30Name

#nss_map_attribute uniqueMember msSFU30PosixMember
#nss_map_attribute userPassword msSFU30Password
#nss_map_attribute homeDirectory msSFU30HomeDirectory
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_objectclass posixGroup Group
#pam_login_attribute msSFU30Name
#pam_filter objectclass=User
#pam_password ad

# configure --enable-mssfu-schema is no longer supported.

# Services for UNIX 2.0 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid msSFUName
#nss_map_attribute uniqueMember posixMember
#nss_map_attribute userPassword msSFUPassword
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup Group
#nss_map_attribute cn msSFUName
#pam_login_attribute msSFUName
#pam_filter objectclass=User
#pam_password ad
#tls_checkpeer yes
```

```
# RFC 2307 (AD) mappings
#nss_map_objectclass posixAccount user
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid sAMAccountName
#nss_map_attribute homeDirectory unixHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup group
#nss_map_attribute uniqueMember member
#pam_login_attribute sAMAccountName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# AuthPassword mappings
#nss_map_attribute userPassword authPassword

# AIX SecureWay mappings
#nss_map_objectclass posixAccount aixAccount
#nss_base_passwd ou=aixaccount,?one
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_base_group ou=aixgroup,?one
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
#pam_password clear

# Netscape SDK LDAPS
#ssl on

# Netscape SDK SSL options
#sslpath /etc/ssl/certs
# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
#ssl start_tls
#ssl on

# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is to use libldap's default behavior, which can be
configured in
# /etc/openldap/ldap.conf using the TLS_REQCERT setting.  The default
for
# OpenLDAP 2.0 and earlier is "no", for 2.1 and later is "yes".
#tls_checkpeer yes
# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
```

```
#tls_cacertfile /etc/ssl/ca.cert
#tls_cacertdir /etc/ssl/certs

# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool

# SSL cipher suite
# See man ciphers for syntax
#tls_ciphers TLSv1

# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key

# Disable SASL security layers. This is needed for AD.
#sasl_secprops maxssf=0

# Override the default Kerberos ticket cache location.
#krb5_ccname FILE:/etc/.ldapcache

# SASL mechanism for PAM authentication - use is experimental
# at present and does not support password policy control
#pam_sasl_mech DIGEST-MD5
#host fibonacci.physics.purdue.edu
uri ldaps://fibonacci.physics.purdue.edu
ssl start_tls
#ssl start_tls
ldap_version 3
tls_reqcert allow
tls_cacertfile /etc/ssl/certs/InCommonSHA2.pem
tls_cacertdir /etc/openldap/cacerts
# you may need to symlink Thawte_Premium_Server_CA.pem in
/etc/openldap/cacerts
rootbinddn cn=admin,dc=physics,dc=purdue,dc=edu

pam_password md5
```

```
binddn cn=unsupported,dc=physics,dc=purdue,dc=edu
bindpw 1WyLrtUhTBSWw
```

18. Edit /etc/openldap/ldap.conf

```
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE   dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-master.example.com:666

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

TLS_CACERTDIR /etc/openldap/cacerts

# Turning this off breaks GSSAPI used with krb5 when rdns = false
SASL_NOCANON    on
URI ldaps://fibonacci.physics.purdue.edu
BASE dc=physics,dc=purdue,dc=edu
```

19. Edit /etc/sssd/sssd.conf

```
[domain/default]

autofs_provider = ldap
cache_credentials = True
ldap_search_base = dc=physics,dc=purdue,dc=edu
id_provider = ldap
auth_provider = ldap
chpass_provider = ldap
ldap_uri = ldaps://fibonacci.physics.purdue.edu
ldap_id_use_start_tls = True
ldap_tls_cacertdir = /etc/openldap/cacerts
krb5_realm = CERN.CH
krb5_server = cerndc.cern.ch

[sssd]
services = nss, pam, autofs
config_file_version = 2
domains = default

[nss]
homedir_substring = /home

[pam]

[sudo]

[autofs]

[ssh]

[pac]

[ifp]
```

20. Edit /etc/sudoers

```
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.

