Konzepte der zentralen User-adminstration mittels LDAP am Beispiel der HP-UX Integration

IT-Symposium 2005
P086

7.April 2005
von Winfried Knobloch

Useradministration via LDAP

Was muß getan werden ?

- User identifizieren und autorisieren
- Accountinformationen zur Verfügung stellen
- zentrale Administration im heterogenen Netzwerk

Useradministration via LDAP

Technische Möglichkeiten – historisch

- Die `libc` bzw. die Applikationen “wissen” wie man an die Daten kommt.
- Was die `libc` nicht kennt, geht nicht ! Und wer ändert etwas an der `libc` ?

Useradministration via LDAP

Technische Möglichkeiten – aktuell

- mittels “Name Service Switch” kann die passende Programmbibliothek ausgewählt werden, um an die informationen zu kommen, z.B.: `libnss_files, libnss_ldap, libnss_nis`, ...
- via PAM-Schnittstelle wird die Authentifizierung flexibel, z.B.: `libpam_unix, libpam_ldap ...`

Useradministration via LDAP

Ansätze

- die Daten auf jedem System in Dateien speichern und lokal auswerten
- die Daten via Netzwerk zugänglich machen und lokal auswerten
- die Daten via Netzwerk zugänglich machen und zusätzliche Netzwerkdienste nutzen

Useradministration via LDAP

Vor- und Nachteile der Ansätze

Jeder Ansatz sollte geprüft werden in Hinsicht

- einfache Administrierbarkeit
- einfache Administrierbarkeit
- Verfügbarkeit
- Anwendungsverträglichkeit

Useradministration via LDAP

Welche Lösungen gibt es zur Zeit ?

- lokale Dateien
- NIS (aka YELLOW PAGES)
- NIS+
- LDAP
- ...

Useradministration via LDAP

Unser Thema – LDAP

Useradministration via LDAP

Was ist LDAP ?

“Das **Lightweight Directory Access Protocol** (**LDAP**) ist in der Computertechnik ein Netzwerkprotokoll, das die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes (eine im Netzwerk verteilte hierarchische Datenbank) erlaubt. Die aktuelle Version ist in RFC 2251 spezifiziert.”
(vgl http://de.wikipedia.org/wiki/LDAP)

Useradministration via LDAP

Was heißt wir nutzen LDAP ?

- Bereithalten der Daten bzw. Funktionalitäten auf zentralen Servern.
- Die einzelnen Systemen fragen die Informationen vom Server ab bzw. delegieren Arbeit.
- Client und Server kommunizieren mittels LDAP-Protokoll.

Useradministration via LDAP

Was kann LDAP ?

- einsetzbar in heterogenen Umgebungen
- kann die Ansprüche der aktuellen Diskussionen, z.B. in Sachen Skalierbarkeit und Security, erfüllen
- leichte Administration
- Realisierung neuer Konzepte

Useradministration via LDAP

Was kann LDAP nicht ?

- Es bietet nicht automatisch ein "vernünftiges" Konzept.
- Das Umsetzen spezieller Eigenschaften, wie Sicherheit, ist möglich aber nicht automatisch dabei.
- Es sind noch nicht alle Applikationen in der Lage NSS und PAM zu nutzen.

Useradministration via LDAP

Zur Implementation einer LDAP-Lösung

- Bei der Planung ist es wichtig Client- und Serverseite zu trennen.
- Da das LDAP-Protokoll standardisiert ist, hat man bei der Wahl des Servers bzw. der Serversoftware eine große Auswahl.
- Clientsoftware gibt es zum Betriebssystem

Useradministration via LDAP

Zur Beachtung == die Erfahrung lehrt:

- Das Konzept für das Verzeichnis/die Organisation der Daten ist wesentlich für die Flexibilität.
- Man muß damit rechnen, daß ungewohnte, unerwartete Effekte auftreten.
- Tests mit allen wichtigen Applikationen sind absolut notwendig !!!

Useradministration via LDAP

Die Auswahl des Servers

Prinzipiell gilt:
Freie Auswahl von Plattform und Software !

