
Vortrag SLAC 2023

OpenLDAP 2.5/2.6. Was ist neu?

Autor:
Stefan KANIA

Ort:
St. Michaelisdonn

16. Mai 2023

1 Übersicht

Seit Dezember 2021 ist der OpenLDAP endlich in einer neuen Version verfügbar. So einiges hat sich geändert und viel neues ist dazu gekommen. Seit der finalen Veröffentlichung der Version 2.5 wurde der Support für die Version 2.4 komplett eingestellt und hat mittlerweile den Status "historical". Selbst Sicherheitsupdates wird es nicht mehr geben. Darum wird es Zeit, bestehende 2.4 Installationen zu aktualisieren.

In diesem Vortrag werde ich die Neuerungen ansprechen und an Hand von Beispielen zeigen.

2 Neuerungen rund um OpenLDAP

- Ersatz des Overlay "memberOf" durch dynamische Gruppen
- Replikation in der Multiproviderumgebung
- Replikation von cn=config
- Die neuen Tools `slapmodify` und `slapdelete` erlauben die Änderung einer Datenbank, auch wenn der Dienst nicht läuft.
- `slapd-watcher` ein Tool zur Prüfung der Replikation in einer Multiproviderumgebung.
- *Large Multi-valued Attribute Support*. Multi-valued Attribute mit sehr vielen Werten werden schneller verarbeitet. Das betrifft sowohl die Suche, als auch das Ändern oder Löschen von Einträgen.
- Der neu Passwordhash *ARGON2* wurde eingeführt. Der Passwordhash sorgt für einen besseren Schutz gegen Brute-force Angriffe, da es nicht mehr reicht viel Rechenleistung zur Verfügung zu stellen, sondern es wird auch eine definierbare Menge an Arbeitsspeicher für das Entschlüsseln benötigt.
- *LDAP Transaction Support*. Beim Einsatz von LMDB als Datenbankbackend können mehrere Operationen zusammen bestätigt werden. Nicht mehr jede einzelne Aktion muss bestätigt werden. Kommt es bei einer Aktion zu einem Fehler, werden alle bis dahin angewendeten Änderungen zurückgezogen.
- Neue Replikationsprotokolle. OpenLDAP kann jetzt Einträge von anderen legacy LDAP Verzeichnissen, zum Beispiel Microsoft Active Directory, replizieren. Zusätzlich zu den eigenen Replikationsprotokollen *Syncrepl* und *Delta Syncrepl*, werden die Microsoft Active Directory Protokolle und DSEE/ODSEE vom Oracle Directory Server unterstützt.
- Mehr Faktoren Authentifizierung Multi-Factor Authentication. Verschiedene Methoden wie zum Beispiel TOTP oder HOTP werden unterstützt
- Das neues Datenbankbackend *Wiredtiger* wurde eingefügt ist aber noch Experimental. Muss immer explizit kompiliert werden.
- Direktes löschen von Overlays und Datenbanken aus der dynamischen Konfiguration. Wenn ein Overlay entfernt werden soll, muss der slapd nicht mehr gestoppt werden.
- In allen Versionen bis 2.4 gibt es einen einzigen Thread-Pool, der Worker-Threads für jede Operation zuweist. Da diese Zuweisung über eine einzige Warteschlange mit einem einzigen lock erfolgt, gerät sie bei großen Arbeitslasten ziemlich ins Stocken und lässt sich nicht gut auf mehrere Kerne skalieren. Daher ist in 2.5 eine konfigurierbare Anzahl von Warteschlangen erlaubt. Dadurch lässt sich der OpenLDAP auf multi-Prozessorsystemen besser skalieren.
- Mit *Asynchronous Meta-directory* von OpenLDAP wurde das Standard meta-directory backend überarbeitet. Mit dem Standard meta-backend ist es lediglich möglich eine kleine Anzahl von LDAP-Server zusammen zu fassen. Mit dem neue Backend ist es möglich, mehrere tausend LDAP-Server zusammen zu fassen, ohne das darunter die Performance leidet. Die Einrichtung und Verwaltung ist aber erheblich komplexer als das meta-directory Backend.

