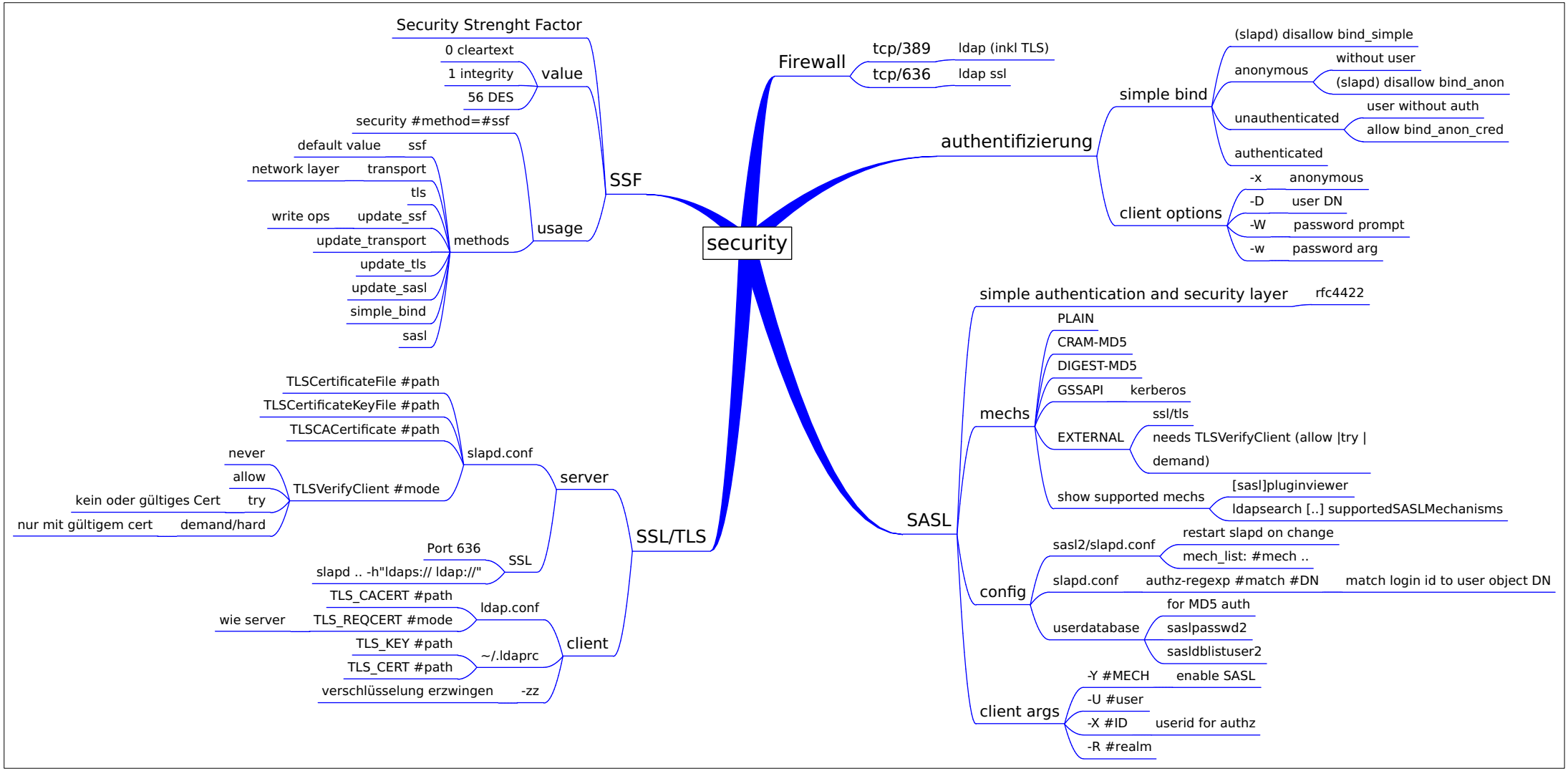
security
SSF
Security Strenght Factor
value
0 cleartext
1 integrity
56 DES
usage
security #method=#ssf
methods
default value
ssf
network layer
transport
tls
write ops
update_ssf
update_transport
update_tls
update_sasl
simple_bind
sasl
SSL/TLS
server
slapd.conf
TLSCertificateFile #path
TLSCertificateKeyFile #path
TLSCACertificate #path
TLSVerifyClient #mode
never
allow
try
kein oder gültiges Cert
demand/hard
nur mit gültigem cert
SSL
Port 636
slapd .. -h"ldaps:// ldap://"
client
ldap.conf
TLS_CACERT #path
TLS_REQCERT #mode
wie server
~/.ldaprc
TLS_KEY #path
TLS_CERT #path
-zz
verschlüsselung erzwingen
Firewall
tcp/389
ldap (inkl TLS)
tcp/636
ldap ssl
authentifizierung
simple bind
(slapd) disallow bind_simple
anonymous
without user
(slapd) disallow bind_anon
unauthenticated
user without auth
allow bind_anon_cred
authenticated
client options
-x
anonymous
-D
user DN
-W
password prompt
-w
password arg
SASL
simple authentication and security layer
rfc4422
mechs
PLAIN
CRAM-MD5
DIGEST-MD5
GSSAPI
kerberos
EXTERNAL
ssl/tls
needs TLSVerifyClient (allow |try | demand)
show supported mechs
[sasl]pluginviewer
ldapsearch [..] supportedSASLMechanisms
config
sasl2/slapd.conf
restart slapd on change
mech_list: #mech ..
slapd.conf
authz-regexp #match #DN
match login id to user object DN
userdatabase
for MD5 auth
saslpasswd2
sasldblistuser2
client args
-Y #MECH
enable SASL
-U #user
-X #ID
userid for authz
-R #realm