



Nikhef IdM en LDAP

Achtergrond, interfaces en implementatie

<http://www.nikhef.nl/nikhef/departments/ct/wiki/index.php/NikIDM>

Onderwerpen

- Doelen van het NikIdM systeem
- Directories en LDAP
 - LDAP begrippen
 - Structuur van de Nikhef NikIdM LDAP directory
 - Access Control
 - Tools
- Attributen en Rollen
 - Automatische wijzigingen en synchronisatie
- Authorisatie in Unix, Cyrus en Apache
- UserAdd tools en configuratie

Doelen Nikhef Identity Management

- nieuwe email service
 - Beheer
 - Schaalbaarheid
- Consistent beheer van gebruikers en SSO
- Grid: certificaataanvragen
- Andere diensten
 - SURFspot
 - SURFnet mail filter
 - Elsevier, Kluwer licensed content
 - ...

Implementatie IdM

- Use case overview voor CT in 2008
 - destijds weinig concrete acties
- Actuele use cases eind 2009
 - grid certificaten via SURFfederatie
 - account beheer voor nieuwe mail service
- Pragmatische keuzes
 - Wel centrale directory voor gebruikers beheer
 - Geen dramatische wijzigingen
 - Keuze: LDAP directory met attribuut-based rechten

Use case I: email

- LDAP directory past goed op nieuwe service
 - Cyrus heeft eigen LDAP interface
 - Goed configureerbaar
- Uitbreidbaar naar de mail hub
 - Alias ondersteuning via LDAP
- Triviaal uitbereidbaar naar Unix accounts
 - Authenticatie, authorisatie en name lookup
 - Vervanging van 'NIS/YP'

Use case II: Grid Certificaten

- Integratie in SURFfederatie
 - Contacten sinds 2005
 - IdM Maturity Scan Nov 2008
 - Aansluiting: 1 IdP per organisatie
 - Criteria in volgorde van belang:
 - Single sign-on (een IdP)
 - Authorisatie onafhankelijk van authN (attributen!)
 - Koppeling bronssystemen (procedures of automatisch)
 - **Beleid**
 - **Beschreven processen**
 - IdP systeem voor koppeling (SAML2)
 - Kwaliteit van IdM voor certificaatdienst

Andere mogelijkheden

- Network access
 - 802.1x voor vaste aansluitingen
 - Radius/eduroam koppeling
- Andere federatieve diensten
 - Elsevier/kluwer/andere tijdschriften
 - SURFspot
 - SSL-email (TERENA Personal CA)
- Fine-grained access control ikohefnet
 - Group-dn based, authorized_service, host...

