LDAP - ein kleiner Einführungsworkshop

Linux-Infotag Augsburg 2017

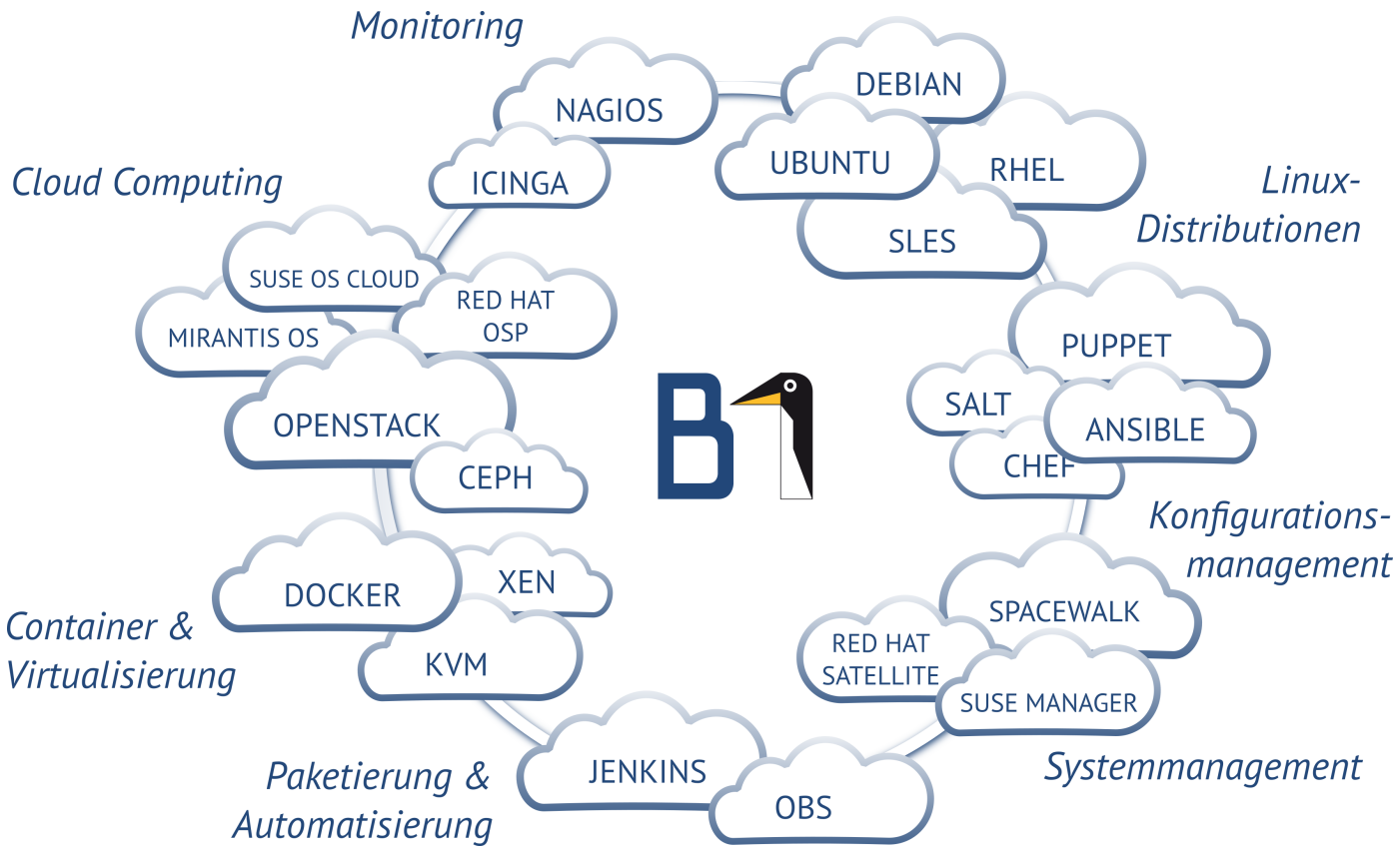
22. April 2017

Michael Wandel
Linux Consultant & Trainer
B1 Systems GmbH
wandel@b1-systems.de

Vorstellung B1 Systems

- gegründet 2004
- primär Linux/Open Source-Themen
- national & international tätig
- ca. 100 Mitarbeiter
- unabhängig von Soft- und Hardware-Herstellern
- Leistungsangebot:
  - Beratung & Consulting
  - Support
  - Entwicklung
  - Training
  - Betrieb
  - Lösungen
- Büros in Rockolding, Köln, Berlin & Dresden

Schwerpunkte



Agenda Workshop

- Willkommen
- LDAP-Grundlagen
- Beispiel LDAP Baum
- Linux Systemanbindung
- Applikationsanbindung
- Erweiterungen

LDAP Grundlagen

- LDAP als Prokoll
- Begriffe im LDAPversum
- LDAP - Objekte
- Beispiele für Objektklassen und Attribute
- LDIF zum Datenaustausch
- LDAP Implementierungen

Beispiel LDAP Baum

- Installation
- Konfiguration
- Werkzeugen im LDAP Umfeld
- Schema und Erweiterungen
- SSL / TLS Einrichtung

LDAP Elemente

- Beispiel einer LDAP Struktur
  - LDAP Objekte und Attribute
  - LDAP Schema für Posix User/Gruppen
  - LDAP Gruppen
  - LDAP Schemaerweiterungen für Applikationen

Nutzung des LDAP Baumes

- LDAP Baum nutzen
  - Systemanbindung mittels SSSD
  - Apache Anbindung
  - Postfix Anbindung
    - Postmap Informationen
    - SASL Authentikation
  - Adressbuch

Agenda Part 5

- LDAP Erweiterungen / Overlays
  - syncprov
  - auditlog
  - unique
  - memberof
  - refint
  - accesslog
  - ppolicy
  - ...

LDAP als Protokoll

- 1993 LDAP Definition RFC 1487
- LDAP v3 Erweiterung RFC 2251
- aktuelles LDAP Hauptdokument RFC 4510
- über 90 RFCs, teilweise auch Ersetzungen

