OpenLDAP 2.5/2.6 was gibt es Neues?

Stefan Kania

SLAC 2023
23.-25. Mai 2023 | Berlin

24. Mai 2023

Stefan Kania
IT-Consulting durch Training

Kurzfassung

Eine schnelle Übersicht

Kurzfassung

Eine schnelle Übersicht

- OpenLDAP 2.4 hat nach 14 Jahren ausgedient

Kurzfassung

Eine schnelle Übersicht

- OpenLDAP 2.4 hat nach 14 Jahren ausgedient
- OpenLDAP 2.4 hat jetzt den Status ”Historical”

Kurzfassung

Eine schnelle Übersicht

- OpenLDAP 2.4 hat nach 14 Jahren ausgedient
- OpenLDAP 2.4 hat jetzt den Status ”Historical”
- Der neue OpenLDAP hat eine erheblich bessere Performance

Kurzfassung

Eine schnelle Übersicht

- OpenLDAP 2.4 hat nach 14 Jahren ausgedient
- OpenLDAP 2.4 hat jetzt den Status ”Historical”
- Der neue OpenLDAP hat eine erheblich bessere Performance
- Die Replikation von cn=config funktioniert

Kurzfassung

Eine schnelle Übersicht

- OpenLDAP 2.4 hat nach 14 Jahren ausgedient
- OpenLDAP 2.4 hat jetzt den Status ”Historical”
- Der neue OpenLDAP hat eine erheblich bessere Performance
- Die Replikation von cn=config funktioniert
- Overlay memberOf ist endlich deprecated

Kurzfassung

Eine schnelle Übersicht

- OpenLDAP 2.4 hat nach 14 Jahren ausgedient
- OpenLDAP 2.4 hat jetzt den Status ”Historical”
- Der neue OpenLDAP hat eine erheblich bessere Performance
- Die Replikation von cn=config funktioniert
- Overlay memberOf ist endlich deprecated
- Eigener Loadbalancer

Kurzfassung

Eine schnelle Übersicht

Kurzfassung

Eine schnelle Übersicht

- Viele neue Overlay

Kurzfassung

Eine schnelle Übersicht

- Viele neue Overlay
- Andere Overlays wurden überarbeitet

Kurzfassung

Eine schnelle Übersicht

- Viele neue Overlay
- Andere Overlays wurden überarbeitet
- OpenLDAP 2.5 LTS Version

Kurzfassung

Eine schnelle Übersicht

- Viele neue Overlay
- Andere Overlays wurden überarbeitet
- OpenLDAP 2.5 LTS Version
- OpenLDAP 2.6 full feature Version

Kurzfassung

Neue Overlay im Schnelldurchlauf

Kurzfassung

Neue Overlay im Schnelldurchlauf

- **autoca** zur Zertifikatsverwaltung

Kurzfassung

Neue Overlay im Schnelldurchlauf

- **autoca** zur Zertifikatsverwaltung
- **homedir** verwaltet den Lebenszyklus von Benutzerverzeichnissen im Netz

Kurzfassung

Neue Overlay im Schnelldurchlauf

- **autoca** zur Zertifikatsverwaltung
- **homedir** verwaltet den Lebenszyklus von Benutzerverzeichnissen im Netz
- **otp** Ja, OpenLDAP kann jetzt 2FA

Kurzfassung

Neue Overlay im Schnelldurchlauf

- **autoca** zur Zertifikatsverwaltung
- **homedir** verwaltet den Lebenszyklus von Benutzerverzeichnissen im Netz
- **otp** Ja, OpenLDAP kann jetzt 2FA
- **ppm** Erweiterung von ppolicy

Kurzfassung

Neue Overlay im Schnelldurchlauf

- **autoca** zur Zertifikatsverwaltung
- **homedir** verwaltet den Lebenszyklus von Benutzerverzeichnissen im Netz
- **otp** Ja, OpenLDAP kann jetzt 2FA
- **ppm** Erweiterung von ppolicy
- **pw-radius** leitet bind-requests an radius-Server weiter

Kurzfassung

Neue Overlay im Schnelldurchlauf

- **autoca** zur Zertifikatsverwaltung
- **homedir** verwaltet den Lebenszyklus von Benutzerverzeichnissen im Netz
- **otp** Ja, OpenLDAP kann jetzt 2FA
- **ppm** Erweiterung von ppolicy
- **pw-radius** leitet bind-requests an radius-Server weiter
- **remoteauth** zur Weiterleitung von Authentifizierung