## Host Aliases
## Groups of machines. You may prefer to use hostnames (perhaps using
## wildcards for entire domains) or IP addresses instead.
# Host_Alias     FILESERVERS = fs1, fs2
```

```
# Host_Alias     MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias ADMINS = jsmith, mikem

## Command Aliases
## These are groups of related commands...

## Networking
# Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping,
/sbin/dhclient, /usr/bin/net, /sbin/iptables, /usr/bin/rfcomm,
/usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool

## Installation and management of software
# Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum

## Services
# Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig,
/usr/bin/systemctl start, /usr/bin/systemctl stop, /usr/bin/systemctl
reload, /usr/bin/systemctl restart, /usr/bin/systemctl status,
/usr/bin/systemctl enable, /usr/bin/systemctl disable

## Updating the locate database
# Cmnd_Alias LOCATE = /usr/bin/updatedb

## Storage
# Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted,
/sbin/partprobe, /bin/mount, /bin/umount

## Delegating permissions
# Cmnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod,
/bin/chgrp

## Processes
# Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill,
/usr/bin/killall

## Drivers
# Cmnd_Alias DRIVERS = /sbin/modprobe

# Defaults specification

#
# Disable "ssh hostname sudo <cmd>", because it will show the password
in clear.
#         You have to run "ssh -t hostname sudo <cmd>".
#
Defaults    requiretty

#
```

```
# Refuse to run if unable to disable echo on the tty. This setting
should also be
# changed in order to be able to use sudo without a tty. See
requiretty above.
#
Defaults   !visiblepw

#
# Preserving HOME has security implications since many programs
# use it when searching for configuration files. Note that HOME
# is already set when the the env_reset option is enabled, so
# this option is only effective for configurations where either
# env_reset is disabled or HOME is present in the env_keep list.
#
Defaults    always_set_home

Defaults    env_reset
Defaults    env_keep =  "COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC
KDEDIR LS_COLORS"
Defaults    env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS
LC_CTYPE"
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT
LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER
LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
XAUTHORITY"

#
# Adding HOME to env_keep may enable a user to run unrestricted
# commands via sudo.
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:

##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING,
PROCESSES, LOCATE, DRIVERS
```

```
## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the

## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now
```

```
## Read drop-in files from /etc/sudoers.d (the # here does not mean a
comment)
#includedir /etc/sudoers.d
```

21. Turn on services

```
systemctl stop firewalld
systemctl disable firewalld
systemctl start iptables
systemctl enable iptables
systemctl enable autofs
systemctl start autofs
systemctl enable nslcd
systemctl start nslcd
systemctl enable rpcbind
systemctl start rpcbind
systemctl enable ypbind
systemctl start ypbind
systemctl enable openafs-client
systemctl start openafs-client
```

Scientific Linux CERN 6 (SLC6) Installation

System Installation

Follow the instructions on http://linux.web.cern.ch/linux/scientific6/docs/install.shtml

1. Create a boot image for a 64 bit system
2. Reboot your computer and press F2 (F12) at startup
3. In the BIOS setup add CD/DVD to boot devices; save BIOS setup and reboot
4. Select **http** as installation method
5. Installation server is: linuxsoft.cern.ch
6. Installation path is: /cern/slc6X/x86_64/
7. Keep default partition layout
8. Set host name to **xxx**.physics.purdue.edu: e.g. serret.physics.purdue.edu
9. Enable network time protocol (server: harbor.ecn.purdue.edu)
10. Set Time Zone to: America/Indianapolis

Customize System

1. Create /data

```
mkdir /data
chmod a+rwx /data
```

   All users should create their own directory in /data (e.g. mkdir /data/norbert) to store local data (no backup).
2. /etc/sysconfig/network

```
NETWORKING=yes
HOSTNAME=xxxx.physics.purdue.edu
NISDOMAIN=purdue-pcn
```

3. /etc/hosts

```
127.0.0.1               localhost.localdomain localhost
xxx.physics.purdue.edu

128.210.67.227    aristotle.physics.purdue.edu aristotle
128.210.67.223    volta.physics.purdue.edu volta
```

4. /etc/group

```
zh:x:1399:
phys:x:1109:
```

5. Install CUPS printers: Add the following line to the file /etc/cups/client.conf

```
ServerName spool.physics.purdue.edu
```

6. Install ldap

```
yum install openldap-clients
yum install nss-pam-ldapd
```

7. Edit /etc/pam_ldap.conf

```
# @(#)$Id: ldap.conf,v 1.38 2006/05/15 08:13:31 lukeh Exp $
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.
#
# The man page for this file is pam_ldap(5)
#
# PADL Software
# http://www.padl.com
#
# Your LDAP server. Must be resolvable without using LDAP.
# Multiple hosts may be specified, each separated by a
# space. How long nss_ldap takes to failover depends on
# whether your LDAP client library supports configurable
# network or connect timeouts (see bind_timelimit).
#host 127.0.0.1
# The distinguished name of the search base.
base dc=physics,dc=purdue,dc=edu
```