3 Neuen Overlays

- **autoca**
Mit diesem Overlay können X.509 certificate authority Funktionen über OpenLDAP ausgerollt werden. Es kann eine eigene CA erstellt werden, die dann dafür sorgt, dass für Benutzer und hosts eigene Zertifikate und Schlüssel generiert werden.
- **homedir**
Das Overlay verwaltet den kompletten Lebenszyklus eines Benutzerverzeichnis von der Erstellung bis zur Archivierung und Löschung. Diese Funktion wurde hauptsächlich für Umgebungen erstellt, in denen die Benutzerauthentifizierung über LDAP durchgeführt wird und die Benutzer über Homedirectories im Netz verfügen.
- **otp**
Über dieses Overlay können zeit- und zählerbasierte one-time Passwörter verwaltet werden. Diese Funktion kann für die 2FA genutzt werden. Zur Erzeugung des zweiten Faktors kann, zum Beispiel der google-authenticator verwendet werden.
- **ppm**
Dabei handelt es sich eigentlich um eine Erweiterung zum Overlay *ppolicy*. Es erlaubt zusätzliche Module zu laden, die weitere Kriterien für die Passwörter hinzufügen. Ein Beispiel findet sich unter <https://gitlab.ow2.org/ldaptoolbox/ppm/-/blob/master/ppm.md>
- **pw-radius**
Das Overlay leitet bind-Operationen an Radius-Server weiter. Bei dem Overlay handelt es sich um ein *contrib-overlay*, das in den Standardpaketen nicht enthalten ist.
- **remoteauth**
Ein mit dem remoteauth-Overlay konfigurierter OpenLDAP-Server bearbeitet eine Authentifizierungsanfrage auf der Grundlage des Vorhandenseins des Attributs *userPassword* im lokalen Eintrag. Wenn das *userPassword* vorhanden ist, wird die Authentifizierung lokal durchgeführt, andernfalls führt das Remoteauth-Overlay die Authentifizierungsanforderung an den konfigurierten Remoteverzeichnis-Server durch.
- **variant**
Dieses Overlay ermöglicht die gemeinsame Nutzung des Wertes eines Attributs in unterschiedlichen Objekten. Im Gegensatz zum Overlay *collect*, können die Quell- und Zielattribute unterschiedlich sein. Auch werden für die Zuweisung der Werte eines Attributs reguläre Ausdrücke unterstützt. So ist es möglich, zum Beispiel, allen Mitarbeitern einer Abteilung immer die entsprechenden Abteilungstelefonnummer zuzuweisen.

4 Overlays mit neuen Funktionen

Einige bestehende Overlays wurden überarbeitet und mit neuen Funktionen ausgestattet.

- **pcache**
Neue Steuerung ermöglicht den Zugriff auf die Cache-DBn. Überwachungsinformationen für den Pcache sind jetzt verfügbar, wenn der Back-Monitor aktiviert ist.
- **ppolicy**
Das Overlay wurde aktualisiert, um dem Entwurf der *draft-behera-ldap-password-policy-10* zu entsprechen. Optional werden die Netscape Password Expiring und Password Expired Controls unterstützt.
- **dynlist**
Das Overlay kann jetzt, neben den bekannten Funktionen, das Attribut *memberOf* dynamisch verwalten. Das Overlay *memberOf* hat jetzt den Status *deprecated* und sollte nicht mehr genutzt werden. Vorteil ist, dass das Overlay auch nachträglich eingerichtet werden kann und alle Gruppenzugehörigkeiten gefunden werden. Das gilt aber, wie schon beim Overlay *memberof* nur für Gruppen, die eine vollständigen DN für die Mitglieder verwaltet.

- unique

Das Overlay kann jetzt die gesamte Datenbank sperren um *race conditions* zu verhindern. So ist es nicht mehr möglich einen Wert in zwei verschiedene Objekte zur selben Zeit zu schreiben.