ELO Indexserver LDAP-Schnittstelle

[Stand: 07.05.2020 | Programmversion: 11.00.000/12.00.000]

Dieses Dokument beschreibt die LDAP-Schnittstelle des ELO Indexservers.

Inhalt

1 Überblick ... 3
1.1 Konfigurationsvorschlag auf der Basis der Systemumgebung ... 3
1.2 Umstieg von der LDAP-Schnittstelle des ELO Access Managers ... 4
2 Funktionsweise ... 6
2.1 Anmeldung mit Namen und Kennwort ... 6
2.1.1 Neuer Benutzer ... 6
2.1.2 Benutzerattribute zuweisen ... 6
2.1.3 Gruppenabgleich ... 7
2.1.4 Vorgesetzten übernehmen ... 7
2.2 SSO-Anmeldung ... 7
2.2.1 SSO mit Domänenname ... 8
2.3 E-Mail-Anmeldung ... 8
2.3.1 Neuer Benutzer ... 8
3 Konfiguration ... 9
3.1 Globale Einstellungen ... 9
3.1.1 Neue Benutzer automatisch erstellen: createNewUser ... 9
3.1.2 Gruppenabgleich: assignGroups ... 9
3.1.3 Benutzer nicht über LDAP authentifizieren: notResponsibleForUserOrGroupIds 10
3.2 Einstellungen je Domäne ... 10
3.2.1 LDAP-Server ... 10
3.2.2 LDAP-ELO-Benutzerzuordnung: attributeForUserPropOS ... 11

3.2.3 Domänenpräfix: domainPrefix 12
3.2.4 Domänenname: name 12
3.2.5 ELO Benutzername bilden: nameFormatter 13
3.2.6 Technisches Konto, defaultUserName, defaultUserPasswordEncr 13
3.2.7 LDAP-Verzeichniszweige mit Benutzern: personSearchDNList 13
3.2.8 LDAP-Verzeichniszweige mit Gruppen: groupSearchDNList 13
3.2.9 Erforderliche Mitgliedschaft: requiredGroup 14
3.2.10 Verbindungs-Timeout: connectionTimeoutSeconds 14
3.2.11 Such-Timeout: searchTimeLimitSeconds 14
3.2.12 Tiefe der rekursiven Gruppensuche: maxGroupNesting 14
3.2.13 Attributname der Gruppenmitgliedschaften: attributeNameMemberOf 14
3.2.14 Attributname der Mailadresse: attributeNameMail 14
3.2.15 Suchfilter für Gruppen eines Benutzers: searchFilterForGroups 15
3.2.16 Suchfilter für Benutzer: searchFilterForPerson 15
3.2.17 Suchfilter für E-Mail-Adressen: searchFilterForMail 15
3.2.18 Attribute, die in ELO gespeichert werden sollen: attributesToRead 15
3.2.19 Attributname für den Administrator eines Benutzers: parentOfNewUser 15
3.2.20 LDAP-Verbindungsoptionen: initialContextEnvironment 16
4 Skripting 17

1 Überblick

ELO Benutzer können ab ELO 11 über ein Indexserver-Plugin gegen LDAP authentifiziert werden. Die Konfiguration erfolgt in einer Textdatei im JSON-Format, die im Konfigurationsverzeichnis des ELO Indexservers liegt.

(Beispielsweise: */elo/config/ix-<Archivname>/ELO-<Servername>-1/ldap.json*)

Beispiel einer ldap.json-Datei mit den wichtigsten Einstellungen:

```
{
  "createNewUser": true,
  "assignGroups": true,
  "notResponsibleForUserOrGroupIds": [
    "0"
  ],
  "domains": [
    {
      "servers": [
        {
          "ldapUrl": "ldap://srvp03.elo.local:389",
        …
      ],
      "attributeForUserPropOS": "sAMAccountName",
      "name": "ELO.LOCAL",
      "domainPrefix": "ELO\\",
      "defaultUserName": "fritzfrei@elo.local",
      "defaultUserPasswordEncr": "…",
      "personSearchDNList": [
        "DC=ELO,DC=LOCAL"
      ],
      "groupSearchDNList": [
      ],
      "nameFormatter": "$CN$",
      "searchFilterForPerson":"(&(objectclass=person)(sAMAccountName={0}))"
      …
    }
  ]
}
```