```
# Another way to specify your LDAP server is to provide an
# uri with the server name. This allows to use
# Unix Domain Sockets to connect to a local LDAP Server.
#uri ldap://127.0.0.1/
#uri ldaps://127.0.0.1/
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator
# The LDAP version to use (defaults to 3
# if supported by client library)
#ldap_version 3
# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
#binddn cn=proxyuser,dc=example,dc=com
# The credentials to bind with.
# Optional: default is no credential.
#bindpw secret
# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
#rootbinddn cn=manager,dc=example,dc=com
# The port.
# Optional: default is 389.
#port 389
# The search scope.
#scope sub
#scope one
#scope base
# Search timelimit
#timelimit 30
# Bind/connect timelimit
#bind_timelimit 30
# Reconnect policy: hard (default) will retry connecting to
# the software with exponential backoff, soft will fail
# immediately.
#bind_policy hard
# Idle timelimit; client will close connections
# (nss_ldap only) if the server has not been contacted
# for the number of seconds specified below.
#idle_timelimit 3600
# Filter to AND with uid=%s
#pam_filter objectclass=account
# The user ID attribute (defaults to uid)
#pam_login_attribute uid
# Search the root DSE for the password policy (works
# with Netscape Directory Server)
#pam_lookup_policy yes
# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
#pam_check_host_attr yes
# Check the 'authorizedService' attribute for access
```

```
# control
# Default is no; if set to yes, and the user has no
# value for the authorizedService attribute, and
# pam_ldap is configured for account management
# (authorization) then the user will not be allowed
# to login.
#pam_check_service_attr yes
# Group to enforce membership of
#pam_groupdn cn=PAM,ou=Groups,dc=example,dc=com
# Group member attribute
#pam_member_attribute uniquemember
# Specify a minium or maximum UID number allowed
#pam_min_uid 0
#pam_max_uid 0
# Template login attribute, default template user
# (can be overriden by value of former attribute
# in user's entry)
#pam_login_attribute userPrincipalName
#pam_template_login_attribute uid
#pam_template_login nobody
# HEADS UP: the pam_crypt, pam_nds_passwd,
# and pam_ad_passwd options are no
# longer supported.
#
# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
#pam_password clear
# Hash password locally; required for University of
# Michigan LDAP server, and works with Netscape
# Directory Server if you're using the UNIX-Crypt
# hash mechanism and not using the NT Synchronization
# service.
#pam_password crypt
# Remove old password first, then update in
# cleartext. Necessary for use with Novell
# Directory Services (NDS)
#pam_password clear_remove_old
#pam_password nds
# RACF is an alias for the above. For use with
# IBM RACF
#pam_password racf
# Update Active Directory password, by
# creating Unicode password and updating
# unicodePwd attribute.
#pam_password ad
# Use the OpenLDAP password change
# extended operation to update the password.
#pam_password exop
# Redirect users to a URL or somesuch on password
# changes.
#pam_password_prohibit_message Please visit http://internal to change
your password.
```

```
# RFC2307bis naming contexts
# Syntax:
# nss_base_XXX  base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
# You can omit the suffix eg:
# nss_base_passwd ou=People,
# to append the default base DN but this
# may incur a small performance impact.
#nss_base_passwd ou=People,dc=example,dc=com?one
#nss_base_shadow ou=People,dc=example,dc=com?one
#nss_base_group  ou=Group,dc=example,dc=com?one
#nss_base_hosts  ou=Hosts,dc=example,dc=com?one
#nss_base_services ou=Services,dc=example,dc=com?one
#nss_base_networks ou=Networks,dc=example,dc=com?one
#nss_base_protocols ou=Protocols,dc=example,dc=com?one
#nss_base_rpc  ou=Rpc,dc=example,dc=com?one
#nss_base_ethers ou=Ethers,dc=example,dc=com?one
#nss_base_netmasks ou=Networks,dc=example,dc=com?ne
#nss_base_bootparams ou=Ethers,dc=example,dc=com?one
#nss_base_aliases ou=Aliases,dc=example,dc=com?one
#nss_base_netgroup ou=Netgroup,dc=example,dc=com?one
# attribute/objectclass mapping
# Syntax:
#nss_map_attribute rfc2307attribute mapped_attribute
#nss_map_objectclass rfc2307objectclass mapped_objectclass
# configure --enable-nds is no longer supported.
# NDS mappings
#nss_map_attribute uniqueMember member
# Services for UNIX 3.5 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount User
#nss_map_attribute uid msSFU30Name
#nss_map_attribute uniqueMember msSFU30PosixMember
#nss_map_attribute userPassword msSFU30Password
#nss_map_attribute homeDirectory msSFU30HomeDirectory
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_objectclass posixGroup Group
#pam_login_attribute msSFU30Name
#pam_filter objectclass=User
#pam_password ad
# configure --enable-mssfu-schema is no longer supported.
# Services for UNIX 2.0 mappings
#nss_map_objectclass posixAccount User
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid msSFUName
#nss_map_attribute uniqueMember posixMember
#nss_map_attribute userPassword msSFUPassword
#nss_map_attribute homeDirectory msSFUHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup Group
#nss_map_attribute cn msSFUName
```