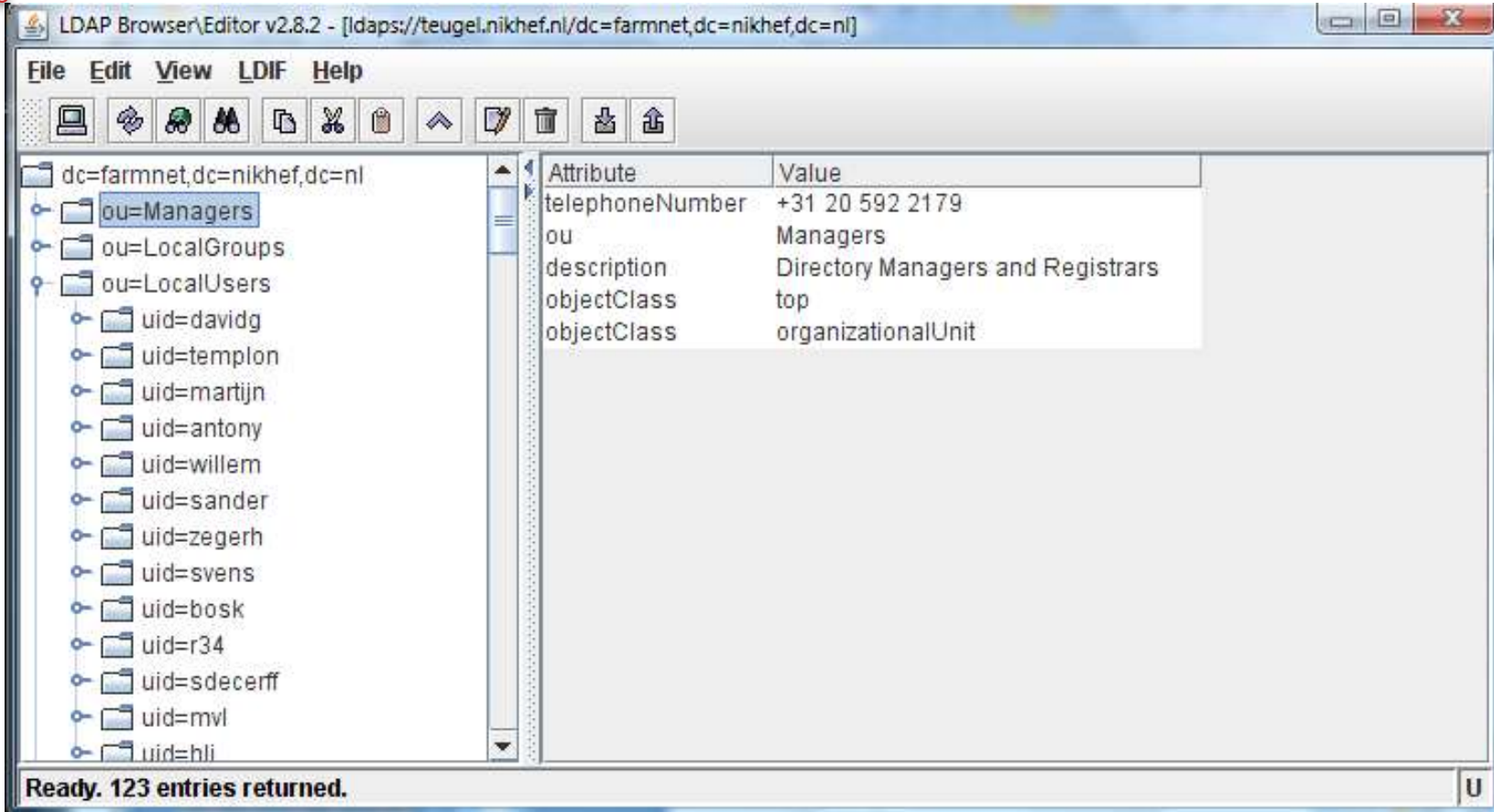
Vervolg uitbreidingen

- Integratie met Active Directory
 - Twee mogelijkheden:
 - Synchronisatie via attribuut-propagatie (LDAP->AD)
 - ~~Alternatieve AD service via Samba~~
- Koppeling NFSv4
 - Kerberos kan LDAP als authenticatie bron gebruiken
 - Password hashes verschillend:
password updates moeten gecentraliseerd worden

LDAP?!

- Light-weight Directory Access Protocol
 - ‘light’ betekent hier: makkelijker dan DAP/X.400!
 - Vele open en closed source implementaties: OpenLDAP, Novell, ActiveDirectory, Oracle, ...
 - Zowel als ‘primair’ systeem inzetbaar als als interface
- Keuze: open source ‘OpenLDAP’ implementatie
 - LDAP database is hier altijd primaire bron
 - Interoperable met bijna alles
 - Consequentie: structuur deels bepaald door clients (NIS schema) beperkte support voor ‘rollen’

LDAP is een directory



The screenshot shows the LDAP Browser/Editor v2.8.2 interface. The title bar indicates the connection path: [ldaps://teugel.nikhef.nl/dc=farmnet,dc=nikhef,dc=nl]. The menu bar includes File, Edit, View, LDIF, and Help. The toolbar contains icons for home, refresh, search, zoom, print, copy, paste, and other standard operations.

