Abschlussprüfung Sommer 2015

Fachinformatiker – Systemintegration

Dokumentation zur betrieblichen Projektarbeit

OpenLDAP- und FreeRADIUS-Server

Kundendokumentation für Administratoren

Abgabetermin: Kaiserslautern, den 18. Mai 2015

Prüfungsbewerber:
Sebastian Deußer
Feuerbachstraße 15
67659 Kaiserslautern

Ausbildungsbetrieb:
taylorix institut für berufliche Bildung e.V.
Lutrinastraße 4
67655 Kaiserslautern

Praktikumsbetrieb:
fgn GmbH
Trippstadter Straße 122
67663 Kaiserslautern

1 Kundendokumentation für Administratoren

1.1 Wichtige Details

- Server `id.fg-networking.de`
- verwendet LDAP-over-SSL (Port 636), LDAP Standardport nur für Loopback aktiviert (zu ändern in /etc/default/slapd)
- Purge des slapd Pakets löscht nicht die LDAP Datenbank (Konfiguration dieses Verhaltens über das Debian Paketkonfigurationsskript)

1.2 Nützliche Links

- https://wiki.debian.org/LDAP/OpenLDAPSetup
- https://wiki.debian.org/FreeRadiusToLdap (zu RADIUS+LDAP, etwas angestaubt sogar für Debian Verhältnisse)
- http://www.postfix.org/LDAP_README.html (Postfix+LDAP Doku)
- http://www.zytrax.com/books/ldap/ch11/multi-dit.html (Beispiel für mehrere Domains in einem LDAP)
- http://httpd.apache.org/docs/2.4/mod/mod_authnz_ldap.html (Apache Doku zum LDAP Auth Modul)

1.3 Ändern des Passworts eines LDAP-Users

Um das Passwort eine Users im LDAP Verzeichnis zu ändern bietet sich für die Kommandozeile `ldappasswd` an. Dazu sollten die LDAP-Utils auf dem jeweiligen Rechner richtig konfiguriert sein (siehe in Einrichten von LDAPS (LDAP-over-SSL) den unteren Teil zur `/etc/ldap/ldap.conf`).

```
ldappasswd -S -W -D "cn=admin,dc=de" -x "uid=username,ou=people
    ,dc=fg-networking,dc=de"
```

Dieser Befehl fragt auf der Kommandozeile das neue Passwort für den Account `username` ab (mit Wiederholung) und fragt wenn beide Passwörte übereinstimmen nach dem Passwort des LDAP-Administrators. Mit den Daten meldet es sich dann am LDAP-Server an und speichert das Passwort dann gehashed in der LDAP Datenbank. Username muss natürlich durch den richtigen Namen ersetzt werden und eventuell die erste dc angepasst werden.

1.4 Erklärung der OpenLDAP Log-Level

Level	Keyword	Description
-1	any	enable all debugging
0		no debugging
1	(0x1 trace)	trace function calls
2	(0x2 packets)	debug packet handling
4	(0x4 args)	heavy trace debugging
8	(0x8 conns)	connection management
16	(0x10 BER)	print out packets sent and received
32	(0x20 filter)	search filter processing
64	(0x40 config)	configuration processing
128	(0x80 ACL)	access control list processing
256	(0x100 stats)	stats log connections/operations/results
512	(0x200 stats2)	stats log entries sent
1024	(0x400 shell)	print communication with shell backends
2048	(0x800 parse)	print entry parsing debugging
16384	(0x4000 sync)	syncrepl consumer processing
32768	(0x8000 none)	only messages that get logged whatever log level is set

Um Log-Level einzustellen kann man entweder die entsprechende Zahl aus der ersten Spalte, den Hex-Wert oder das Schlüsselwort aus Spalte 2 verwenden. Werden die Zahlen aus Spalte 1 verwendet kann man mehrere Log-Level gleichzeitig auswählen indem man ihre Wert miteinander addiert.