1.1 Konfigurationsvorschlag auf der Basis der Systemumgebung

Nach dem ersten Start des ELO Indexservers findet man im Konfigurationsverzeichnis des ELO Indexservers die Datei *ldap-auto.json*. Sie enthält eine LDAP-Schnittstellenkonfiguration, die aus den Einstellungen der Server-Umgebung abgeleitet ist.

Um die Datei zu aktivieren, muss sie in *ldap.json* umbenannt werden. Mit wenigen Anpassungen sollte es möglich sein, eine passende Konfiguration zu erstellen.

Erforderliche Anpassungen:

- LDAP-Anbindung des ELO Access Managers ausschalten: Tabelle *amoptions*, optid=50, optvalue="false".

Entfernen Sie "(E10…E10E42)" aus `notResponsibleForUserOrGroupIds`, wenn „ELO Service" über LDAP authentifiziert werden soll. Es bleibt: `"notResponsibleForUserOrGroupIds": [ "0"],`

- Geben Sie `defaultUserName` und `defaultUserPasswordEncr` an (siehe *3.2.6 Technisches Konto, defaultUserName, defaultUserPasswordEncr*), damit SSO funktioniert (siehe *2.2 SSO-Anmeldung*).
- Geben Sie in `personSearchDNList` die Liste der Verzeichniszweige an, in denen Benutzer gesucht werden.
- Geben Sie in `groupSearchDNList` die Liste der Verzeichniszweige an, die für den Gruppenabgleich relevante Gruppen enthalten (siehe *2.1.3 Gruppenabgleich*).
- ELO 12: Setzen Sie `attributeSuperior`, damit der Vorgesetzte übernommen wird (siehe *2.1.4 Vorgesetzten übernehmen*).

1.2 Umstieg von der LDAP-Schnittstelle des ELO Access Managers

Um den Umstieg von der LDAP-Schnittstelle des ELO Access Mangers zu erleichtern, kann das LDAP-Plugin die alte *ldap.cfg* in eine neue *ldap.json* umwandeln. Das Vorgehen dazu ist wie folgt:

- Stellen Sie sicher, dass die LDAP-Schnittstelle des ELOam eingeschaltet ist:
  - Tabelle *amoptions*, optid=50, optvalue='true'
- Stellen Sie sicher, dass die ADUser-Klasse aktiv ist:
  - Tabelle *amoptions*, optid=51, optvalue='…ADUser'
- Kopieren Sie die Datei *ldap.cfg* ins Konfigurationsverzeichnis des ELO Indexservers.
- Starten Sie den ELO Indexserver neu
- Kontrollieren Sie Einstellungen in der Datei *ldap.json*. Insbesondere muss die Einstellung für die Zuweisung des Benutzernamens gleich sein (bspw. `"nameFormatter": "$CN$"`), andernfalls können sich die Benutzer nicht mehr mit dem ELO-Benutzernamen anmelden.
- Deaktivieren Sie die LDAP-Schnittstelle des ELOam:
  - Tabelle *amoptions*, optid=50, optvalue='false'

- Starten Sie ELO Indexserver und ELOam (ELO 11) neu.

2 Funktionsweise

2.1 Anmeldung mit Namen und Kennwort

Die Authentifizierung gegen den LDAP-Server erfolgt im LDAP-Plugin grundsätzlich mit einem **userPrincipalName**, unabhängig von den Konfigurationseinstellungen.

Allerdings gibt der Benutzer in der Regel nicht den userPrincipalName sondern seinen ELO Benutzernamen zur Anmeldung an, und **der userPrincipalName muss aus den Benutzerdaten ermittelt werden**.

