64 02/04

nux-Magazin

ST LDAP Manager: Zope verwaltet ein LDAP-Directory

Zentral managen

Wenn der Applikationsserver Zope im Zentrum der IT-Landschaft steht und seine Benutzerverwaltung zudem per LDAP macht, keimt beim zuständigen Admin bald ein Wunsch auf: Praktisch wäre es, das ganze LDAP-Verzeichnis in Zope statt mit Spezialtools zu verwalten. Gottfried J. M. Grosshans



Zope besitzt eine eigene und damit proprietäre Userverwaltung [1]. Um nicht mehrere Benutzerdatenbanken führen zu müssen, erlaubt es der LDAP User Folder [2], die Userverwaltung einem (Open-)LDAP-Server ([3] bis [6]) zu überlassen. Der Linux-Magazin-Artikel [7] beschreibt das Kopplungsmanöver per LDAP User Folder.

Admins, die diese Softwarekombination am Laufen haben, möchten vielleicht gern ihr LDAP-Directory ganz und gar über Zope verwalten (lassen). Der LDAP User Folder als reiner Zope/LDAP-Koppler setzt diesem Ansinnen aber Grenzen. Beispielsweise das Delegieren einzelner Aufgaben an User funktioniert so nicht. Hier kommt der ST LDAP Manager, der auch als LDAP Directory Manager firmiert, ins Spiel. Dieser Beitrag beschreibt Installation, Setup und Funktion anhand eines Beispiels. Den ST LDAP Manager **[9]** installieren zu können, setzt eine Verbindung zwischen Zope, Library Python-LDAP, dem LDAP User Folder und dem LDAP-Server voraus, wie sie **[7]** beschreibt. Das Zusammenspiel der einzelnen Komponenten zeigt **Abbildung 1. [7]** benutzte einen Workaround, um Python-LDAP zu installieren, der nicht gerade durch Eleganz in Erinnerung bleibt. Zwischenzeitlich ist der Autor auf die Zope-Version 2.6.2 (als Tar-Datei) umgestiegen und hat Python-LDAP aus den Quellen installiert. Der **Kasten "Installationsarbeiten"** beschreibt die Schritte.

User Folder und ST LDAP Manager konfigurieren

Es ist ratsam, zunächst ein Testszenario anzulegen, um sich nicht selbst aus Zope auszusperren. Das gelingt beispielsweise

ST LDAP Manager

Wer Zope, den LDAP User Folder und (Open-) LDAP bisher im Einsatz hat, kann nach dem Abarbeiten der Anleitung in diesem Artikel in Zope:

- LDAP-Schemata ändern,
- eine dedizierte Rollenstruktur f
 ür LDAP-Admins festlegen,
- Usern die Änderung ihrer eigenen LDAP-Daten erlauben,
- Usern die Suche in LDAP-Verzeichnissen nach vorgegebenen Mustern je nach Rechten einer Usergruppe ermöglichen,
- Formularmasken flexibel anpassen,
- LDAP-Objektklassen managen,
- fertige Konfigurationsdateien f
 ür LDAP-Server erzeugen.



Abbildung 1: Die grüne Verbindung stellt die Kommunikation zwischen den Komponenten dar.

Abteilung	Mitarbeiter
Management	G. Grosshans
Marketing	Thomas Grundmann
Consulting	Volker Packe Katharina Weiler
Developer	lrina Bosley Bernd Pallaske
System Administrators	Michael Lips

Abbildung 2: Die neue interne Struktur der aus [7] bekannten Beispielfirma Cytux.

DAP

durch das Anlegen eines Ordnerobjekts »test«. In diesem Ordner legt der Zope-Admin ein LDAP-User-Folder-Objekt an, um die Rollenverteilung der User in diesem Ordnerobjekt an LDAP zu binden. Das setzt einen funktionierenden und administrierten LDAP-Server voraus Als Beispiel dient wie in **[7]** die Firma Cytux, diesmal allerdings um ein paar Mitarbeiter erweitert (Abbildung 2). Abbildung 3 zeigt die Konfigurationseinträge für den LDAP User Folder. Jetzt sollte der Admin die Schemata im LDAP User Folder anpassen, damit die Einträge