Zum debuggen der Probleme die bei der Durchführung des Projekts auftraten erwiesen sich die meisten der Zusatzausgaben als ungeeignet, lediglich die Traces der Level 1 (0x1 trace) und 4 (0x4 args) konnten weiterhelfen, enthielten aber auch keine weiterführenden Informationen bei Problemen mit dem Zugriff auf die Verzeichnis-Datenbank.

Wenn wie in diesem Projekt ein OpenLDAP-Server mit einem `slapd.d`-Konfigurationsordner statt einer `slapd.conf`-Konfigurationsdatei verwendet wird, muss man, wie sämtliche anderen Einstellungen auch, den Log-Level über eine vorbereitete Datei und `ldapmodify` verändern. Eine entsprechende Datei sieht wie folgt aus:

```
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: 5
```

Diese Datei würde den Log-Level auf 5 setzen. Der entsprechende `ldapmodify`-Aufruf ist dann:

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f olcLogLevel.ldif
```

1.5 Ausgeben des Inhalts der LDAP-Datenbank

Mit dem Kommandozeilenprogramm `ldapsearch` kann man nach Einträgen in der LDAP Datenbank suchen. Man kann sich damit auch den gesamten Inhalt der Datenbank anzeigen lassen. Dies geht am einfachsten mit

```
ldapsearch -x -LLL -H ldaps://id.fg-networking.de -b dc=de
```

Erklärung der Parameter: -x stellt auf einfache Authentifizierung um (im Gegensatz zu SASL), -LLL gibt die Daten im LDIF Format aus, ohne Kommentare und ohne Anzeige der Versionsnummer, mit -H wird die URI des LDAP Servers übergeben und -b gibt den Startpunkt im Datenbankbaum für die Suche an.

1.6 Hinzufügen eigener Konfiguration und Schema zum OpenLDAP-Server

Neuer Versionen von OpenLDAP benutzen nicht mehr die slapd.conf, sondern ein Konfigurationsverzeichnis slapd.d mit eigener Datenstruktur. Um neue Konfigurationen hinzuzufügen legt man eine LDIF-Datei mit der Konfiguration an und importiert diese mit

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f <file.ldif>
```

Um ein neues Schema einzufügen kopiert man das .schema File nach `/etc/ldap/schema`. Dann erstellt man sich eine temporäre Konfig-Datei (hier als Beispiel `/tmp/schema.conf`) mit folgendem Inhalt

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/mypersonalschema.schema
```

mypersonalschema.schema sei hier das neue Schema. Nun erstellt man sich ein temporäres Verzeichnis (hier `/tmp/ldif_output`) und ruft folgendes auf

```
slaptest -f /tmp/schema.conf -F /tmp/ldif_output
```

Nun editiert man das generierte File z.B. mit

```
vim "/tmp/ldif_output/cn=config/cn=schema/cn={4}
    mypersonalschema.ldif"
```

Hier ändert man dann die ersten drei Zeilen wie folgt

```
dn: cn=mypersonalschema,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: mypersonalschema
```

Am Ende der Datei löscht man dann noch die Zeilen mit folgenden Anfängen

```
structuralObjectClass:
entryUUID:
creatorsName:
createTimestamp:
entryCSN:
modifiersName:
modifyTimestamp:
```

Nun kann man das Ganze in die Systemkonfiguration importieren

```
ldapadd -Y EXTERNAL -H ldapi:/// -f "/tmp/ldif_output/cn=config
    /cn=schema/cn={4}mypersonalschema.ldif"
```

Bei erfolgreichen Import findet sich das Schema nun in `/etc/ldap/slapd.d/cn=config/cn=schema/cn={4}mypersonalschema.ldif`

1.7 Einrichten von LDAPS (LDAP-over-SSL)

Zuerst muss man Zertifikat und privaten Schlüssel für das LDAP erzeugen (siehe FGN-CA im Wiki) und diese zusammen mit dem Zertifikat der CA auf den LDAP-Server ablegen (vorzugsweise in `/etc/ssl/certs` bzw. `/etc/ssl/private`). Damit der LDAP-Server die auch verwendet erstellt man eine entsprechende LDIF Datei (hier `olcSSL.ldif`).

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ssl/certs/fg-networking.de_ca.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ssl/private/id.fg-networking.de-
    key-2015-05-05.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ssl/certs/id.fg-networking.de-crt
    -2015-05-05.pem
```

die man dann in die Konfig importiert mit

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f olcSSL.ldif
```

Nun muss man noch den `SLAPD_SERVICES` Eintrag in `/etc/default/slapd` anpassen damit LDAP auf SSL Verbindungen lauscht.