Kurzfassung

Neue Overlay im Schnelldurchlauf

- **autoca** zur Zertifikatsverwaltung
- **homedir** verwaltet den Lebenszyklus von Benutzerverzeichnissen im Netz
- **otp** Ja, OpenLDAP kann jetzt 2FA
- **ppm** Erweiterung von ppolicy
- **pw-radius** leitet bind-requests an radius-Server weiter
- **remoteauth** zur Weiterleitung von Authentifizierung
- **variant** Werte eines Attributes mit anderen Objekten teilen

Kurzfassung

Overlays im Neuerungen

Kurzfassung

Overlays im Neuerungen

- **pcache** Zugriff auf cache-DB möglich für cn=monitor

Kurzfassung

Overlays im Neuerungen

- **pcache** Zugriff auf cache-DB möglich für cn=monitor
- **ppolicy** entspricht jetzt ”draft-behera-ldap-password-policy-10”.

Kurzfassung

Overlays im Neuerungen

- **pcache** Zugriff auf cache-DB möglich für cn=monitor
- **ppolicy** entspricht jetzt ”draft-behera-ldap-password-policy-10”.
- **dynlist** Kann jetzt auch memberOf

Kurzfassung

Overlays im Neuerungen

- **pcache** Zugriff auf cache-DB möglich für cn=monitor
- **ppolicy** entspricht jetzt ”draft-behera-ldap-password-policy-10”.
- **dynlist** Kann jetzt auch memberOf
- **unique** sperrt die gesamte DB als Schutz vor *race conditions*

Neue Overlays

Zertifikate mit autoca

Neue Overlays

Zertifikate mit autoca

- automatische Erstellung von Zertifikaten für Benutzer und Hosts

Neue Overlays

Zertifikate mit autoca

- automatische Erstellung von Zertifikaten für Benutzer und Hosts
- Verwaltung der eigene CA zur Erstellung der Zertifikate

Neue Overlays

Zertifikate mit autoca

- automatische Erstellung von Zertifikaten für Benutzer und Hosts
- Verwaltung der eigene CA zur Erstellung der Zertifikate
- Zertifikate werden mit ”ldapsearch” erzeugt

Neue Overlays

Zertifikate mit autoca

- automatische Erstellung von Zertifikaten für Benutzer und Hosts
- Verwaltung der eigene CA zur Erstellung der Zertifikate
- Zertifikate werden mit ”ldapsearch” erzeugt
- Zertifikate liegen in den Objekten als Binärdatei

Neue Overlays

Basisverzeichnisse mit homedir

Neue Overlays

Basisverzeichnisse mit homedir

- Verwaltung von Basisverzeichnissen der Benutzer im Netz

Neue Overlays

Basisverzeichnisse mit homedir

- Verwaltung von Basisverzeichnissen der Benutzer im Netz
- Erstellung von Verzeichnissen

Neue Overlays

Basisverzeichnisse mit homedir

- Verwaltung von Basisverzeichnissen der Benutzer im Netz
- Erstellung von Verzeichnissen
- Backup von Verzeichnissen

Neue Overlays

Basisverzeichnisse mit homedir

- Verwaltung von Basisverzeichnissen der Benutzer im Netz
- Erstellung von Verzeichnissen
- Backup von Verzeichnissen
- Archivierung von Verzeichnissen

Neue Overlays

Basisverzeichnisse mit homedir

- Verwaltung von Basisverzeichnissen der Benutzer im Netz
- Erstellung von Verzeichnissen
- Backup von Verzeichnissen
- Archivierung von Verzeichnissen
- Löschen von Verzeichnissen

Neue Overlays

One time password und 2FA mit otp

Neue Overlays

One time password und 2FA mit otp

- Zeit- oder zählerbasierte Passwörter

Neue Overlays

One time password und 2FA mit otp

- Zeit- oder zählerbasierte Passwörter
- Erstellung des QR-Codes für authenticator App

Neue Overlays

Strenger Passwortregeln mit ppm

Neue Overlays

Strenger Passwortregeln mit ppm

- ppm ist kein eigentliche Overlay, mehr eine Erweiterung

Neue Overlays

Strenger Passwortregeln mit ppm

- ppm ist kein eigentliche Overlay, mehr eine Erweiterung
- Kann von ppolicy zur Erweiterung der Richtlinien genutzt werden

Neue Overlays

Bind an Radius-Server mit pw-radius

Neue Overlays

Bind an Radius-Server mit pw-radius

- Leitet bind-requests an einen Radius-Server weiter

Neue Overlays

Bind an Radius-Server mit pw-radius

- Leitet bind-requests an einen Radius-Server weiter
- Ist ein contrib-Overlay nicht im Standard enthalten