Mozila Firebird		
Eile Edit View Go Bookr	arks Iools Belp	
o. o. o o o o o	🔕 🔍 http://grobi01.cytux.de:8080/test/acl_users/manage_m	ain 💌
C Bookmarks	8 Cope on http://grobi01.cytux 8 Chttp://grobmanage_main 6	8 8
Configure	LDAP Schesses Users Groups Log Unde Our	vership Security
LDAPUserFolder at /ter	t/acl_users	Help1
Change the basic properties o	your LDAPUserFolder on this form.	
Title		
Login Name Attribute	Canonical Name (cn)	
RDN Attribute	Canonical Name (cn)	
Users Base DN	ou=mitarbeiter.dc=cytux.dc=de Scope SUBTREE •	1
Group storage	Groups stored on LDAP server	
Groups Base DN	ou=Abteilung.dc=cytux.dc=de Scope SUBTREE •	1
Manager DN	cn=Manager.dc=cytux.dc=de Password *****	
Manager DN Usage	Always Read-only	
User object classes	top.person	
User password encryption	clear 💌	
Default User Roles	Anonymous	
	Apply Changes	[
Done		

Abbildung 3: Die Konfigurationseinträge für den LDAP User Folder. Die Sternchen verbergen »secret«.





der LDAP-Verzeichnisse über den LDAP User Folder einstellbar sind.

Wer das Beispiel eins zu eins durchspielen will, muss Gruppen und Mitarbeiter aus Abbildung 2 in das LDAP-Verzeichnis übernehmen – andernfalls natürlich die der eigenen Firma. Die Pflege kann

Installationsarbeiten

1. Die Datei »python-Idap-2.0.0pre19.tar.gz« (oder eventuell eine neue Version) von der Projektseite [8] ist mit »tar xvfz *Datei*« zu entpacken.

2. Nach dem Wechseln ins Entpack-Verzeichnis ändert man die Datei »setup.py«: In die Zeilen 105 und 113 gehört vor die Module »Idap« und »Idap.schema« ein Hash (»#«). Das Auskommentieren ist nötig, da beide Module nicht mit Python 2.1 klarkommen. Wer Python ab Version 2.3 für Zope benutzt, darf sich diesen Schritt sparen.

3. Dann ist die Datei »setup.cfg« im gleichen Verzeichnis dran, sodass in ihr folgende Library- und Include-Pfade angegeben sind:

library_dirs = /usr/local/7
lib Zope-Pfad/lib /usr/lib
include_dirs = /usr/local/7
include Zope-Pfad/include /usr/7
include /usr/include/sasl

Im absolut anzugebenen »*Zope-Pfad*« ist der Zope-Server installiert.

4. Der Aufruf »*Zope-Pfad*/bin/python setup.py build« erzeugt die Python-LDAP-Module und »*Zope-Pfad*/bin/python setup.py install« installiert sie.

5. Anschließend installiert man den LDAP User Folder wie in [7] beschrieben durch Entpacken der Datei im Zope-Produktverzeichnis »*Zope-Pfad*/lib/python/Products«. Wie gehabt sollten keine Rindviecher im Produktpfad in Zopes Webinterface erscheinen, was darauf hindeuten würde, dass die Installation von Python-LDAP nicht erfolgreich war.

6. Um den ST LDAP Manager zu installieren, ist dessen Tar-Datei von [9] ebenfalls im Zope-Produktverzeichnis zu entpacken. Nach einem Neustart erscheint auch der ST-DAP-Manager-Eintrag im Produktpfad des Webinterface. Damit ist die Installation abgeschlossen. entweder über den LDAP User Folder oder ein anderes LDAP-Admin-Tool außerhalb von Zope geschehen. Anschließend ordnet man die Mitarbeiter ihren Gruppen wie in Abbildung 2 zu.

Nun legt der Admin in der Testumgebung ein LDAP-Directory-Manager-Objekt an. Nach dem Auswählen des Objekttyps zur Neuanlage fordert Zope dazu auf, Daten der Struktur des LDAP-Servers in ein Formular einzutragen. Für das Beispiel lauten die Angaben wie in **Abbildung 4**. Das Speichern mit »Save Changes« beendet die Vorkonfiguration.