Folglich wird vor der Anmeldung am LDAP-Server versucht, den Benutzer im ELO zu finden. Dafür wird der Benutzer-Cache im ELO Indexserver nach dem angegebenen Namen durchsucht.

In dem gefunden Benutzerdatensatz dient das Feld *Windows-Benutzer* als Ausgangswert für die Anmeldung am LDAP. Es enthält standardmäßig den **sAMAccountName**, ggf. mit vorangestelltem Domäenenpräfix (siehe *3.2.3 Domänenpräfix: domainPrefix*). Der userPrincipalName wird daraus abgeleitet mit:

`userPrincipalName = sAMAccountName + @ + Domäne`.

Mit der Einstellung `attributeForUserPropOS` (siehe *3.2 Einstellungen je Domäne*), kann der Windows-Benutzer auf den „echten" userPrincipalName umgestellt werden. Allerdings ergibt sich dadurch eine Einschränkung bei SSO (siehe *2.2 SSO-Anmeldung*).

2.1.1 Neuer Benutzer

Wenn sich ein **neuer Benutzer** erstmalig am ELO anmeldet, muss er **den sAMAccountName oder den userPrincipalName angeben,** weil es noch keinen Datensatz zum Benutzer gibt, in dem der Windows-Benutzer hinterlegt ist.

2.1.2 Benutzerattribute zuweisen

Nach erfolgreicher Anmeldung werden die Benutzerattribute über eine Suche im LDAP-System ermittelt. Gesucht wird in den Zweigen des LDAP-Systems, die in der Einstellung `personSearchDNList` (siehe *3.2.7 LDAP-Verzeichniszweige mit Benutzern: personSearchDNList*) aufgelistet sind. Die Suche wird eingeschränkt auf den Filterausdruck `searchFilterForPerson` (siehe *3.2.16 Suchfilter für Benutzer: searchFilterForPerson*). Ihm wird als Parameter das in `attributeForUserPropOS` (siehe *3.2.2 LDAP-ELO-Benutzerzuordnung: attributeForUserPropOS*) definierte Attribut übergeben (sAMAccountName oder userPrincipalName).

Die Attribute aus dem LDAP-Server werden in den ELO Benutzerdatensatz übernommen. Beispielsweise wird für den ELO Benutzernamen die Einstellung `nameFormatter` (siehe *3.2.5 ELO Benutzername bilden: nameFormatter*) ausgewertet.

2.1.3 Gruppenabgleich

Die LDAP-Gruppenzuordnung kann im ELO nachgebildet werden, wenn die Option `assignGroups` (siehe *3.1.2 Gruppenabgleich: assignGroups*) gesetzt ist. In den LDAP-Verzeichniszweigen `groupSearchDNList` (siehe *3.2.8 LDAP-Verzeichniszweige mit Gruppen: groupSearchDNList*) wird unter der Einschränkung von `searchFilterForGroups` (siehe *3.2.15 Suchfilter für Gruppen eines Benutzers: searchFilterForGroups*) nach den Gruppen eines Benutzers gesucht. Die Auflösungstiefe von ineinander geschachtelten Gruppen kann mit der Option `maxGroupNesting` (siehe *3.2.12 Tiefe der rekursiven Gruppensuche: maxGroupNesting*) begrenzt werden.

2.1.4 Vorgesetzten übernehmen

Der im LDAP-Verzeichnis angegebene Vorgesetzte eines Benutzers kann ins ELO übernommen werden.

> **Information:** Der Vorgesetzte muss bereits im ELO existieren, andernfalls gibt es eine WARN-Meldung in der Log-Datei.

In ELO 11 muss in der Option `attributesToRead` das Attribut `manager` aufgeführt sein, damit die Übernahme funktioniert (siehe *3.2.18 Attribute, die in ELO gespeichert werden sollen: attributesToRead*).