```
#pam_login_attribute msSFUName
#pam_filter objectclass=User
#pam_password ad
# RFC 2307 (AD) mappings
#nss_map_objectclass posixAccount user
#nss_map_objectclass shadowAccount user
#nss_map_attribute uid sAMAccountName
#nss_map_attribute homeDirectory unixHomeDirectory
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup group
#nss_map_attribute uniqueMember member
#pam_login_attribute sAMAccountName
#pam_filter objectclass=User
#pam_password ad
# configure --enable-authpassword is no longer supported
# AuthPassword mappings
#nss_map_attribute userPassword authPassword
# AIX SecureWay mappings
#nss_map_objectclass posixAccount aixAccount
#nss_base_passwd ou=aixaccount,?one
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_base_group ou=aixgroup,?one
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
#pam_password clear
# Netscape SDK LDAPS
#ssl on
# Netscape SDK SSL options
#sslpath /etc/ssl/certs
# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
#ssl start_tls
#ssl on
# OpenLDAP SSL options
# Require and verify server certificate (yes/no)
# Default is to use libldap's default behavior, which can be
configured in
# /etc/openldap/ldap.conf using the TLS_REQCERT setting.  The default
for
# OpenLDAP 2.0 and earlier is "no", for 2.1 and later is "yes".
#tls_checkpeer yes
# CA certificates for server certificate verification
# At least one of these are required if tls_checkpeer is "yes"
#tls_cacertfile /etc/ssl/ca.cert
#tls_cacertdir /etc/ssl/certs
# Seed the PRNG if /dev/urandom is not provided
#tls_randfile /var/run/egd-pool
```

```
# SSL cipher suite
# See man ciphers for syntax
#tls_ciphers TLSv1
# Client certificate and key
# Use these, if your server requires client authentication.
#tls_cert
#tls_key
# Disable SASL security layers. This is needed for AD.
#sasl_secprops maxssf=0
# Override the default Kerberos ticket cache location.
#krb5_ccname FILE:/etc/.ldapcache
# SASL mechanism for PAM authentication - use is experimental
# at present and does not support password policy control
#pam_sasl_mech DIGEST-MD5
#host fibonacci.physics.purdue.edu
base dc=physics,dc=purdue,dc=edu
uri ldaps://fibonacci.physics.purdue.edu
ssl on
#ssl start_tls
ldap_version 3
tls_reqcert allow
tls_cacertfile /etc/ssl/certs/InCommonSHA2.pem
tls_cacertdir /etc/ssl/certs
# you may need to symlink Thawte_Premium_Server_CA.pem in
/etc/openldap/cacerts
rootbinddn cn=admin,dc=physics,dc=purdue,dc=edu
pam_password md5
```

```
binddn cn=unsupported,dc=physics,dc=purdue,dc=edu
bindpw *********
```

8. Edit /etc/nslcd.conf