Arbeiten mit dem ST LDAP Manager

Jetzt steht im Testordner das neue Objekt »LDAP«. Ein Klick darauf führt wieder zur Konfigurationsseite von ST LDAP Manager. Die Lasche »People« am oberen Fensterrand präsentiert eine Suchmaske, die per Namen nach Mitarbeitern fahndet. Die Daten der gefundenen Person sind per Klick auch änderbar – die nötigen Rechte vorausgesetzt.

Da aber im Moment der Anmeldung noch der Rollenkontext von Zope gültig ist, hat man keinerlei Rechte LDAP-Daten zu ändern. Darum muss der Admin seinen Rollenkontext durch Neu-Anmelden ändern. Hierzu klickt er auf »Login« und bekommt eine Anmelde-Aufforderung. Im Beispiel heißt der Systemadministrator Michael Lips – beim Anmelden erhält er jetzt die Rechte als Administrator. Als Standard definiert der ST LDAP Manager eine Gruppe »System Administrators« als LDAP-Administratorgruppe. Damit besitzt die Rolle jetzt die Schreibrechte auf LDAP-Daten.

Wenn der frisch gebackene Admin jetzt über die »People«-Lasche wieder einen User sucht und findet, wird er einige Links zusätzlich sehen. Abbildung 5 zeigt das Formular für das Ändern der Benutzerdaten. Das System führt automatisch nur zu den Formularen, für die der Bediener Rechte besitzt. Durch einen Klick auf andere Bereiche erscheinen weitere Formularfelder.

Der ST LDAP Manager ist so voreingestellt, dass Angehörige der LDAP-Gruppe »System Administrators« andere User, Gruppen und Schemata modifizieren dürfen. Mitarbeiter, die dieser Gruppe nicht angehören, dürfen nur ihre eigenen Daten samt Kennwort ändern.

Über die Lasche »ORG Units« lassen sich ORG-Units nach dem gleichen Schema suchen und bearbeiten. Die recht simple LDAP-Struktur von Cytux nutzt aber praktisch keine komplexe ORG-Units-Struktur. Analog zu den Mitarbeitern und ORG-Units funktioniert es mit Gruppen: »Groups | Browse Groups Tree« fördert beispielsweise die Firmenstruktur nach Gruppen sortiert zu Tage. Per Klick auf die entsprechende Gruppe gelangt man wieder zu den Änderungsmasken – soweit es die Rolle erlaubt.

Hier lassen sich mit dem Button »Select Owner« Administratoren für diese eine Gruppe einrichten, die Gruppendaten bearbeiten dürfen (siehe Abbildung 6). Wenn es darum geht, der Gruppe Mitar-

Bookmarks		S Cope o	n http://grobi01		Chttp://grob%	Cdc%3Dde 🛞	
-	Configure	T People T	Org Units	Groups	Scheme	Searching & OrgCh	art 🕇 Save Settings
DAP Directo	ry Manager at	t /test/idap					н
n=volker	Packe,ou	=mitarbeite	r,ac=cytu	x,dc=de			
General	Personal	Telephone	Postal Mail	E-Mail	Organization	System	Searc
Attribute		Value					
Branch					_		
Category					_		
Common Na	me(s)	Volker P	acke		_		
Description							
Display Nem							
Company man	-						
Email Addres	55						
Home Page							
Office Numb	er						
Title							
User Passwo	rd	******				Enter confin Passe	your new password and mit if you change your or rord, you will be logged ou

Abbildung 5: Die Änderung der Daten eines LDAP-Users ist jetzt möglich.

Mozila Frebro		000
Elle Edit View Go	Bookmarks Tools Help	
@, @, @ © @ (🖸 🙆 🔍 http://grobi01.cytux.de.808	WestIdapimanage_groups?distinguishedName=cn%3DCo 💌
Q Bookmarks	Zope on http://grobi01.cytux Solution Alignment A	p://grobgory=System @
Cent	pure People Org Units Groups Sch	ema Searching & OrgChart Save Settings
LDAP Directory Mana	iger at /test/ <u>idap</u>	Help!
cn=Consulting,	ou=abteilung,dc=cytux,dc=de	
General	System	Browse Groups Tree
Attribute	Value	
Category		80
Description		
Group Name	Consulting	
Members	cn=Katharina Weiler,ou=mitarbeiter,dc=cytux, cn=Manager,dc=cytux,dc=de cn=Volker Packe.ou=mitarbeiter,dc=cytux.dc=	dc=de Update Membership
Object Class	groupOfUniqueNames top	
Organization		_
Organizational Unit		-
Owner		Select owner
See Also		Select seeAlso
	Save Cancel	
Done		