```
SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
```

(für localhost kann man weiterhin den Standard LDAP (ohne SLL) Port 389 verwenden, LDAPS lauscht standardmäßig auf Port 636). Nach einem Neustart von slapd ist LDAP-over-SSL nun verwendbar.

Auf den Clients muss dann das FGN CA Zertifikat an passende Stelle gelegt werden und folgende Zeile in `/etc/ldap/ldap.conf` eingetragen werden.

```
TLS_CACERT    /etc/ssl/certs/fg-networking.de_ca.pem
```

Fehlt die kann der Client nicht das LDAP Server Zertifikat verifizieren und bricht bei Debian Standardeinstellungen die Verbindung ab. Außerdem muss man in dieselbe Datei noch die neue LDAP Server URI eintragen, z.B.

```
URI ldaps://id.fg-networking.de
BASE dc=fg-networking,dc=de
```

Hier sollte man unter `BASE` auch die LDAP Standard Searchbase angeben, die sinnvollsten Werte dürften hier `dc=fg-networking,dc=de` und `dc=de` sein.

1.8 Änderungen an der Apache Konfiguration

Zur Anbindung von LDAP an einen Apache Web-Server wird die `mod_authnz_ldap` verwendet. In der Konfig-Datei `/etc/apache2/mods-available/ldap.conf` muss auch wieder das CA Zertifikat eingetragen werden um LDAPS verwenden zu können. Dazu trägt man (außerhalb jeglichen `<Location>` Kontexts) ein:

```
LDAPTrustedGlobalCert CA_BASE64 /etc/ssl/certs/fg-networking.de
    .pem
```

(In dieser Datei war bereits auch schon der ldap-status handler definiert, an dieser Einstellung muss nichts verändert werden). In der passenden Seitenkonfig (auf NMS: `/etc/apache2/sites-available/default-ssl`) muss man dann noch die URL vom LDAP Server anpassen. Auf NMS sieht die neue Konfig wie folgt aus:

```
<Location />
    AuthType  Basic
    AuthName  "FGN NMS"
    AuthzLDAPAuthoritative  off
    AuthBasicProvider ldap
    AuthLDAPURL ldaps://id.fg-networking.de:636/dc=fg-
   networking,dc=de?uid?sub?
    require valid-user
    Satisfy any
 </Location>
```

1.9 Konfiguration des FreeRADIUS-Servers

Zuerst einmal zusätzlich das Paket `freeradius-ldap` installieren (bei Debian sind zwar schon Beispielkonfigs für LDAP mitgeliefert, aber die tatsächlichen Module sind erst in diesem Paket enthalten). In `/etc/freeradius/clients.conf` muss unter `secret` das zu den Uni Mailservern passende Shared Secret eingetragen werden (dies wurde aus der Konfiguration von CommuniGate ausgelesen). Wenn noch Clients an den RADIUS angebunden werden sollen muss unten für die passenden IPs ein Shared Secret vergeben werden das dann auch im Client eingetragen werden muss.

Um LDAP als Authentifizierungsmethode für User zu aktivieren muss in `/etc/freeradius/users` folgende Zeile eingetragen werden:

```
DEFAULT Auth-Type := LDAP
```

Hier ist zu beachten das **EAP nicht mehr funktioniert**. Soll EAP irgendwann benutzt werden sollen muss hier eine andere Möglichkeit gefunden werden (die Dokumentation schlägt eine ähnliche Eintragung für jeden Benutzer einzeln vor).

In `/etc/freeradius/modules/ldap` muss unter `server` der richtige LDAP Server (`id.fg-networking.de`) und unter `basedn` die richtige Searchbase angegeben werden (hier `dc=fg-networking,dc=de`, **muss evtl. noch angepasst werden**)

In `/etc/freeradius/sites-enabled/default` müssen alle Zeilen die `ldap` einkommentiert werden. Einzige Ausnahme bildet die Zeile bei der in den Kommentaren davor erwähnt das sie nur benötigt wird wenn `edir_account_policy_check = yes` eingestellt wurde (Zeile 488 in der aktuellen Datei).

Zum Testen des Ganzen wurde `radtest` aus dem Paket `freeradius-utils` verwendet. Der Aufruf war:

```
radtest <username> <passwort> id.fg-networking.de:1812 10
        <shared-secret>
```

Die Werte in spitzen Klammern müssen natürlich durch die entsprechenden Werte ersetzt werden (ohne die spitzen Klammern).

1.10 Erläuterungen zu den verwendeten LDAP Schemas

0. `core` – Enthält LDAP Core Attribute (X.501), wird immer benötigt
1. `cosine` – Enthält die LDAPv3 Attribute (Cosine and Internet X.500 (RFC1274))
2. `nis` – Schema zur Verwendung von NIS, bei uns vermutlich nicht benötigt aber Teil der Linux/Unix Standardinstallationen
3. `inetorgperson` – Schema für die gängigen Personenattribute und andere Attribute für organisationsorientierte Dienste
4. `freeradius` – Schema für RADIUS Atrribute, aus der FreeRADIUS Doku (`/usr/share/doc/freeradius/examples/openldap.schema`)
5. `postfix` – Schema mit zusätzlichen Attributen für postfix address rewrite, von den Autoren des Galileo Press OpenLDAP 2.4 Praxisbuches (in der FGN Bibliothek)

(0-3 sind Teil der Debian Standardkonfig)

1.11 Erstellung der LDAP-Verzeichnisstruktur

Die leere Datenbank wurde mit dem interaktiven Debian config script (aufgerufen mit `dpkg-reconfigure slapd`) erzeugt. Als Domain und Organization Name wurde `de` genommen. Die restlichen Fragen wurden mit den Standardantworten beantwortet. Für die drei Domains wurde dann folgende LDIF-Datei (`add_DNs.ldif`) zum Erzeugen verwendet

```
dn: dc=fg-networking,dc=de
o: fg-networking.de
objectClass: top
objectClass: dcObject
objectClass: organization

dn: dc=schabler,dc=de
o: schabler.de
objectClass: top
objectClass: dcObject
objectClass: organization

dn: dc=worden,dc=de
o: worden.de
```

```
objectClass: top
objectClass: dcObject
objectClass: organization
```

Diese wird (nachdem man den LDAP daemon slapd gestoppt hat) in die Datenbank eingefügt mit

```
slapadd -n 1 -l add_DNs.ldif
```

Der Content wird hier mit `slapadd` eingefügt da dies der einfachste Weg ist um dcObjects in der LDAP Datenbank zu erstellen. Für die meisten anderen Datenmanipulationen ist ldapmodify die sicherere und sauberere Variante. Danach kann man (und muss für den nächsten Schritt auch) `slapd` wieder starten.

Als nächstes wurden die `people` organizationalUnits erzeugt, in die alle User Einträge kommen sollen (da wir vor der Fertigstellung des neuen Mailservers nur echte Anwenderaccounts migrieren (keine Mailinglisten Accounts u.ä.) ist dies auch erstmal die einzige benötigte OU). Zum Erzeugen der OUs wurde wieder eine LDIF Datei (`add_content.ldif`) erstellt.

