AD Server Name: adserver.cluster.com

Domain : CLUSTER.COM

**suse1:~ # cat /etc/krb5.conf**

[libdefaults]

default\_realm = CLUSTER.COM

dns\_lookup\_kdc = false

dns\_lookup\_realm = false

ticket\_lifetime = 86400

renew\_lifetime = 604800

forwardable = true

rdns = true

default\_tgs\_enctypes = rc4-hmac

default\_tkt\_enctypes = rc4-hmac

permitted\_enctypes = rc4-hmac

udp\_preference\_limit = 1

kdc\_timeout = 3000

default\_ccache\_name = FILE:/tmp/krb5cc\_%{uid}

clockskew = 300

[realms]

CLUSTER.COM = {

kdc = adserver.cluster.com

admin\_server = adserver.cluster.com

master\_kdc = adserver.cluster.com

default\_domain = cluster.com

}

[domain\_realm]

.cluster.com = CLUSTER.COM

cluster.com = CLUSTER.COM

[logging]

kdc = FILE:/var/log/krb5/krb5kdc.log

admin\_server = FILE:/var/log/krb5/kadmind.log

default = SYSLOG:NOTICE:DAEMON

[appdefaults] --------------- **Entry automatically added after setup**

pam = {

ticket\_lifetime = 1d

renew\_lifetime = 1d

forwardable = true

proxiable = false

minimum\_uid = 1

}

suse1:~ #

**suse1:~ # cat /etc/samba/smb.conf**

# smb.conf is the main Samba configuration file. You find a full commented

# version at /usr/share/doc/packages/samba/examples/smb.conf.SUSE if the

# samba-doc package is installed.

[global]

workgroup = CLUSTER

passdb backend = tdbsam

printing = cups

printcap name = cups

printcap cache time = 750

cups options = raw

map to guest = Bad User

include = /etc/samba/dhcp.conf

logon path = \\%L\profiles\.msprofile

logon home = \\%L\%U\.9xprofile

logon drive = P:

usershare allow guests = No

idmap gid = 10000 – 20000

idmap uid = 10000 – 20000

realm = CLUSTER.COM

security = ADS

template homedir = /home/%D/%U

template shell = /bin/bash

winbind refresh tickets = yes

winbind use default domain = yes

kerberos method = secrets and keytab

client signing = yes

client use spnego = yes

usershare max shares = 100

winbind offline logon = yes

[homes]

comment = Home Directories

valid users = %S, %D%w%S

browseable = No

read only = No

inherit acls = Yes

[profiles]

comment = Network Profiles Service

path = %H

read only = No

store dos attributes = Yes

create mask = 0600

directory mask = 0700

[users]

comment = All users

path = /home

read only = No

inherit acls = Yes

veto files = /aquota.user/groups/shares/

[groups]

comment = All groups

path = /home/groups

read only = No

inherit acls = Yes

[printers]

comment = All Printers

path = /var/tmp

printable = Yes

create mask = 0600

browseable = No

[print$]

comment = Printer Drivers

path = /var/lib/samba/drivers

write list = @ntadmin root

force group = ntadmin

create mask = 0664

directory mask = 0775

suse1:~ #

suse1:~ # cat /etc/hosts

#

# hosts This file describes a number of hostname-to-address

# mappings for the TCP/IP subsystem. It is mostly

# used at boot time, when no name servers are running.

# On small systems, this file can be used instead of a

# "named" name server.

# Syntax:

#

# IP-Address Full-Qualified-Hostname Short-Hostname

#

127.0.0.1 localhost

# special IPv6 addresses

::1 localhost ipv6-localhost ipv6-loopback

fe00::0 ipv6-localnet

ff00::0 ipv6-mcastprefix

ff02::1 ipv6-allnodes

ff02::2 ipv6-allrouters

ff02::3 ipv6-allhosts

# Added by SMT registration do not remove, retain comment as well

35.185.34.152 smt-gce.susecloud.net smt-gce

10.142.0.5 suse1.cluster.com suse1

10.138.0.3 adserver.cluster.com adserver

suse1:~ # cat /etc/resolv.conf

### /etc/resolv.conf file autogenerated by netconfig!

#

# Before you change this file manually, consider to define the

# static DNS configuration using the following variables in the

# /etc/sysconfig/network/config file:

# NETCONFIG\_DNS\_STATIC\_SEARCHLIST

# NETCONFIG\_DNS\_STATIC\_SERVERS

# NETCONFIG\_DNS\_FORWARDER

# or disable DNS configuration updates via netconfig by setting:

# NETCONFIG\_DNS\_POLICY=''

#

# See also the netconfig(8) manual page and other documentation.

#

# Note: Manual change of this file disables netconfig too, but

# may get lost when this file contains comments or empty lines

# only, the netconfig settings are same with settings in this

# file and in case of a "netconfig update -f" call.

#

### Please remove (at least) this line when you modify the file!

search cluster.com

nameserver 10.138.0.3

nameserver 169.254.169.254

suse1:~ #

**suse1:~ # cat /etc/sssd/sssd.conf**

[sssd]