In ELO 12 muss in der Option `attributeSuperior` der Attributnamen angegeben werden, in dem der Vorgesetzte gespeichert ist

2.2 SSO-Anmeldung

Bei der SSO-Anmeldung wird der Benutzer selbst nicht gegen den LDAP-Server authentifiziert. Es wird angenommen, dass dies bereits vom vorgeschalteten SSO-Mechanismus sichergestellt ist. Stattdessen erfolgt eine Anmeldung am LDAP-Server mit einem technischen Konto, mit dem im LDAP-Server nach den Gruppen und Attributen des Benutzers gesucht wird. Das technische Konto wird in der Konfigurationsdatei durch `defaultUserName` und `defaultUserPasswordEncrypted` angegeben (siehe *3.2.6 Technisches Konto, defaultUserName, defaultUserPasswordEncr*).

Das SSO liefert als Ergebnis den sAMAccountName. Unter diesem Namen wird der zugehörige ELO-Benutzer im Benutzer-Cache gesucht. Sofern sAMAccountName als Windows-Benutzer hinterlegt ist, ist die Suche erfolgreich.

Mit der Option `attributeNameForPropOS` kann der Windows-Benutzer jedoch auf den userPrincipalName eingestellt sein. Damit der Benutzer trotzdem zugeordnet werden kann, muss in diesem Fall der ELO Benutzername gleich dem sAMAccountName sein.

2.2.1 SSO mit Domänenname

Als Benutzername gibt die SSO-Anmeldung standardmäßig nur den sAMAccountName ohne vorangestellte Domäne weiter, was bei mehreren Domänen in der Konfiguration nicht ausreichend ist. Um den Benutzernamen in der Form `<Domäne>\<sAMAccountName>` zu bekommen, ist folgende Zeile in der **Config-Datei des ELO Indexservers** (*config.xml)* anzugeben:

```
<entry key="ntlm.domainUserFormat">{0}\{1}</entry>
```

Als Domänenname erhält man über SSO den „kurzen" (NetBIOS) Namen – nicht den DNS-Namen. Dieser kurze Domänenname muss als Domänenpräfix (siehe *3.2.3 Domänenpräfix: domainPrefix*) konfiguriert werden.

> **Information:** Um Domänen-Administrator und ELO Administrator trennen zu können, ist die ELO Indexserver-Option `sso.preventAdministrator="true"` zu setzen. Die Option verhindert, dass sich der Benutzer *Administrator* per SSO anmelden kann.

2.3 E-Mail-Anmeldung

Im ersten Schritt wird die E-Mail-Adresse im Benutzer-Cache gesucht und wie in Abschnitt *2.1 Anmeldung mit Namen und Kennwort* verfahren.

2.3.1 Neuer Benutzer

Ist die E-Mail-Adresse nicht im Benutzer-Cache bekannt, wird eine Anmeldung am LDAP-Server mit E-Mail-Adresse als userPrincipalName versucht. Scheitert die Anmeldung, wird eine Sitzung über ein technisches Konto erstellt, das in `defaultUserName` und `defaultUserPasswordEncrypted` angegeben ist (siehe *3.2.6 Technisches Konto, defaultUserName, defaultUserPasswordEncr*).

Mit dieser Sitzung wird der sAMAccountName oder userPrincipalName gesucht, der zum Benutzer mit der gegebenen E-Mail-Adresse gehört. Es werden diejenigen Zweige des LDAP-Systems gesucht, die in der Einstellung `personSearchDNList` (siehe *3.2.7 LDAP-Verzeichniszweige mit Benutzern: personSearchDNList*) aufgelistet sind. Die Suche wird eingeschränkt auf den Filterausdruck `searchFilterForMail` (siehe *3.2.17 Suchfilter für E-Mail-Adressen: searchFilterForMail*). Dem Filterausdruck wird als Parameter die E-Mail-Adresse übergeben.