```
dn: ou=people,dc=fg-networking,dc=de
objectClass: organizationalUnit
ou: people

dn: ou=people,dc=schabler,dc=de
objectClass: organizationalUnit
ou: people

dn: ou=people,dc=worden,dc=de
objectClass: organizationalUnit
ou: people
```

Die wurde dann in die Datenbank eingefügt mit

```
ldapmodify -a -H ldapi:/// -D cn=admin,dc=de -W -f add_content.
    ldif
```

Anschließend kann man die User einfügen. Wir haben dazu nach dem folgenden minimalem Template per Skript aus den Klartextdateien von CommuniGate das LDIF dafür generiert.

```
dn: uid=username,ou=people,dc=fg-networking,dc=de
objectClass: inetOrgPerson
objectClass: person
uid: username
sn: Nachname
givenName: Vorname
cn: Vorname Nachname
displayName: Vorname Nachname
userPassword: password
```

1.12 Änderungen an der OpenVPN Konfiguration

Konfigurationsdateien `/etc/openvpn/tcp.config` und `/etc/openvpn/udp.config`

```
plugin /usr/lib/openvpn/openvpn-auth-ldap.so /etc/openvpn/auth-
    ldap.config
```

Die Einträge sind notwendig damit das LDAP Plugin überhaupt verwendet wird.

Konfigurationsdatei `/etc/openvpn/auth-ldap.config`

```
<LDAP>
        URL             ldaps://id.fg-networking.de:636
        Timeout         15
        TLSEnable       no
        FollowReferrals yes
        TLSCACertFile   /etc/ssl/certs/fg-networking.de_ca.pem
</LDAP>

<Authorization>
        BaseDN          "dc=fg-networking,dc=de"
        SearchFilter    "(&(uid=%u))"
        RequireGroup    false
</Authorization>
```

OpenVPN muss neu gestartet werden, um die geänderte Konfigurationsdatei anzuwenden.

1.13 Konfiguration der Firewall

Der folgende Block zeigt die Ausgabe der Uncomplicated Firewall (`ufw`) über ihre aktuellen Regeln (`ufw` verwendet als Standardregel, die als letzte angewendet wird wenn keine andere Regel zutrifft, ein implizites `* DENY ALL` das nicht angezeigt wird):

```
root@id:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
636                        ALLOW       131.246.197.0/25
636                        ALLOW       10.122.0.0/16
1812                       ALLOW       131.246.197.0/25
1813                       ALLOW       131.246.197.0/25
1812                       ALLOW       10.122.0.0/16
1813                       ALLOW       10.122.0.0/16
1812                       ALLOW       131.246.120.208/28
1812                       ALLOW       131.246.5.14
22                         ALLOW       Anywhere (v6)
```

- SSH (Port 22) ist wie bei Servern bei fgn üblich von sämtlichen Quellrechnern erlaubt (IPv4 und IPv6)

- LDAPS (Port 636) ist aus dem fgn-Subnetz (131.246.197.0/25) und dem privaten fgn-Infrastruktur-Netz (10.122.0.0/16)
- RADIUS (Port 1812 ist der generelle Port des FreeRADIUS-Daemons und Port 1813 ist der Port für Accounting) ist zugelassen für Verbindungen aus dem öffentlichen fgn-Subnetz (131.246.197.0/25), dem privaten fgn-Infrastruktur-Netz (10.122.0.0/16), den TU E-Mail-Servern 131.246.120.208/28 und dem RADIUS-Server der TU 131.246.5.14. Der RADIUS-Proxy Port 1814 wurde hier nicht gebraucht weswegen keine Verbindungen zu ihn freigeschaltet wurden.

Die Firewall-Regeln wurden nach Vorbild der Regeln für den CommuniGate Server erstellt.

1.14 Auf den neuen LDAP-Server umgestellte Systeme

- nms Webserver
- aio Webserver
- lab-mm Webserver
- OpenVPN

1.15 Noch nicht umgestellte Systeme

- Egroupware (mangels Passwort und Fachwissen vom System)
- Mailserver

Anmerkung: Eine Kundendokumentation für Anwender war nicht notwendig da sich auf Anwenderseite nach der Umstellung keine sichtbaren Änderungen gibt.