Aber bisher hat HP für die Clientsoftware nur die Interaktion mit `Netscape Directory Server` auf HP-UX Systemen und `Windows ADS` garantiert.

Useradministration via LDAP

Alternative Serverplattformen

`Novell eDirectory` auf HP-UX / Linux / ...

`OpenLDAP` auf Linux / ...

`SunOne ( iPlanet )`

`...`

Useradministration via LDAP

Die Clientsoftware für HP-UX

“HP-UX LDAP-UX Integration”

- diese Software gibt es im Internet auf der Seite
  http://www.software.hp.com
- sie kostet **0 €**
- Dokumentationen und White Papers findet man unter **http://www.docs.hp.com/en/internet.html**

Useradministration via LDAP

Die aktuelle Version: B.03.30*

Verfügbar für alle HP-UX 11.X Betriebssysteme

Was tun mit HP-UX 10.X und älteren ?

Betriebssysteme die noch nicht via NSS/PAM anbinden lassen, kann man mit dem *NIS/LDAP Gateway* anbinden.

Useradministration via LDAP

Schritte zum Einrichten des Clients

1) Installation der LDAP-Clientsoftware

2) Sicherstellen, daß die notwendigen Informationen auf dem Server verfügbar sind.
(es gibt `setup` und Migrationsskripte)

3) Anpassen der Konfigurationsdateien

In `/etc/opt/ldapux/ldapux_client.conf` passende aktive Einträge für Profile-DN und Server ergänzen:

```
Service: NSS
LDAP_HOSTPORT="15.140.8.81:389"
PROFILE_ENTRY_DN="cn=ldapuxprofile,dc=scvalue,dc=hp"
PROGRAM="/opt/ldapux/config/create_profile_cache"
```

und den einen seziellen Eintrag aktivieren

```
password_as="x"
```

In der Datei

`/etc/opt/ldapux/ldapclientd.conf`

sicherstellen, daß der folgenden Eintrag aktiv ist

```
[StartOnBoot]
enable=yes
```

4) Initialer Download des Profiles

```
/opt/ldapux/config/get_profile_entry -s nss
```


5) sicherstellen, daß der Client-Dämon läuft

```
/sbin/init.d/ldapclientd.rc stop
/sbin/init.d/ldapclientd.rc start
```

und ein erster Test

```
/opt/ldapux/config/display_profile_cache
```

Wird das Attributmapping angezeigt ?

6)Anpassen der Userverwaltung

Editieren/anpassen der Datei /etc/nsswitch.conf, zumindest folgende Zeile sollte aktiv sein

```
passwd: ldap files
```

(je nach Umgebung auch andere Zeilen anpassen)

```
cp -p /etc/pam.conf /etc/pam.conf.vorher
cp -p /etc/pam.LDAP /etc/pam.conf
```


7) Und schon kann man loslegen ☺ !!!

Besser ist aber nochmals zu testen !

```
id <User-Name>
/usr/contrib/bin/nsquery passwd <User-Name>
```

Und natürlich ein Login-Versuch !

Useradministration via LDAP

Abfragen des aktuell benutzten Mappings

```
#> /opt/ldapux/config/display_profile_cache

Global Information from the Configuration Profile
=================================================
    host[:port]:          15.140.8.81:389
    default search base:  dc=scvalue,dc=hp
    auth:                 simple
    profilecachettl:      0 = infinite
    follow referrals:     enabled
    search time limit:    0 = no limit
    bind time limit:      5 seconds
    credential level:     anonymous
```



```
PASSWD service configuration
============================
    Attribute:            is mapped to:
    ----------            -------------
    name:                 uid
    uid number:           uidnumber
    primary gid:          gidnumber
    login shell:          loginshell
    passwd:               *NULL*
    home directory:       homedirectory
    gecos 1:              gecos
    gecos 2:
    gecos 3:
    gecos 4:
    gecos 5:

    Search Descriptor
    -----------------
    search[0]:            dc=scvalue,dc=hp?sub?(objectclass=posixaccount)


....
```

```
GROUP service configuration
===========================
    Attribute:            is mapped to:
    ----------            ------------
    name:                 cn
    gid:                  gidnumber
    members:              memberuid
    passwd:               userPassword

    Search Descriptor
    -----------------
    search[0]:            dc=scvalue,dc=hp?sub?(objectclass=posixgroup)

Pluggable Authentication Module (PAM)  service configuration
============================================================
    Attribute:            is mapped to:
    ----------            -------------
 ...
```