Anschließend erfolgt eine Anmeldung mit userPrincipalName am LDAP-Server. Bei erfolgreicher Anmeldung wird wie in Abschnitt *2.1.2 Benutzerattribute zuweisen* verfahren.

3 Konfiguration

Beachten Sie:

- Für alle Einstellungen ist die Groß-/Kleinschreibung zu beachten.
- Die Optionsnamen sind in Anführungszeichen zu setzen.
- Optionswerte true/false und Zahlen werden ohne Anführungszeichen angegeben. Optionswerte mit Zeichenketten erfordern Anführungszeichen.
- Optionsname und -wert werden durch Doppelpunkt getrennt.
- Am Ende der Zeile steht ein Komma, außer bei der letzten Zeile eines Blocks.
- Kommentare sind nicht möglich.
- Die Optionen `"changedMembers"` sind zu ignorieren.

3.1 Globale Einstellungen

3.1.1 Neue Benutzer automatisch erstellen: createNewUser

Wenn diese Option eingeschaltet ist, wird ein Benutzer nach der Anmeldung automatisch im ELO angelegt, sofern er noch nicht existiert. Siehe auch `parentOfNewUser` (*3.2.19 Attributname für den Administrator eines Benutzers: parentOfNewUser*).

Beispiel:

```
  "createNewUser": true,
```

Information: Die erstmalige Anmeldung eines neuen Benutzers muss mit UserPrincipalName, sAMAccountName oder der E-Mail-Adresse erfolgen.

3.1.2 Gruppenabgleich: assignGroups

Nach erfolgreicher Anmeldung können dem Benutzer in ELO die Gruppen zugewiesen werden, die er im LDAP-System hat.

Beispiel:

```
  "assignGroups": true,
```



Information: Es werden nur die Gruppen zugewiesen, die im LDAP-System und im ELO dieselben Namen haben.

3.1.3 Benutzer nicht über LDAP authentifizieren: notResponsibleForUserOrGroupIds

Diejenigen Benutzer, die es nur in ELO aber nicht im LDAP-System gibt, kann man mit dieser Option von der LDAP-Anmeldung ausnehmen. Die Option besteht aus einer Liste von Benutzer-IDs oder -GUIDs in Anführungszeichen. Daneben sind auch Gruppen-IDs und -GUIDs erlaubt, womit angezeigt wird, dass alle Gruppenmitglieder nicht über LDAP, sondern über ELO authentifiziert werden sollen.

Beispiel, Administrator und ELO Service nicht über LDAP authentifizieren:

```
  "notResponsibleForUserOrGroupIds": [
    "0",
    "(E10E1000-E100-E100-E100-E10E10E10E42)"
  ],
```

3.2 Einstellungen je Domäne

Die ELO Benutzer können in verschiedenen Domänen liegen. Für jede Domäne ist ein Satz der hier vorgestellten Einstellungen anzugeben. Die Domänen-Definitionen sind in dem Array `domains` aufzuführen.

Beispiel:

```
  "domains": [
    {
    … first domain
    },
    {
    … second domain
    }
  ],
  …
```

3.2.1 LDAP-Server

Eine Domäne kann zur Lastverteilung über mehrere LDAP-Server angesprochen werden. Die Definitionen der Server-Eigenschaften ist im Array `servers` anzugeben.

Mit `ldapUrl` wird die Verbindung zum LDAP-Server über TCP bestimmt. Das Element `priority` gibt an, zu welcher Wahrscheinlichkeit dieser Servereintrag verwendet werden soll.

Beispiel:

```
  "domains": [
    {
      "servers": [
        {
          "ldapUrl": "ldap://srvp04vm.elo.local:389",
          "priority": 0.3333333333333333,
        },
        {
          "ldapUrl": "ldap://srvp03.elo.local:389",
          "priority": 0.3333333333333333,
        },
        {
          "ldapUrl": "ldap://srvp05vm.elo.local:389",
          "priority": 0.3333333333333333,
        }
      ],
```

3.2.2 LDAP-ELO-Benutzerzuordnung: attributeForUserPropOS

Für jede Domäne muss festgelegt werden, ob zum ELO Benutzer in der Eigenschaft Windows-Benutzer der userPrincipalName oder sAMAccountName gespeichert wird.