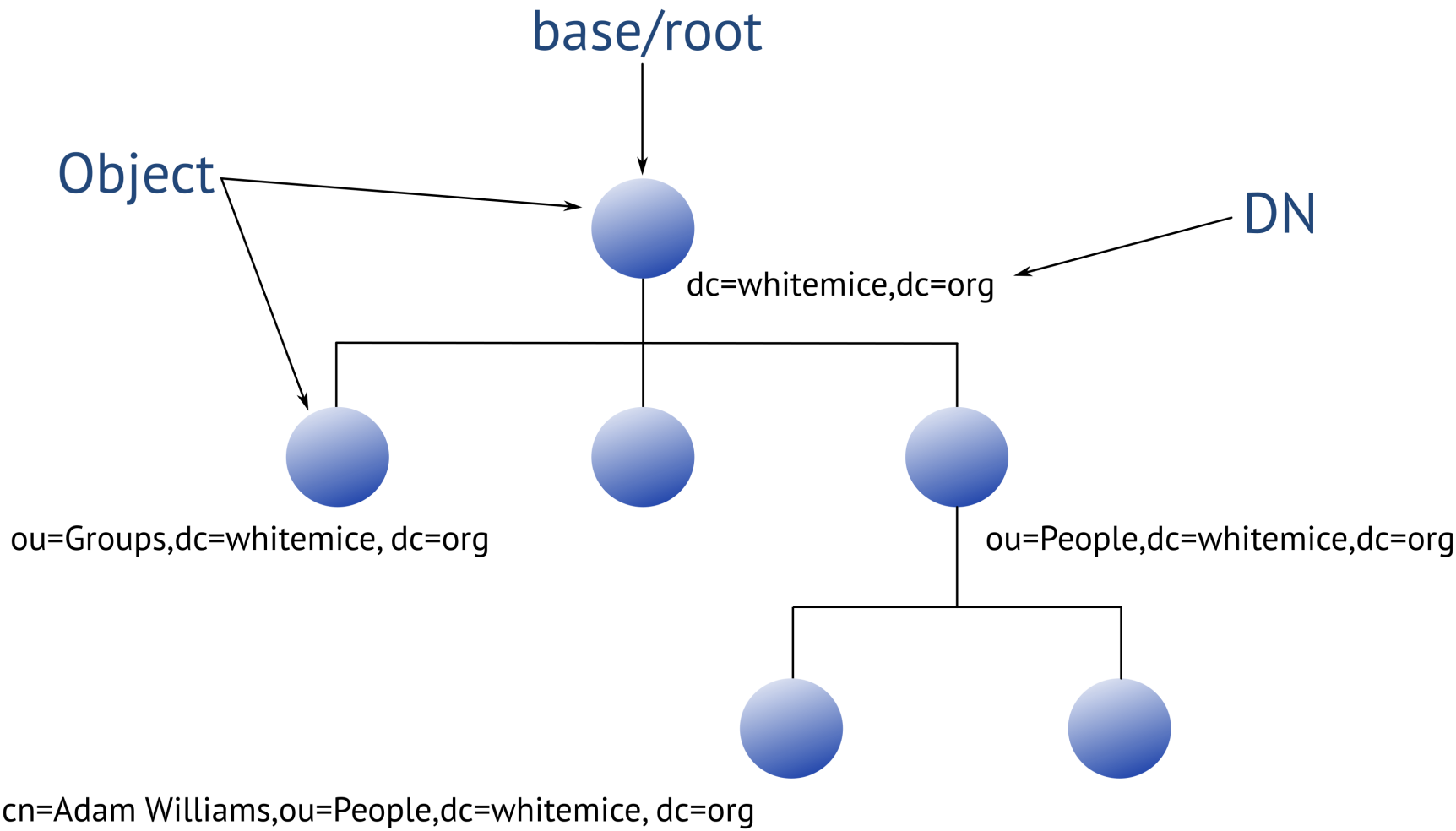
siehe auch:
`https://www.ldap.com/ldap-specifications-defined-in-rfcs`

Protokoll Elemente

- Bind
- Search
- Compare
- Add
- Delete
- Modify
- ModifyDN
- Unbind

- Abandon
- Extended
- StartTLS

Begriffe im LDAPversum



LDAP Objekte

- hierarchische Struktur
- Root-Objekt (Base,Suffix)
- jedes Objekt besitzt eindeutigen DN
- strukturelle Objektklassen (structural)
- Erweiterungen durch Hilfsklassen (auxiliary)
- Attribute (Must oder May)
- LDIF Format für LDAP Import/Export

Beispiele:Objektklassen und Attribute

Objektklassen

- organization
- organizationalUnit
- person
- organizationalPerson
- inetorgPerson
- account
- groupOfNames
- groupOfuniqueNames
- posixAccount
- posixGroup

Attribute

- cn, commonName
- o, organizationName
- ou, organizationalUnitName
- sn, surName
- gn, givenName
- description
- l, localityName
- uid, userid
- userPassword
- jpegPhoto

Schemabeispiel :Objektklassen und Attribute

Definition Objektklasse: account

```
objectclass ( 0.9.2342.19200300.100.4.5 NAME 'account'
        SUP top STRUCTURAL
        MUST userid
        MAY ( description $ seeAlso $ localityName $
                organizationName $ organizationalUnitName $ host )
        )
```

Definition Attribut: host

```
attributetype ( 0.9.2342.19200300.100.1.9 NAME 'host'
        DESC 'RFC1274: host computer'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{256} )
```

Beispiel für LDIF LDAP Objekt

Basis Objekt im LDIF-Format

```
dn: dc=example,dc=com
objectclass: top
objectclass: organization
objectclass: dcobject
dc: example
o: LDAP Workshop
```

LDAP Implenentierungen

- OpenLDAP
- 389 Directory Server
- Microsoft Active Directory
- Samba 4 mit AD Unterstützung
- Oracle Internet Directory
- Apache Directory Server / OpenDJ
- Tivoli Directory Server
- ldapjs
- ...