Neue Overlays

Authentifizierung mit remoteauth

Neue Overlays

Authentifizierung mit remoteauth

- Verwendet das Attribute ”userPassword”

Neue Overlays

Authentifizierung mit remoteauth

- Verwendet das Attribute ”userPassword”
- Ist das Attribut vorhanden, lokale Authentifizierung

Neue Overlays

Authentifizierung mit remoteauth

- Verwendet das Attribute ”userPassword”
- Ist das Attribut vorhanden, lokale Authentifizierung
- Ist das Attribut nicht vorhanden, Weiterleitung der Authentifizierung

Neue Overlays

Gemeinsam genutzte Attribute mit variant

Neue Overlays

Gemeinsam genutzte Attribute mit variant

- Werte eines Attribute eines Objekts können weitergereicht werden

Neue Overlays

Gemeinsam genutzte Attribute mit variant

- Werte eines Attribute eines Objekts können weitergereicht werden
- Die Attribute von Quelle und Ziel können unterschiedlich sein (anders als collect)

Neue Overlays

Gemeinsam genutzte Attribute mit variant

- Werte eines Attribute eines Objekts können weitergereicht werden
- Die Attribute von Quelle und Ziel können unterschiedlich sein (anders als collect)
- Die Verwendung von Regulären Ausdrücken ist möglich

Neue Overlays

Gemeinsam genutzte Attribute mit variant

- Werte eines Attribute eines Objekts können weitergereicht werden
- Die Attribute von Quelle und Ziel können unterschiedlich sein (anders als collect)
- Die Verwendung von Regulären Ausdrücken ist möglich
- Add und Delete der alternativen Attribute führen zu ”constraint violation”

Geänderte Overlays

Monitoring für pcache

Geänderte Overlays

Monitoring für pcache

- Der direkte Zugriff auf die cache-DB ist möglich

Geänderte Overlays

Monitoring für pcache

- Der direkte Zugriff auf die cache-DB ist möglich
- cn=monitor wertet den cache aus

Geänderte Overlays

Passwortrichtlinien mit ppolicy

Geänderte Overlays

Passwortrichtlinien mit ppolicy

- Anpassung an ”draft-behera-ldap-password-policy-10”

Geänderte Overlays

Passwortrichtlinien mit ppolicy

- Anpassung an ”draft-behera-ldap-password-policy-10”
- Schema ist integriert

Geänderte Overlays

Passwortrichtlinien mit ppolicy

- Anpassung an ”draft-behera-ldap-password-policy-10”
- Schema ist integriert
- Unterstützung der Netscape Passwortregeln

Geänderte Overlays

Listen mit dynlist

Geänderte Overlays

Listen mit dynlist

- Vollwertiger Ersatz für Overlay memberOf

Geänderte Overlays

Listen mit dynlist

- Vollwertiger Ersatz für Overlay memberOf
- kann auch noch nachträglich eingerichtet werden

Geänderte Overlays

Listen mit dynlist

- Vollwertiger Ersatz für Overlay memberOf
- kann auch noch nachträglich eingerichtet werden
- Generierung des Attributs memberOf on the fly

Geänderte Overlays

Eindeutigkeit mit unique

Geänderte Overlays

Eindeutigkeit mit unique

- Komplette DB-sperre verhindert ”race condition”

Loadbalancer mit lloadd

Protokollorientierter Loadbancer

Loadbalancer mit lloadd

Protokollorientierter Loadbancer

- Weiterleitung der Authentifizierung mit Proxyauth

Loadbalancer mit lloadd

Protokollorientierter Loadbancer

- Weiterleitung der Authentifizierung mit Proxyauth
- write_coherence über ”sticky sessions”(Nur 2.6)

Loadbalancer mit lloadd

Protokollorientierter Loadbancer

- Weiterleitung der Authentifizierung mit Proxyauth
- write_coherence über ”sticky sessions”(Nur 2.6)
- Weiterleitung auf pro-operation-base nicht pro-connection-base

Loadbalancer mit lloadd

Protokollorientierter Loadbancer

- Weiterleitung der Authentifizierung mit Proxyauth
- write_coherence über ”sticky sessions”(Nur 2.6)
- Weiterleitung auf pro-operation-base nicht pro-connection-base
- standalone Daemon oder über slapd

Loadbalancer mit lloadd

Protokollorientierter Loadbancer

- Weiterleitung der Authentifizierung mit Proxyauth
- write_coherence über ”sticky sessions”(Nur 2.6)
- Weiterleitung auf pro-operation-base nicht pro-connection-base
- standalone Daemon oder über slapd
- Überwachung mittels cn=monitor

Abbildung: And now the practical part