```
# /etc/nslcd.conf
# nslcd configuration file. See nslcd.conf(5)
# for details.
# The user and group nslcd should run as.
uid nslcd
gid ldap
# The location at which the LDAP server(s) should be reachable.
uri ldaps://fibonacci.physics.purdue.edu
# The search base that will be used for all queries.
base dc=physics,dc=purdue,dc=edu
# The LDAP protocol version to use.
#ldap_version 3
# The DN to bind with for normal lookups.
binddn cn=unsupported,dc=physics,dc=purdue,dc=edu
bindpw 1WyLrtUhTBSWw
# The DN used for password modifications by root.
#rootpwmoddn cn=admin,dc=example,dc=com
# SSL options
#ssl off
tls_reqcert allow
# The search scope.
#scope sub
#ssl start_tls
#ssl on
#tls_cacertfile /etc/ssl/certs/Thawte_Premium_Server_CA.pem
tls_cacertfile /etc/ssl/certs/InCommonSHA2.pem
ssl start_tls
ssl on
```

9. ln -s /usr/share/purple/ca-certs/Thawte_Premium_Server_CA.pem /etc/openldap/cacerts/.
10. /etc/yp.conf

```
domain purdue-pcn broadcast
```

11. /etc/sysconfig/authconfig

```
USEMD5=no
USECRACKLIB=yes
USEDB=no
USEHESIOD=no
USELDAP=yes
USENIS=yes
USEPASSWDQC=no
USEWINBIND=no
USEKERBEROS=yes
USELDAPAUTH=yes
USESHADOW=yes
USESMBAUTH=no
USEWINBINDAUTH=no
USELOCAUTHORIZE=yes
PASSWDALGORITHM=md5
```

12. Edit /etc/nsswitch.conf

```
passwd:     files ldap nis
shadow:     files ldap
group:      files nis

hosts:      files nis dns

bootparams: nisplus [NOTFOUND=return] files

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files

netgroup:   files nis ldap

publickey:  nisplus

automount:  files nis ldap
aliases:    files nisplus
```

13. run

```
authconfig --enablekrb5 --enableldap --enableldapauth --enablenis
--updateall
```

14. ln -s /bin/bash /usr/local/bin/bash
15. Automount /project, /home, /cvmfs:
    /etc/auto.master:

```
#
/misc    /etc/auto.misc
/project /etc/auto.project
/home    /etc/auto.home
/cvmfs   /etc/auto.cvmfs
/net    -hosts
+auto.master
```

/etc/auto.home:

```
* -fstype=nfs,rw,soft,intr,rsize=32768,wsize=32768,nolock
aristotle.physics.purdue.edu:/net/aristotle/home/&
```

/etc/auto.project:

```
cmsphys
-fstype=nfs,rw,grpid,soft,intr,nosuid,nodev,rsize=16384,wsize=16384,t
imeo=8,retrans=4,proto=tcp kepler:/net/kepler/project0/cmsphys
*
-fstype=nfs,rw,grpid,soft,intr,nosuid,nodev,rsize=16384,wsize=16384,t
imeo=9,retrans=4,proto=tcp kepler:/net/kepler/project0/&
```

16. /etc/krb5.conf

```
[libdefaults]
 default_realm = CERN.CH
 ticket_lifetime = 25h
 renew_lifetime = 120h
 forwardable = true
 proxiable = true
 default_tkt_enctypes = arcfour-hmac-md5 aes256-cts aes128-cts
des3-cbc-sha1 des-cbc-md5 des-cbc-crc
 chpw_prompt = true
 allow_weak_crypto = true

[realms]
 CERN.CH = {
  default_domain = cern.ch
  kpasswd_server = cerndc.cern.ch
  admin_server = cerndc.cern.ch
  kdc = cerndc.cern.ch
  v4_name_convert = {
     host = {
         rcmd = host
     }
  }
 }

 FNAL.GOV = {
```

```
  default_domain = fnal.gov
  admin_server = krb-fnal-admin.fnal.gov
  kdc = krb-fnal-1.fnal.gov:88
  kdc = krb-fnal-2.fnal.gov:88
  kdc = krb-fnal-3.fnal.gov:88
 }

 CENTRAL.PURDUE.LCL = {
  kdc = 128.210.63.203
  kdc = 1061cendc01.central.purdue.lcl
  admin_server = 1061cendc01.central.purdue.lcl
  default_domain = 1061cendc01.central.purdue.lcl
 }

[domain_realm]
 .cern.ch = CERN.CH
 .fnal.gov = FNAL.GOV
 .central.purdue.lcl = CENTRAL.PURDUE.LCL
 central.purdue.lcl = CENTRAL.PURDUE.LCL

[appdefaults]
 pam = {
   external = true
   krb4_convert = false
   krb4_convert_524 = false
   krb4_use_as_req = false
```