config\_file\_version = 2

services = nss, pam

# SSSD will not start if you do not configure any domains.

# Add new domain configurations as [domain/<NAME>] sections, and

# then add the list of domains (in the order you want them to be

# queried) to the "domains" attribute below and uncomment it.

; domains = LDAP

domains = AD

[nss]

filter\_users = root

filter\_groups = root

[pam]

[domain/AD]

debug\_level = 6

id\_provider = ad

auth\_provider = ad

ad\_domain = cluster.com

ad\_server = adserver.cluster.com

ad\_hostname = adserver.cluster.com

ldap\_id\_mapping = True

override\_homedir = /home/%u

ldap\_schema = ad

[domain/default]

auth\_provider = krb5

chpass\_provider = krb5

krb5\_realm = CLUSTER.COM

krb5\_server = adserver.cluster.com

krb5\_validate = False

krb5\_renewable\_lifetime = 1d

krb5\_lifetime = 1d

# Example LDAP domain

; [domain/LDAP]

; id\_provider = ldap

; auth\_provider = ldap

# ldap\_schema can be set to "rfc2307", which stores group member names in the

# "memberuid" attribute, or to "rfc2307bis", which stores group member DNs in

# the "member" attribute. If you do not know this value, ask your LDAP

# administrator.

; ldap\_schema = rfc2307

; ldap\_uri = ldap://ldap.mydomain.org

; ldap\_search\_base = dc=mydomain,dc=org

# Note that enabling enumeration will have a moderate performance impact.

# Consequently, the default value for enumeration is FALSE.

# Refer to the sssd.conf man page for full details.

; enumerate = false

# Allow offline logins by locally storing password hashes (default: false).

; cache\_credentials = true

# An example Active Directory domain. Please note that this configuration

# works for AD 2003R2 and AD 2008, because they use pretty much RFC2307bis

# compliant attribute names. To support UNIX clients with AD 2003 or older,

# you must install Microsoft Services For Unix and map LDAP attributes onto

# msSFU30\* attribute names.

; [domain/AD]

; id\_provider = ldap

; auth\_provider = krb5

; chpass\_provider = krb5

;

; ldap\_uri = ldap://your.ad.example.com

; ldap\_search\_base = dc=example,dc=com

; ldap\_schema = rfc2307bis

; ldap\_sasl\_mech = GSSAPI

; ldap\_user\_object\_class = user

; ldap\_group\_object\_class = group

; ldap\_user\_home\_directory = unixHomeDirectory

; ldap\_user\_principal = userPrincipalName

; ldap\_account\_expire\_policy = ad

; ldap\_force\_upper\_case\_realm = true

;