Beispiel LDAP Baum

- Installation
- Konfiguration `slapd.conf` versus `slapd.d`
- Backup und Restore
- Werkzeuge im LDAP-Umfeld
- Schemaerweiterungen
- SSL/TLS-Einrichtung
- Praktische Übungen

Installation LDAP Server und Client

LDAP Server

```
yum install openldap-servers
```

LDAP Clients

```
yum install openldap-clients
```

alternative Repo Quelle: `https://ltb-project.org/`

Konfigurationsumfeld

- OpenLDAP Server
  - Konfigurationsverzeichnis
    `/etc/openldapd/slapd.d`
  - Konfigurationsdatei (veraltet)
    `/etc/openldap/slapd.conf`
- OpenLDAP Clients
  - Konfigurationsdatei LDAP Client
    `/etc/openldap/ldap.conf`

Backup, Restore & more

Backup

```
slapcat -b dc=example,dc=com > ldap-$(date +%F-%T).ldif

slapcat -b cn=config > ldap-config-$(date +%F-%T).ldif
```

Backup kann auch im laufenden Betrieb gemacht werden

Restore

```
service slapd stop
rm -rf /var/lib/ldap/*
slapadd < ldap.ldif
chown -R ldap:ldap /var/lib/ldap
service slapd start
```

Restore bei gestopptem Service

Beispiel LDAP Baum

Dateiverzeichnis `slapd.d`

```
cn=config
    cn=schema
        cn={0}core.ldif
    cn=schema.ldif
    olcDatabase={0}config.ldif
    olcDatabase={-1}frontend.ldif
    olcDatabase={1}monitor.ldif
    olcDatabase={2}hdb.ldif
cn=config.ldif
```

LDAP slap-Tools serverseitig

- slapadd
- slapcat
- slappasswd
- slapacl
- slapindex
- slaptest
- ...

Passwordhash erzeugen

```
slappasswd -h {SSHA} -s geheim
```

LDAP Client Tools

- ldapadd
- ldapsearch
- ldapdelete
- ldapmodify
- ldapmodrdn
- ldapwhoami
- ldapurl
- ...

LDAP Objekt löschen

```
ldapdelete -x -W -D cn=admin,dc=example,dc=com \
     uid=heinz,ou=users,dc=example,dc=com
```

Das Beispiel setzt eine konfigurierte `/etc/openldap/ldap.conf` voraus.

Schemaerweiterungen

- LDAP Standardschema -> core
- Schemaerweiterungen
  - cosine
  - inetorgperson
  - nis (alternativ rfc2307bis)
  - ppolicy
  - dyngroup
  - ...

Schema hinzufügen

```
ldapadd -Y EXTERNAL -H ldapi:///  \
     -f /etc/openldap/schema/cosine.schema
```

Praktische Beispiele

Übungen zur Online-Konfiguration

- Online Konfiguration `cn=config`
- Erstellen eines Basisobjektes
- Schema und Moduleerweiterungen
- Hinzufügen von ersten Objekten mittels LDIF Dateien
- Suchen im LDAP Baum
- Passwortänderung eines Benutzers

Browser und Editoren

Überblick aktulle Browser und Editoren

- ldapvi (*)
- shelldap
- Apache Directory Studio (*)
- jxplorer
- phpldapadmin
- LDAP Account Manager (lam)
- FusionDirectory

Praktische Übungen

Freie Workshop Übungen

- Installation und Übungen mit ldapvi
- Einrichtung Apache Direchtory Studio

Aktivierung LDAPS Protokoll

- SSL, da Passwörter im Klartext übertragen werden
- alternativ START_TLS über ldap://
- Defaultzertifikate im moznss Format unter `/etc/openldap/certs`

