Monitoring OpenLDAP

how to find out whether slapd is in healthy state

by Michael Ströder <michael@stroeder.com>
at LDAPcon 2017

Why detailed health check?

- Changes have risks
- Big changes impose even higher risks
- Complex configurations can go easily wrong -- with config management it could be messed up all at once ;-)
- Things can go wrong even if there's no change
- You have to react quickly -- eventually during night
- You're nervous during working on change/incident
- Ideally detailed failure information shown

What can go wrong?

- Memory leaks
- Network / firewalling messed up (other department)
- Certificates expired or renewed with wrong parameters
- Connected components are broken
- Abnormal load
- Configuration errors
- back-mdb maxsize reached
- Replication out of sync

slapd_checkmk.py -- basics (1)

- Local access via LDAPI with SASL-EXTERNAL
- Reads most config stuff from cn=config
  → not much a priori configuration needed
- Reads entries from cn=monitor with one search request
- ACLs needed to read cn=config and cn=monitor
- Runs as *root* to access some system resources
- Checks DNS resolution of *olcSaslHost*

slapd_checkmk.py -- basics (2)

- Checks wheter slapd has to be restarted due to updated slapd.conf and TLS cert/key/DHparam files
- Performance data from cn=monitor:
  - bytes and PDU counters
  - requests per request type
- Dynamically adds check items depending on database backends and syncrepl config found
  → might confuse check inventory!
- Count entries in backends with *slapo-noopsrch*

slapd_checkmk.sh

```
#!/bin/sh
# shell wrapper script for slapd_checkmk.py
# {{ ansible_managed }}

/usr/bin/python2 -ROO slapd_checkmk.py \
  'ldapi://' \
  'ldaps://slapd-c1.example.com' \
  'dn:uid=slapd-c1,ou=slapd,dc=example,dc=com'
```

slapd_checkmk.py -- TLS checks

- Server cert validity
- LDAPS connection to real service FQDN with libldap doing TLS hostname check
- Local TLS client cert mapping with SASL-EXTERNAL
- LDAPS / SASL-EXTERNAL connection to all provider replicas
- Currently does not check whether server cert on disk is really used

slapd_checkmk.py -- syncrepl checks (1)

- Parses *olcSyncrepl* attribute:
  - provider LDAP URL
  - authc information
  - network parameters (timeouts etc.)
- LDAPS / SASL-EXTERNAL connection to all provider replicas to read and compare *contextCSN*
- Full replication topology is checked

slapd_checkmk.py -- syncrepl checks (2)

- Many providers means many check items
- Many alarms even if only one provider is down
- Many providers unreachable → many timeouts → check interval exceeded
- Sometimes false alarms regarding *contextCSN*

slapd_checkmk.py -- back-sock

- Find back-sock listeners configured as overlay in cn=config
- back-sock listeners implemented with *python-slapdsock* with internal monitoring
- Send custom *MONITOR* request to
  - check connectivity
  - query performance data

To-do

- Customizable output to feed into different monitoring systems (next: Prometheus)
- Support syncrepl check with simple bind and StartTLS
- Multi-threading to shorten provider over-all check latency in case many providers are unreachable
- New check memory/swap size used by slapd (mem-leaks)
- check MDB maxsize (preferrably without invoking CLI tool)

Wish list for cn=monitor

- Error counters, e.g. invalidCredentials(49)
- back-mdb stats to avoid invoking an external CLI tool or library (likely separetely linked)
- syncrepl state information?

Conclusion

- Useful as health check even without monitoring backend :-)
- Many check items may cause many alarms -- annoying to admins
  → Use monitoring with check hierarchy to reduce alarms
- Use short time-outs to not exceed check interval time
- Grab it: https://www.stroeder.com/software.html