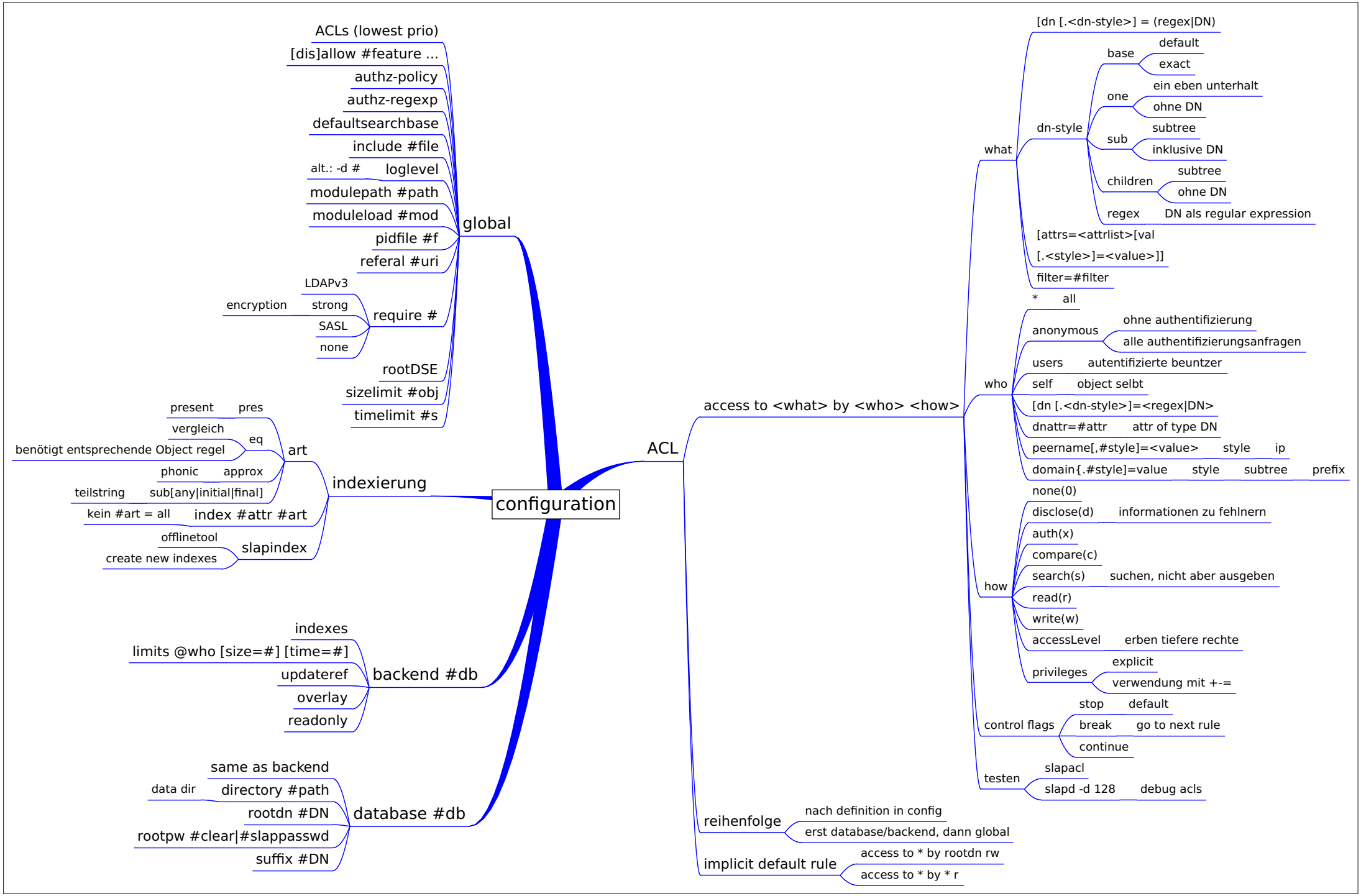
configuration
global
ACLs (lowest prio)
[dis]allow #feature ...
authz-policy
authz-regexp
defaultsearchbase
include #file
loglevel
alt.: -d #
modulepath #path
moduleload #mod
pidfile #f
referal #uri
require #
LDAPv3
strong
encryption
SASL
none
rootDSE
sizelimit #obj
timelimit #s
indexierung
art
pres
present
eq
vergleich
benötigt entsprechende Object regel
approx
phonic
sub[any|initial|final]
teilstring
index #attr #art
kein #art = all
slapindex
offlinetool
create new indexes
backend #db
indexes
limits @who [size=#] [time=#]
updateref
overlay
readonly
database #db
same as backend
directory #path
data dir
rootdn #DN
rootpw #clear|#slappasswd
suffix #DN
ACL
access to <what> by <who> <how>
what
[dn [.<dn-style>] = (regex|DN)
dn-style
base
default
exact
one
ein eben unterhalt
ohne DN
sub
subtree
inklusive DN
children
subtree
ohne DN
regex
DN als regular expression
[attrs=<attrlist>[val
[.<style>]=<value>]]
filter=#filter
who
*
all
anonymous
ohne authentifizierung
alle authentifizierungsanfragen
users
autentifizierte beuntzer
self
object selbt
[dn [.<dn-style>]=<regex|DN>
dnattr=#attr
attr of type DN
peername[,#style]=<value>
style
ip
domain{.#style]=value
style
subtree
prefix
how
none(0)
disclose(d)
informationen zu fehlnern
auth(x)
compare(c)
search(s)
suchen, nicht aber ausgeben
read(r)
write(w)
accessLevel
erben tiefere rechte
privileges
explicit
verwendung mit +-=
control flags
stop
default
break
go to next rule
continue
testen
slapacl
slapd -d 128
debug acls
reihenfolge
nach definition in config
erst database/backend, dann global
implicit default rule
access to * by rootdn rw
access to * by * r