Ist sAMAccountName gewählt und ein Domänenpräfix `domainPrefix` (siehe *3.2.3 Domänenpräfix: domainPrefix*) definiert, enthält der Windows-Benutzer den Account-Namen mit vorangestelltem Domänenpräfix.

Beispiel mit sAMAccountName = fritzfrei und

```
ldap.json:
{
  …
  attributeForUserPropOS = "sAMAccountName",
  domainPrefix="ELO\\",
  …
}

-> Windows-Benutzer = "ELO\\fritzfrei"
```

Information: Für die Einstellung `attributeForUserPropOS` sind aktuell nur die Werte sAMAccountName und userPrincipalName erlaubt. Achten Sie auf korrekte Groß-/Kleinschreibung.

> **Information:** Wenn die Einstellung auf userPrincipalName geändert wird, muss auch `searchFilterForPerson` (*3.2.16 Suchfilter für Benutzer: searchFilterForPerson*) angepasst werden.

3.2.3 Domänenpräfix: domainPrefix

Das Domänenpräfix ist erforderlich, wenn mehrere Domänen konfiguriert werden und zum ELO Benutzer der sAMAccountName als Windows-Benutzer geführt wird (siehe Einstellung `attributeForUserPropOS` *3.2.2 LDAP-ELO-Benutzerzuordnung: attributeForUserPropOS*).

Das Domänenpräfix muss mit einem **Trennzeichen** abgeschlossen werden. Dadurch wird das Präfix vom Benutzernamen separiert. Es sollte vorzugsweise ein Backslash verwendet werden. Weil jedoch der Backslash eine besondere Bedeutung im JSON-Format hat, muss er hier verdoppelt werden. Beispiel:

```
"domainPrefix": "ELO\\",
```

Wenn SSO genutzt werden soll, muss das Domänenpräfix mit dem „kurzen“ (NetBIOS) Domänennamen übereinstimmen (siehe *2.2 SSO-Anmeldung*).

> **Information:** Das für SSO passende Domänenpräfix finden Sie (auf dem Client-Computer) in der Umgebungsvariablen *USERDOMAIN*.

> **Hinweis:** Für SSO mit Domänenpräfix muss in der Datei *config.xml* des ELO Indexservers die Option `"ntlm.domainUserFormat"` gesetzt werden (siehe *2.2.1 SSO mit Domänenname*).

3.2.4 Domänenname: name

Geben Sie in dieser Option den DNS-Namen der Domäne an. Die Einstellung wird verwendet, wenn aus dem sAMAccountName der userPrincipalName gebildet wird.

Beispiel:

```
"name": "ELO.LOCAL",
```

> **Information:** Den DNS-Namen finden Sie in der Umgebungsvariablen *USERDNSDOMAIN*.

3.2.5 ELO Benutzername bilden: nameFormatter

Aus verschiedenen LDAP-Attributen des Benutzers kann der Benutzername für ELO zusammengestellt werden. Hierfür kann ein Formatausdruck mit Platzhaltern angegeben werden. Die Platzhalter sind in $-Zeichen eingerahmt und entsprechen den LDAP-Attributnamen.

Beispiel, Anzeigename aus LDAP als ELO Benutzername

```
"nameFormatter": "$CN$",
```

3.2.6 Technisches Konto, defaultUserName, defaultUserPasswordEncr

Für SSO wird ein technisches Konto benötigt, unter dessen Anmeldung der vom SSO-Mechanismus übergebene Benutzername (i.d.R. sAMAccountName) im LDAP gesucht werden kann. Ferner muss das Konto ausreichende Berechtigungen haben, um die Benutzerattribute und Gruppenzugehörigkeiten zu lesen.