Abbildung 6: Über »Select Owner« lässt sich ein Gruppenadministrator bestimmen, »Update Membership« ordnet der Gruppe die Mitarbeiter zu.

LDAP Manager

beiter zuzuordnen, ist der Button »Update Membership« gefragt. Das Gleiche bewirkt der entsprechende Button in der Startseite der Lasche »Groups«.

Viele Möglichkeiten

Wie gezeigt ist das System in der Standardkonfiguration schon sehr flexibel gestaltet. Doch die Gestaltungsmöglichkeiten sind damit nicht erschöpft. Beispielsweise versetzt die Lasche »Searching & Orgchart« den Admin in die Lage, die Suchmasken frei anzupassen und zu erweitern. Auch das Anzeigeverhalten der Gruppenstrukturen kann er dort einstellen. Wem das nicht reicht, der passt alle Schemata über die Lasche »Schema« an. Hier wählt er auch das Wunschobjekt: »People«, »ORG-Units« oder »Groups« und modifiziert es anschließend nach Belieben.

In gleicher Weise lassen sich über den Link »Select Attributes« (siehe Abbildung 8) beziehungsweise »Manage Attributes« die Attribute für die einzelnen Änderungsmasken und über »Display Categories« einzelne Unterkategorien der Masken zuerst auswählen und dann verwalten. Die Lasche »Roles« öffnet den

Listing 1: Konfiguration von OpenLDAP

001 # Start of LDAP Manager generated	035 filter=(objectclass=person)	136 by group="cn=System Administrators,
configuration	036 attrs=physicalDeliveryOfficeName,	ou=Abteilung,dc=cytux,dc=de" write
002	st, street, title	137 by * read
003 access to dn="cn=subschema" by * read	037 by self read	138
004	038 by dnattr=manager read	139 access to dn.subtree="ou=abteilung,
005 access to dn.subtree="ou=mitarbeiter,	039 by users read	dc=cytux,dc=de"
dc=cytux,dc=de"	040 by anonymous read	140 filter=((objectclass=groupofnames)
006 filter=(objectclass=person)		(objectclass=groupofuniquenames))
007 attrs=children,entry	112 access to dn.subtree="ou=abteilung,	141 attrs=o
008 by * read	dc=cytux,dc=de"	142 by self read
009	113 filter=(objectclass=organizationalunit)	143 by users read
010 access to dn.subtree="ou=mitarbeiter,	114 attrs=children,entry	144 by anonymous auth
dc=cytux,dc=de"	115 by group="cn=System Administrators,	145
011 filter=(objectclass=person)	ou=Abteilung,dc=cytux,dc=de" write	146 access to dn.subtree="ou=abteilung,
012 attrs=homePhone,homePostalAddress,	116 by * read	dc=cytux,dc=de"
mobile,pager	117	147 filter=((objectclass=groupofnames)
013 by self write	118 access to dn.subtree="ou=abteilung,	(objectclass=groupofuniquenames))
014 by dnattr=manager read	dc=cytux,dc=de"	148 attrs=cn,objectClass,ou
015 by users auth	<pre>119 filter=(objectclass=organizationalunit)</pre>	149 by self read
016 by anonymous auth	120 attrs=businessCategory,description,	150 by users read
017	facsimileTelephoneNumber,1,ou,	151 by anonymous read
018 access to dn.subtree="ou=mitarbeiter,	physicalDeliveryOfficeName,postOfficeBox,	152
dc=cytux,dc=de"	<pre>postalAddress,postalCode,searchGuide,</pre>	153 access to dn.subtree="ou=abteilung,
019 filter=(objectclass=person)	<pre>seeAlso,st,street,telephoneNumber</pre>	dc=cytux,dc=de"
020 attrs=mail,mailAlternateAddress,	121 by self auth	<pre>154 filter=((objectclass=groupofnames)</pre>
objectClass,uid	122 by dnattr=manager read	(objectclass=groupofuniquenames))
021 by self read	123 by users read	155 attrs=businessCategory,description,owner
022 by dnattr=manager read	124 by anonymous read	156 by self write
023 by users read	125	157 by users read
024 by anonymous read	126 access to dn.subtree="ou=abteilung,	158 by anonymous auth
025	dc=cytux,dc=de"	159
026 access to dn.subtree="ou=mitarbeiter,	127 filter=(objectclass=organizationalunit)	160 access to dn.subtree="ou=abteilung,
dc=cytux,dc=de"	128 attrs=objectClass	dc=cytux,dc=de"
027 filter=(objectclass=person)	129 by self auth	<pre>161 filter=((objectclass=groupofnames)</pre>
028 attrs=0	130 by users read	(objectclass=groupofuniquenames))
029 by self read	131 by anonymous read	<pre>162 attrs=seeAlso,uniqueMember</pre>
030 by dnattr=manager read	132	163 by self write
031 by users auth	133 access to dn.subtree="ou=abteilung,	164 by users read
032 by anonymous auth	dc=cytux,dc=de"	165 by anonymous read
033	134 filter=((objectclass=groupofnames)	166
034 access to dn.subtree="ou=mitarbeiter,	(objectclass=groupofuniquenames))	167 # End of LDAP Manager generated
dc=cytux,dc=de"	135 attrs=children,entry	configuration