Datei: `/etc/sysconfig/slapd`

ldaps:// Protokoll-Aktivierung

```
...
SLAPD_URLS=‘‘ldapi:/// ldap:/// ldaps:///’’
...
```

LDAP für Posix Logins nutzen

- LDAP Posix Objekte/Attribute
- NSS, Identität im Linuxsystem
- PAM, Authentifikation und Authorisierung
- verschiedene LDAP Clients

LDAP für Posix Logins nutzen

Beispiele Objekklassen Schema NIS:

User	posixaccount, shadowaccount
Group	posixgroup
Hosts	ipHost
Services	ipService

Beispiel LDIF Posix User

uid=heinz

```
dn: uid=heinz,ou=users,dc=example,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgPerson
objectclass: posixAccount
objectclass: shadowAccount
cn: Heinz Ketchup
gn: Heinz
sn: Ketchup
uid: heinz
uidnumber:6001
gidnumber:5001
homedirectory: /home/heinz
userPassword: ketchup
```

Beispiel LDIF Posix Group

cn=ldapuser

```
dn: cn=ldapuser,ou=groups,dc=example,dc=com
objectclass: top
objectclass: posixgroup
cn: ldapuser
gidnumber: 5001
memberuid: heinz
```

Beispiel LDIF LDAP Gruppe

cn=ldapuser

```
dn: cn=webuser,ou=groups,dc=example,dc=com
objectclass: top
objectclass: groupOfNames
member: uid=elke,ou=users,dc=example,dc=com
```

Linux SSSD Anbindung

Warum SSSD ?

- SSSD unterschiedlichste Anbindung
  ldap, kerberos, ipa, ad, ...
- Caching und Cachekontrolle
- Multi Domänen
- Debugging
- Hohe Flexibilität
- ...

Installation und Konfiguration sssd-ldap 1/2

Installation sssd-ldap

```
yum install sssd-ldap
```

Konfiguration mit authconfig

```
authconfig --enablesssd --enablesssdauth \
   --ldapserver=ldap1.example.com \
   --enableldaptls \
   --enablemkhomedir \
   --update
```

Installation und Konfiguration sssd-ldap 2/2

Beispiel `sssd.conf`

```
[sssd]
domains = LDAP
services = nss, pam
config_file_version = 2
[nss]
[pam]
[domain/LDAP]
cache_credentials = true
id_provider = ldap
auth_provider = ldap
ldap_uri = ldap://ldap1.example.com
ldap_search_base = dc=example,dc=com
ldap_id\_use_start_tls = true
ldap_tls_reqcert = allow
```

Grundlagen Applikationsanbindung

- LDAP Applikations Informationen
  - LDAP URL oder Hostname
  - BaseDN
  - BindDN
  - BindPW
  - Filter
  - evtl. Attribute Mapping
- native LDAP Anbindung
- Anbindund per SASL
- Anbidung per PAM

Beispiel Apache Anbidung

- Module seit 2.2 im Core
- Authentikation und Authorization
- Eigener LDAP Cache
- Viele Authorisierungsmöglichkeiten (Filter, Gruppen, einzelne User)

Installation LDAP Modul

```
yum install mod_ldap
```

Beispiel Apache Anbidung II

Beispiel .htaccess

```
AuthType Basic
AuthName "LOGIN"
AuthBasicProvider ldap
AuthzLDAPAuthoritative on
AuthLDAPURL
   "ldap://ldap1.example.com/dc=example,dc=com?uid?sub?(objectClass=*)"
AuthLDAPBindDN "cn=admin,dc=example,dc=com"
AuthLDAPBindPassword geheim
require valid-user
```

Vielen Dank für Ihre Aufmerksamkeit!

Bei weiteren Fragen wenden Sie sich bitte an info@b1-systems.de
oder +49 (0)8457 - 931096