Das Konto wird allein für die Authentifizierung gegen den LDAP-Server verwendet. Es hat keine Beziehung zur ELO Benutzerverwaltung, muss also kein ELO Benutzerkonto sein.

Als `defaultUserName` muss ein userPrincipalName angegeben werden.

In `defaultUserPasswordEncr` kann ein unverschlüsseltes Kennwort eingetragen werden, das der ELO Indexserver beim Neustart verschlüsselt zurückspeichert.

Beispiel:

```
"defaultUserName": "fritzfrei@elo.local",
"defaultUserPasswordEncr": "…",
```

3.2.7 LDAP-Verzeichniszweige mit Benutzern: personSearchDNList

In dieser Liste wird festgelegt, in welchen Zweigen des LDAP-Verzeichnisses nach Benutzern gesucht wird. Die Liste darf nicht leer sein.

Beispiel:

```
"personSearchDNList": [
    "OU=Hamburg,DC=diefirma,DC=de",
    "OU=Stuttgart,DC=diefirma,DC=de"
],
```

3.2.8 LDAP-Verzeichniszweige mit Gruppen: groupSearchDNList

In dieser Liste wird festgelegt, in welchen Zweigen des LDAP-Verzeichnisses die Gruppen liegen müssen, die für den Gruppenabgleich in Frage kommen. Ist die Liste leer, gehen alle Gruppen des Benutzers in den Gruppenabgleich ein.

Beispiel:

```
"groupSearchDNList": [
    "DC=ELO,DC=LOCAL"
],
```

3.2.9 Erforderliche Mitgliedschaft: requiredGroup

Mit dieser Einstellung kann die Anmeldung auf solche Anwender beschränkt werden, die Mitglied einer bestimmten Gruppe im LDAP-Verzeichnis sind. Die Angabe ist als Common Name vorzunehmen.

Beispiel:

```
"requiredGroup": "Composers"
```

3.2.10 Verbindungs-Timeout: connectionTimeoutSeconds

Die LDAP-Schnittstelle bricht nach dieser Anzahl von Sekunden einen Verbindungsaufbau zum LDAP-Server ab. Anschließend wird der nächste Server in der Liste probiert (siehe *3.2.1 LDAP-Server*).

```
"connectionTimeoutSeconds": 10,
```

3.2.11 Such-Timeout: searchTimeLimitSeconds

Bei einer Suche nach Benutzern oder Gruppen wird dieser Timeout-Wert an den LDAP-Server übergeben.

```
"searchTimeLimitSeconds": 10,
```

3.2.12 Tiefe der rekursiven Gruppensuche: maxGroupNesting

Beim Sammeln von Benutzergruppen für den Gruppenabgleich kann hiermit die Tiefe der Gruppe-In-Gruppe-Beziehungen angegeben werden. Der Wert 0 bedeutet dabei, dass unbegrenzt tiefe Verschachtelungen ausgewertet werden.

```
"maxGroupNesting": 0,
```

3.2.13 Attributname der Gruppenmitgliedschaften: attributeNameMemberOf

Mit dieser Einstellung wird bestimmt, welches LDAP-Attribut die Mitgliedschaften in Gruppen enthält.

```
"attributeNameMemberOf": "memberOf",
```

3.2.14 Attributname der Mailadresse: attributeNameMail

Die E-Mail-Adresse des Benutzers speichert das LDAP-Verzeichnis in dieser Eigenschaft.

```
"attributeNameMail": "mail",
```

3.2.15 Suchfilter für Gruppen eines Benutzers: searchFilterForGroups

Die Suche nach den Gruppen eines Benutzers kann mit diesem Filter eingegrenzt werden. Für den Platzhalter „{0}“ wird der DN (Distinguished Name) des Benutzers übergeben.

```
"searchFilterForGroups": "(&(objectCategory=group)(member={0}))",
```