	entigure People	Cong Units Groups	bi01 cy 🛞	C http://grohem	aRoles 🛞
AP Directo	www.Mananer.at./	estidan			Hele
mon Schem	18 . Go				
bject lasses	Select Attributes	Display Categories	Roles	Manage Attributes	Object
oles					
Self		The role controlling a	ccess to the au	theriticated user's a	
Anonyr	nous Liser	The role controlling a	coass by an ar	onemous (i.e., up-a	whirecord, shanticated) use
Authen	nous User ticated User	The role controlling a The role controlling a directory, in general.	iccess by an ar in authenticated	forymous (i.e., un-au diuser's access to th	wn record. .thenticated) use e objects in the
Anonyr Authen Direct I Rena	nous User 6cated User Manager me	The role controlling a The role controlling a directory, in general. The role controlling a manager. (Not the 20	in authenticated in authenticated incress to a user opermanager ro	onymous (i.e., un-ai d usen's access to th n's record by that us le.)	whirecord, dhenticated) use elobjects in the ens direct
Anonyr Authen Direct I Rena	nous User Ecated User Manager me	The role controlling a The role controlling a directory, in general. The role controlling a manager. (Not the 2 Group Distinguish	eccess by an ar in authenticated eccess to a user ope manager ro ed Name(s)	onymous (i.e., un-a d user's access to th r's record by that us le.)	wn record. zhventicated) use e objects in the er's direct
Anonyr Authen Direct I Rena onfigured I Divisior	nous User 6cated User Manager me Roles nal Administrators	The role controlling a The role controlling a directory, in general The role controlling a manager. (Not the Zo Group Distinguish	eccess by an ar in authenticated eccess to a user ppe manager ro ed Name(s)	nonymous (i.e., un-ai d user's access to th d's record by that us le.)	wn record. zhventicated) use e objects in the er's direct
Anonyr Authen Direct I Rena onfigured I Division System Delet	nous User dicated User Manager me Roles hal Administrators h Administrators *	The role controlling a The role controlling a directory, in general The role controlling a manager. (Not the 2: Group Distinguish	eccess by an ar in authenticated inccess to a user inccess to a us	onymous (i.e., un-a d user's access to th r's record by that us le.)	wn record. dhenticated) use e objects in the er's direct
Anonyr Authen Direct I Rena onfigured I Division System Delet e this form to	nous User ticated User Manager me Roles nat Administrators a dministrators e o add a new role to	The role controlling a the role controlling a directory, in general. The role controlling a manager. (Not the 20 Group Distinguish the Configured Roles	incress by an ar in authenticated incress to a user incress to a u	ronymous (i.e., un-a d user's access to th ''s record by that us le.)	en record Alvent cated une e objects in the er's direct
Anonyr Authen Direct I Rena onfigured I Division System Delet e this form b	nous User Boated User Manager me Mal Administrators Administrators a o add a new role to AAP Group Roles	The role controlling a directory, in general directory, in general The role controlling a manager. Diot the 2d Group Distinguish the Configured Roles Group Distinguish	incress by an ar in authenticated incress to a user incress to user incress to a user incress to user incress to a user	sonymous (i.e., un-a d user's access to th 's necord by that us le J	en necora Alvent cated une e objects in the er's direct