```
    ticket_lifetime = 25h
  }
```

1. /etc/ssh/ssh_config

```
GSSAPIAuthentication yes
GSSAPIDelegateCredentials yes
GSSAPIKeyExchange no
GSSAPITrustDNS yes
PubkeyAuthentication no
PasswordAuthentication yes
```

2. /etc/passwd (This will allow you to login with your CERN afs account and mounts your CERN afs home directory)

```
neumeist:x:11701:1399:Norbert
NEUMEISTER:/afs/cern.ch/user/n/neumeist:/bin/tcsh
hdyoo:x:34127:1399:Hwidong YOO:/afs/cern.ch/user/h/hdyoo:/bin/tcsh
asvyatko:x:24584:1399:Alexey
SVYATKOVKIY:/afs/cern.ch/user/a/asvyatko:/bin/tcsh
```

3. Edit /etc/pam.d/system-auth

```
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        sufficient    pam_krb5.so use_first_pass
auth        sufficient    pam_ldap.so use_first_pass
auth        required      pam_deny.so

account     sufficient    pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     [default=bad success=ok user_unknown=ignore] pam_krb5.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3
password    sufficient    pam_unix.so md5 shadow nis nullok
try_first_pass use_authtok
password    sufficient    pam_krb5.so use_authtok
password    sufficient    pam_ldap.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in
crond quiet use_uid
session     required      pam_unix.so
session     required      pam_krb5.so
session     optional      pam_ldap.so
```

4. turn on ypbind, turn off sssd, turn on AFS

```
/sbin/chkconfig --add afs
 /sbin/chkconfig --del iptables
 /sbin/chkconfig --del sssd
 /sbin/chkconfig --add ypbind
 /sbin/chkconfig autofs on
 /sbin/chkconfig iptables off
 /sbin/chkconfig ypbind on
 /sbin/chkconfig sssd off
 service sssd stop
 service iptables stop
 service autofs start
 service ypbind start
```

5. Firewall: Switch off iptables
6. Java: Download and install Java SE Runtime Environment JRE 6 (select Linux_64)
7. /etc/mime.types

```
type=application/x-java-jnlp-file desc="Java Web Start" exts="jnlp
```

8. In addition you want to install: flash-plugin.x86_64, mplayer.x86_64, mplayer-gui.x86_64, gnome-mplayer.x86_64, kmplayer.x86_64, mplayer-codecs-addon.i386, mplayer-doc.x86_64, jre.x86_64
9. switch off nscd: /etc/init.d/nscd stop
10. In case automount doesn't work:

```
mount -t nfs aristotle:/net/aristotle/home /home -o
rw,bg,intr,nosuid,udp,rsize=8192,wsize=8192,timeo=8
```

Scientific Linux CERN 5 (SLC5) Installation

System Installation

Follow the instructions on http://linux.web.cern.ch/linux/scientific5/docs/install.shtml

1. Create a boot image for a 64 bit system
2. Reboot your computer and press F2 (F12) at startup
3. In the BIOS setup add CD/DVD to boot devices; save BIOS setup and reboot
4. Select **http** as installation method
5. Installation server is: linuxsoft.cern.ch
6. Installation path is: /cern/slc5X/x86_64/
7. Keep default partition layout
8. Set host name to **xxx**.physics.purdue.edu: e.g. serret.physics.purdue.edu
9. Enable network time protocol (server: harbor.ecn.purdue.edu)
10. Set Time Zone to: America/Indianapolis

Customize System

Follow these instructions to mount PCN home directories with pam-cifs.
Do not forget:

```
ln -s /lib/security/pam_cifs.so /lib64/security/pam_cifs.so
```

1. Create /data

```
mkdir /data
chmod a+rwx /data
```

   All users should create their own directory in /data (e.g. mkdir /data/norbert) to store local data (no backup).
2. /etc/sysconfig/network

```
NETWORKING=yes
HOSTNAME=xxxx.physics.purdue.edu
NISDOMAIN=purdue-pcn
```

3. /etc/hosts

```
127.0.0.1               localhost.localdomain localhost
xxx.physics.purdue.edu
```

4. /etc/group

```
zh:x:1399:
phys:x:1109:
```

5. Install CUPS printers: Add the following line to the file /etc/cups/client.conf

```
ServerName spool.physics.purdue.edu
```

6. Install the amd automounter and make sure autofs is switched off