Useradministration via LDAP

Bemerkungen zur Serverkonfiguration

`/opt/ldapux/config/setup`

ermöglicht die erstmalige Konfiguration eines NDS oder Windows ADS Servers

`/opt/ldapux/migrate`

enthält Skripte zur Migration der Daten eines NIS-Servers

Useradministration via LDAP

Für Freunde der OpenLDAP Software

Um einen OpenLDAP Server für HP-UX Clients benutzen zu können, muß man folgendes tun:

Useradministration via LDAP

1)Compile/Install/Configure basic OpenLDAP

2)Schema changes:

-> OpenLDAP comes with the NIS Schema file, not enabled by default, so we have to activate it manually (NIS - RFC 2307)

-> ldapuxprofile - Created a schema file with the objectclass and attributes needed

To enable the schema changes I added the following lines to the slapd.conf file

```
include  /usr/local/etc/openldap/schema/cosine.schema
include  /usr/local/etc/openldap/schema/inetorgperson.schema
include  /usr/local/etc/openldap/schema/nis.schema
include  /usr/local/etc/openldap/schema/ldapux.schema
```

3)Setup access control

Added the following ACL's to the slapd.conf file, this is just the basic ACL to restrict access to the posixAccount info.


```
#
# Restrict access to userpassword to only the user itself
#
access to attr=userPassword
        by self write
        by anonymous auth
        by * none
#
# Don't allow anyone to modify Unix uid, gid and homedirectory
#
access to attr=uidNumber,gidNumber,homeDirectory
        by * read
#
# Allow the user to modify all other attributes of their entry
#   access to *
        by self write
        by * read
```

4) Start slapd

5)Create the Profile entry in the directory

6) Configuration and activation of SSL environment.

Useradministration via LDAP

Ein Beispiel für ein ldapuxprofile

```
version: 1
dn: cn=ldapuxprofile,dc=scvalue,dc=hp
objectClass: top
objectClass: duaconfigprofile
cn: ldapuxprofile
preferredserverlist: 15.140.8.81:389
defaultsearchbase: dc=scvalue,dc=hp
bindtimelimit: 5
authenticationmethod: simple
attributemap: passwd:userpassword=*NULL*
attributemap: shadow:userpassword=*NULL*
servicesearchdescriptor: passwd:dc=scvalue,dc=hp?sub?
(objectclass=posixaccount)
servicesearchdescriptor: shadow:dc=scvalue,dc=hp?sub?
(objectclass=shadowaccount)
servicesearchdescriptor: group:dc=scvalue,dc=hp?sub?
(objectclass=posixgroup)
```

```
servicesearchdescriptor: pam:dc=scvalue,dc=hp?sub?
(objectclass=posixaccount)
servicesearchdescriptor: rpc:dc=scvalue,dc=hp?sub?(objectclass=oncrpc)
servicesearchdescriptor: protocols:dc=scvalue,dc=hp?sub?
(objectclass=ipprotocol)
servicesearchdescriptor: networks:dc=scvalue,dc=hp?sub?
(objectclass=ipnetwork)
servicesearchdescriptor: hosts:dc=scvalue,dc=hp?sub?(objectclass=iphost)
servicesearchdescriptor: services:dc=scvalue,dc=hp?sub?
(objectclass=ipservice)
servicesearchdescriptor: netgroup:dc=scvalue,dc=hp?sub?
(objectclass=nisnetgroup)
servicesearchdescriptor: printers:dc=scvalue,dc=hp?sub?
(objectclass=printerlpr)
```