Abbildung 7: Die Lasche »Roles« führt zum feingranularen Rechtemanagement.



Abbildung 9: Sicherung der Daten in Formaten für LDAP-Server.

Zugang zu dem feingranular aufgebauten Rechtemanagement, wie es **Abbildung 7** zeigt. Hier ist zu sehen, dass die Rolle »Systems Administrators«, wie nicht anders zu erwarten, schon definiert ist. Ein Klick auf diese Rolle befördert die Maske für die dedizierte Einstellung aller Rechte der zugehörigen Gruppe auf den Schirm.

Über den Link »Object Controllers« wird eingestellt, wer bestimmte Objekte än-

so erzeugten Ausgabedatei zu sehen, die dem Setup aus Abbildung 9 entspricht.

Zope als Admin-Zentrale

Der ST LDAP Manager erweitert Zope und LDAP User Folder so, dass ein Admin eine LDAP-Datenbank von hier aus flexibel managen kann. Der Beitrag skizziert die Basisfunktionalität des Softwaretrios. Es verwaltet bei Bedarf auch

View Go Bookmarks Tools Help Edit 🕘 🙆 🕘 🔕 🙆 🖸 🔇 🍳 http://grobi01.cytux.de.9080/te etidap B Zope on http://grobi0... ⊗ Shttp://g...aManaged ⊗ 8 • Go Select Attributes Object Display Categories Manage Attributes Object Controllers Roles conert of an object's distinguished name. The naming attribute identifies objects, and it's value be unique in any container. The naming attribute is a required attribute, in addition to those red by the LDAP schema. ibute (also kr wn as relative distinguished name or RDN) is the left-most st be ning attribute cn • Set Select attributes to manage his form to select the attributes that will be used for managing person objects (i.e., will show forms). Select items on one side and click the buttons to move them to the other side. Unman Managed businessCategory destinationIndicator >> carLicense mployeeNumber departmentNur description ~< nternationali SDNNumber pegPhoto displayName le dURI employeeType oreferredLanguage egisteredAddress eletexTerminalider aletex i so alexNumber iserCertificate iserPKC512 userSMINECertific x121Address physicalDeliv stofficeB ostalAddress stalCode ired attributes e are the attributes that are required, given the object classes selected for this type of object uired objectClass



dern darf. Außerdem besteht noch die Option, per »Save Settings« die eingestellten Schemata in auch für LDAP-Server lesbare Konfigurationsdateien zu sichern – das spart viel Tipparbeit. In Listing 1 ist der Ausschnitt einer deutlich komplexere LDAP-Strukturen. Nähere Erläuterungen zu den einzelnen Formularen von ST LDAP Manager geben ausführliche Hilfeseiten. *(jk)*

Infos

- [1] Zope: [http://www.zope.org], [http://www. zope.com], [http://www.dzug.org]
- [2] LDAP User Folder: [http://www.dataflake. org/software/Idapuserfolder]
- [3] OpenLDAP: [http://www.openIdap.org]
- [4] V. Schwaberow, "OpenLDAP-Praxis": Linux-Magazin 5/2001, S. 84
- [5] Th. King, "Workshop: LDAP, Teil1": Linux-Magazin 6/01, S. 106
- [6] Th. King, "Workshop: LDAP, Teil2": Linux-Magazin 8/01, S. 119
- [7] G. Grosshans, "Verbindliche Auskünfte": Linux-Magazin 11/03, S. 106
- [8] Python-LDAP: [http://python-Idap.sf.net]
- [9] ST LDAP Manager (LDAP Directory Manager): [http://zope.org/Members/stevray/ STLDAPManager]