```
yum install am-utils
```

7. /etc/amd.conf

```
# GLOBAL OPTIONS SECTION
[ global ]
normalize_hostnames =   no
print_pid =             yes
pid_file =              /var/run/amd.pid
restart_mounts =        yes
auto_dir =              /net
#log_file =             /var/log/amd
log_file =              syslog
log_options =           all
#debug_options =        all
plock =                 no
selectors_on_default =  yes
print_version =         no
#map_type =             file
search_path =           /etc
browsable_dirs =        yes
show_statfs_entries =   no
fully_qualified_hosts = no
cache_duration =        300

# DEFINE AN AMD MOUNT POINT
[/home]
map_name = amd.home

[/project]
map_name = amd.project
```

8. /etc/amd.home

```
#comment: amd.home map
/defaults       fs:=/net/${rhost}/home;\

opts:=rw,bg,grpid,intr,nosuid,nodev,quota,proto=udp,vers=3,\
                rsize=8192,wsize=8192,timeo=8,retrans=4;\
                rfs:=/net/${rhost}/home;\
                sublink:=${key};\
                type:=nfsl

#-- All other accounts

# Everbody else falls back to a * entry
*               rhost:=aristotle
```

/etc/amd.project

```
#comment: amd.project map
/defaults       fs:=/net/${rhost.}/project;\
                opts:=rw,bg,grpid,intr,nosuid,nodev,proto=tcp,vers=3,\
                rsize=16384,wsize=16384,timeo=8,retrans=4;\
                rfs:=/net/${rhost.}/project;\
                sublink:="${key}";\
                type:=nfsl

cmsphys         rhost:=kepler;rfs:=/net/${rhost.}/project0;fs:=${rfs}
```

9. /etc/krb5.conf

```
[libdefaults]
 default_realm = CERN.CH
 ticket_lifetime = 25h
 renew_lifetime = 120h
 forwardable = true
 proxiable = true
 default_tkt_enctypes = arcfour-hmac-md5 aes256-cts aes128-cts
des3-cbc-sha1 des-cbc-md5 des-cbc-crc

[realms]
 CERN.CH = {
  default_domain = cern.ch
  kpasswd_server = afskrb5m.cern.ch
  admin_server = afskrb5m.cern.ch
  kdc = cerndc.cern.ch

  v4_name_convert = {
     host = {
         rcmd = host
     }
  }
 }
```

```
 FNAL.GOV = {
  default_domain = fnal.gov
  admin_server = krb-fnal-admin.fnal.gov
  kdc = krb-fnal-1.fnal.gov:88
  kdc = krb-fnal-2.fnal.gov:88
  kdc = krb-fnal-3.fnal.gov:88
 }

 CENTRAL.PURDUE.LCL = {
  kdc = 128.210.63.203
  kdc = 1061cendc01.central.purdue.lcl
  admin_server = 1061cendc01.central.purdue.lcl
  default_domain = 1061cendc01.central.purdue.lcl
 }

[domain_realm]
 .cern.ch = CERN.CH
 .fnal.gov = FNAL.GOV
 .central.purdue.lcl = CENTRAL.PURDUE.LCL
 central.purdue.lcl = CENTRAL.PURDUE.LCL

[appdefaults]
 pam = {
   external = true
   krb4_convert = false
   krb4_convert_524 = false
   krb4_use_as_req = false
   ticket_lifetime = 25h
```

```
}
```

10. /etc/yp.conf

```
domain purdue-pcn broadcast
```

11. /etc/ldap.conf

```
host volta.physics.purdue.edu
base dc=physics,dc=purdue,dc=edu
uri ldaps://volta.physics.purdue.edu
ssl start_tls
ssl on
ldap_version 3
tls_checkpeer yes
tls_cacertfile /usr/share/purple/ca-certs/Thawte_Premium_Server_CA.pem
tls_cacertdir /etc/openldap/cacerts
# you may need to symlink Thawte_Premium_Server_CA.pem in
/etc/openldap/cacerts
rootbinddn cn=admin,dc=physics,dc=purdue,dc=edu

pam_password md5

binddn cn=unsupported,dc=physics,dc=purdue,dc=edu
bindpw *********
```

12. chmod 0600 /etc/ldap.conf (Note: Because of a bug it needs to be chmod 0644 /etc/ldap.conf)
13. ln -s /bin/bash /usr/local/bin/bash
14. ln -s /usr/share/purple/ca-certs/Thawte_Premium_Server_CA.pem /etc/openldap/cacerts/.
15. /etc/nsswitch.conf