; krb5\_server = your.ad.example.com

; krb5\_realm = EXAMPLE.COM

suse1:~ #

**suse1:~ # cat /etc/nsswitch.conf**

#

# /etc/nsswitch.conf

#

# An example Name Service Switch config file. This file should be

# sorted with the most-used services at the beginning.

#

# The entry '[NOTFOUND=return]' means that the search for an

# entry should stop if the search in the previous entry turned

# up nothing. Note that if the search failed due to some other reason

# (like no NIS server responding) then the search continues with the

# next entry.

#

# Legal entries are:

#

# compat Use compatibility setup

# nisplus Use NIS+ (NIS version 3)

# nis Use NIS (NIS version 2), also called YP

# dns Use DNS (Domain Name Service)

# files Use the local files

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

#

# For more information, please read the nsswitch.conf.5 manual page.

#

# passwd: files nis

# shadow: files nis

# group: files nis

passwd: files sss winbind ----🡪 winbind adds automatically

group: files sss winbind

hosts: files dns

networks: files dns

services: files

protocols: files

rpc: files

ethers: files

netmasks: files

netgroup: files nis

publickey: files

bootparams: files

automount: files nis

aliases: files

suse1:~ #

-==============================================================================

**suse1:~ # cat /etc/nscd.conf**

#

# /etc/nscd.conf

#

# An example Name Service Cache config file. This file is needed by nscd.

#

# Legal entries are:

#

# logfile <file>

# debug-level <level>

# threads <initial #threads to use>

# max-threads <maximum #threads to use>

# server-user <user to run server as instead of root>

# server-user is ignored if nscd is started with -S parameters

# stat-user <user who is allowed to request statistics>

# reload-count unlimited|<number>

# paranoia <yes|no>

# restart-interval <time in seconds>

#

# enable-cache <service> <yes|no>

# positive-time-to-live <service> <time in seconds>

# negative-time-to-live <service> <time in seconds>

# suggested-size <service> <prime number>

# check-files <service> <yes|no>

# persistent <service> <yes|no>

# shared <service> <yes|no>

# max-db-size <service> <number bytes>

# auto-propagate <service> <yes|no>

#

# Currently supported cache names (services): passwd, group, hosts, services

#

# logfile /var/log/nscd.log

# threads 4

# max-threads 32

server-user nscd

# stat-user somebody

debug-level 0

# reload-count 5

paranoia no

# restart-interval 3600

enable-cache passwd no

positive-time-to-live passwd 600

negative-time-to-live passwd 20

suggested-size passwd 211

check-files passwd yes

persistent passwd yes

shared passwd yes

max-db-size passwd 33554432

auto-propagate passwd yes

enable-cache group no

positive-time-to-live group 3600

negative-time-to-live group 60

suggested-size group 211

check-files group yes

persistent group yes

shared group yes

max-db-size group 33554432

auto-propagate group yes

enable-cache hosts yes

positive-time-to-live hosts 600

negative-time-to-live hosts 0

suggested-size hosts 211

check-files hosts yes

persistent hosts no

shared hosts yes

max-db-size hosts 33554432

enable-cache services yes

positive-time-to-live services 28800

negative-time-to-live services 20

suggested-size services 211

check-files services yes

persistent services yes

shared services yes

max-db-size services 33554432

enable-cache netgroup yes

positive-time-to-live netgroup 28800

negative-time-to-live netgroup 20

suggested-size netgroup 211

check-files netgroup yes

persistent netgroup yes

shared netgroup yes

max-db-size netgroup 33554432

suse1:~ #

suse1:~ # cat /etc/pam.d/common-auth

#%PAM-1.0

#

# This file is autogenerated by pam-config. All changes

# will be overwritten.

#

# Authentication-related modules common to all services

#

# This file is included from other service-specific PAM config files,

# and should contain a list of the authentication modules that define

# the central authentication scheme for use on the system

# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the

# traditional Unix authentication mechanisms.

#

auth required pam\_env.so

auth sufficient pam\_unix.so try\_first\_pass

auth sufficient pam\_sss.so use\_first\_pass

auth required pam\_winbind.so use\_first\_pass

suse1:~ # cat /etc/pam.d/common-account

#%PAM-1.0

#

# This file is autogenerated by pam-config. All changes

# will be overwritten.

#

# Account-related modules common to all services

#

# This file is included from other service-specific PAM config files,

# and should contain a list of the account modules that define

# the central access policy for use on the system. The default is to

# only deny service to users whose accounts are expired.

#

account requisite pam\_unix.so try\_first\_pass

account sufficient pam\_localuser.so

account sufficient pam\_sss.so use\_first\_pass

account required pam\_winbind.so use\_first\_pass

suse1:~ #

suse1:~ # cat /etc/pam.d/common-session

#%PAM-1.0

#

# This file is autogenerated by pam-config. All changes

# will be overwritten.

#

# Session-related modules common to all services

#

# This file is included from other service-specific PAM config files,

# and should contain a list of modules that define tasks to be performed

# at the start and end of sessions of \*any\* kind (both interactive and

# non-interactive

#

session optional pam\_mkhomedir.so

session required pam\_limits.so

session required pam\_unix.so try\_first\_pass

session optional pam\_sss.so

session required pam\_winbind.so

session optional pam\_umask.so

session optional pam\_systemd.so

session optional pam\_env.so

suse1:~ #

suse1:~ #

suse1:~ # cat /etc/pam.d/common-password

#%PAM-1.0

#

# This file is autogenerated by pam-config. All changes

# will be overwritten.

#

# Password-related modules common to all services

#

# This file is included from other service-specific PAM config files,

# and should contain a list of modules that define the services to be

# used to change user passwords.

#

password sufficient pam\_winbind.so

password requisite pam\_cracklib.so

password sufficient pam\_unix.so use\_authtok nullok shadow try\_first\_pass

password required pam\_sss.so use\_authtok

suse1:~ #