3.2.16 Suchfilter für Benutzer: searchFilterForPerson

Die Suche nach Benutzern kann mit diesem Filter eingegrenzt werden. Für den Platzhalter „{0}“ wird der Windows-Benutzer (attributeForUserPropOS, siehe *3.2.2 LDAP-ELO-Benutzerzuordnung: attributeForUserPropOS*) übergeben.

```
"searchFilterForPerson": "(&(objectclass=person)(sAMAccountName={0}))",
```

3.2.17 Suchfilter für E-Mail-Adressen: searchFilterForMail

Bei einer ersten Anmeldung mit E-Mail-Adresse wird der Benutzer über diesen Filter im LDAP-Verzeichnis gesucht. Für den „{0}“ wird die E-Mail-Adresse übergeben.

```
"searchFilterForMail": "(&(objectclass=person)(mail={0}))",
```

3.2.18 Attribute, die in ELO gespeichert werden sollen: attributesToRead

Diese Benutzer-Attribute werden nach erfolgreicher Anmeldung in die ELO Datenbank übertragen. Über die API des ELO Indexservers können sie im Element `UserInfo.ldapProperties` ausgelesen werden.

```
"attributesToRead": [
        "manager",
        "cn",
        "objectguid",
        …
        "useraccountcontrol"
      ],
```



Information: Aus dem Attribut *manager* wird der Vorgesetzte des ELO Benutzers ermittelt. Der Vorgesetzte muss bereits im ELO bekannt sein.

3.2.19 Attributname für den Administrator eines Benutzers: parentOfNewUser

Für Benutzer, die über die LDAP-Schnittstelle erstellt werden, kann hier festgelegt werden, welcher ELO Benutzer als Administrator zugewiesen wird. Die Angabe kann als ID, GUID oder Benutzername erfolgen.

```
" parentOfNewUser": "Fritz Frei",
```



Information: Diese Option gilt ab ELO12.

3.2.20 LDAP-Verbindungsoptionen: initialContextEnvironment

Mit diesen Optionen kann der Aufbau der Verbindung zum LDAP-Server gesteuert werden.

```
"initialContextEnvironment": {
  "java.naming.factory.initial": "com.sun.jndi.ldap.LdapCtxFactory",
  "java.naming.ldap.attributes.binary": "objectGUID …",
  "com.sun.jndi.ldap.connect.pool": "true",
  "java.naming.security.authentication": "simple"
},
```

4 Skripting

Auf einzelne Schritte der Anmeldung kann per Skripting Einfluss genommen werden. Hierzu wird ein Objekt, das die Schnittstelle `de.elo.ix.client.ldap.LdapUserDirectoryHandler` implementiert, in das LDAP-Plugin eingehängt. In der API-Dokumentation des ELO Indexservers sind die Methoden der Schnittstelle beschrieben.

Beispiel:

```
var interfaceName = "de.elo.ix.client.plugin.UserDirectory";
var UserInfoC = Packages.de.elo.ix.client.UserInfoC;

function init() {
 // Get LDAP service
 var ldapService = ixPlugins.getService(interfaceName);

 // Create a factory object derived from Ldap…HandlerFactory
 var factory = new JavaAdapter(
  Packages.de.elo.ix.client.ldap.LdapUserDirectoryHandlerFactory, {

   // Called from LDAP service to get a callback handler
   createHandler : function(defaultHandler,
        config, userName, password, runAsName) {

     // Create a callback handler
     var adapter = new JavaAdapter(
     Packages.de.elo.ix.client.ldap.LdapUserDirectoryHandlerWrapper, {

      // Mandatory: return the default handler supplied in the constructor
      getInnerHandler : function() {
       return defaultHandler;
      },

      // Optional: e.g. assign additional properties after authenticated
      assignUserName : function(ui, domain, userName, attributes) {
        defaultHandler.assignUserName(ui, domain, userName, attributes);
        ui.userProps[UserInfoC.PROP_ACTION] = "hello ldap";
      }
    });
    return adapter;
   }
 });

 ldapService.setHandlerFactory(factory);
}

init();
```