```
passwd:     files ldap nis
shadow:     files ldap
group:      files nis

hosts:      files nis dns

bootparams: nisplus [NOTFOUND=return] files

ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files

netgroup:   files nis ldap

publickey:  nisplus

automount:  files nis ldap
aliases:    files nisplus
```

16. /etc/sysconfig/authconfig

```
USEMD5=no
USECRACKLIB=yes
USEDB=no
USEHESIOD=no
USELDAP=yes
USENIS=yes
USEPASSWDQC=no
USEWINBIND=no
USEKERBEROS=yes
USELDAPAUTH=yes
USESHADOW=yes
USESMBAUTH=no
USEWINBINDAUTH=no
USELOCAUTHORIZE=yes
PASSWDALGORITHM=md5
```

17. /etc/ssh/ssh_config

```
GSSAPIAuthentication yes
GSSAPIDelegateCredentials yes
GSSAPIKeyExchange no
GSSAPITrustDNS yes
PubkeyAuthentication no
PasswordAuthentication yes
```

18. AFS

```
/sbin/chkconfig --add afs
 /sbin/chkconfig --add amd
 /sbin/chkconfig --del autofs
 /sbin/chkconfig --del iptables
 /sbin/chkconfig autofs off
 /sbin/chkconfig iptables off
 /sbin/chkconfig amd on
 /sbin/service autofs stop
 /sbin/service iptables stop
 /sbin/service amd start
```

19. /etc/passwd (This will allow you to login with your CERN afs account and mounts your CERN afs home directory)

```
neumeist:x:11701:1399:Norbert
NEUMEISTER:/afs/cern.ch/user/n/neumeist:/bin/tcsh
aeverett:x:8547:1399:Adam
EVERETT:/afs/cern.ch/user/a/aeverett:/bin/tcsh
hdyoo:x:34127:1399:Hwidong YOO:/afs/cern.ch/user/h/hdyoo:/bin/tcsh
asvyatko:x:24584:1399:Alexey
SVYATKOVKIY:/afs/cern.ch/user/a/asvyatko:/bin/tcsh
```

20. /etc/pam.d/system-auth (for pam_cifs mounted homedirs)

```
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        required      pam_cifs.so debug
auth        sufficient    pam_krb5.so use_first_pass
auth        sufficient    pam_ldap.so use_first_pass debug
auth        required      pam_deny.so

account     sufficient    pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_krb5.so
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
debug
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3
password    sufficient    pam_unix.so md5 shadow nis nullok
try_first_pass use_authtok
password    sufficient    pam_krb5.so use_authtok
password    sufficient    pam_ldap.so use_authtok debug
password    required      pam_deny.so

session    optional     pam_keyinit.so revoke
session    required     pam_limits.so
session    [success=1   default=ignore] pam_succeed_if.so service in
crond quiet use_uid
session    required     pam_mkhomedir.so umask=077 skel=/etc/skel
session    required     pam_unix.so
session    required     pam_krb5.so
session    optional     pam_cifs.so debug background=0 prefix=/home
mount_home=1 source=//gutenberg.physics.purdue.edu windomain=ONEPURDUE
```

21. /etc/pam.d/system-auth (for amd mounted homedirs)

```
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        sufficient    pam_krb5.so use_first_pass
auth        sufficient    pam_ldap.so use_first_pass
auth        required      pam_deny.so

account     sufficient    pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_ldap.so
account     [default=bad success=ok user_unknown=ignore] pam_krb5.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3
password    sufficient    pam_unix.so md5 shadow nis nullok
try_first_pass use_authtok
password    sufficient    pam_krb5.so use_authtok
password    sufficient    pam_ldap.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in
crond quiet use_uid
session     required      pam_unix.so
session     required      pam_krb5.so
session     optional      pam_ldap.so
```

22. Firewall: Switch off iptables
23. Java: Download and install Java SE Runtime Environment JRE 6 (select Linux_64)
24. /etc/mime.types

```
type=application/x-java-jnlp-file desc="Java Web Start" exts="jnlp
```

25. In addition you want to install: flash-plugin.x86_64, mplayer.x86_64, mplayer-gui.x86_64, gnome-mplayer.x86_64, kmplayer.x86_64, mplayer-codecs-addon.i386, mplayer-doc.x86_64, jre.x86_64
26. switch off nscd: /etc/init.d/nscd stop

1. Install

```
rpm -U am-utils-6.1.5-14.fc12.x86_64.rpm
```