The left pane displays a directory tree for the domain `dc=farmnet,dc=nikhef,dc=nl`. The tree structure is as follows:

- dc=farmnet,dc=nikhef,dc=nl
 - ou=Managers
 - ou=LocalGroups
 - ou=LocalUsers
 - uid=dauidg
 - uid=templon
 - uid=martijn
 - uid=antony
 - uid=willem
 - uid=sander
 - uid=zegerh
 - uid=svens
 - uid=bosk
 - uid=r34
 - uid=sdecerff
 - uid=mvl
 - uid=hli

The right pane shows the details for the selected `ou=Managers` entry, presented as a table:

Attribute	Value
telephoneNumber	+31 20 592 2179
ou	Managers
description	Directory Managers and Registrars
objectClass	top
objectClass	organizationalUnit

The status bar at the bottom of the window displays the message: **Ready. 123 entries returned.**

David Groep
Nikhef
Amsterdam
PDP & Grid

Attribute	Value
schacUserStatus	urn:mace:terena.org:schac:userStatus:nikhef.nl:affiliation:active
eduPersonEntitlement	http://nikhef.nl/entitlements/ndpf-login
objectClass	top
objectClass	posixAccount
objectClass	hostObject
objectClass	authorizedServiceObject
objectClass	inetOrgPerson
objectClass	eduPerson
objectClass	ldapPublicKey
objectClass	schacEntryMetadata
objectClass	schacUserEntitlements
objectClass	mailAccount
userPassword	BINARY (41b)
uid	davidg
mail	davidg@nikhef.nl
uidNumber	5917
cn	David Groep
loginShell	/bin/bash
sshPublicKey	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCvXT9wFN0xVg33suYb6t6
sshPublicKey	ssh-rsa AAAAB3NzaC1yc2EAAAABlwAAQEAzd+YrpvDWbG65I5msiNnqv6
maildrop	davidg
host	*
gidNumber	5900
mailacceptinggeneralid	davidg
mailacceptinggeneralid	david.groep
gecos	David Groep, H1.50,+31 20 592 2179
description	David L. Groep
homeDirectory	/user/davidg
sn	Groep
authorizedService	sshd
authorizedService	login
authorizedService	openvpn
authorizedService	svn
eduPersonNickname	David
schacExpiryDate	20400906060200Z

David Groep
Nikhef
Amsterdam
PDP & Grid





dc=farmnet,dc=nikhef,dc=nl	Attribute	Value
ou=Managers	owner	cn=David Groep,ou=Managers,dc=farmnet,dc=nikhef,dc=nl
ou=LocalGroups	description	System Administrators of the NDPF
ou=LocalUsers	objectClass	top
ou=automount	objectClass	groupOfUniqueNames
ou=Poolaccounts	uniqueMember	uid=davidg,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
ou=DirectoryGroups	uniqueMember	uid=ronalds,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
cn=SystemAdministrators	uniqueMember	uid=templon,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
cn=nDPFSubVersionUsers	uniqueMember	uid=sveng,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
cn=nDPFInteractiveUsers	uniqueMember	uid=tsuerink,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
cn=gridSrvAdministrators	uniqueMember	uid=dennisvd,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
cn=gridSrvInteractiveUsers	uniqueMember	uid=janjust,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
cn=nDPFPrivilegedUsers	uniqueMember	uid=okoeroo,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
cn=gridSrvPrivilegedUsers	uniqueMember	uid=tond,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
cn=nDPFAliceVOboxUsers	uniqueMember	uid=paulks,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
cn=nordicPrivilegedUsers	uniqueMember	uid=fbernabe,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
cn=ikonetUsers	uniqueMember	uid=fbernabe,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
ou=OrganicUnits	cn	SystemAdministrators
cn=PDP		
cn=CT		
ou=GenericUsers		
ou=poolaccounts		
ou=iteam		

David Groep
Nikhef
Amsterdam
PDP & Grid

Schemata

- Directory, net als database, heeft een *schema*
 - Bepaalt structuur van de directory
 - Geeft types aan velden (attributen)
 - Groepeert attributen in *objecten*
 - Invoer moet voldoen aan schema of wordt gewijgerd!
- Directory heeft een boomstructuur
 - Entry heeft een naam en een of meer attributen
 - Entry heeft 0 of meer kinderen

NikIDM Directory Tree

- **ou=Managers**
 - Iedereen die de LDAP directory mag wijzigen (in policy termen, de 'registrars')
 - Logins voor automatische processen: backup, replicatie, PRIS matching, opschonen, expiration
- **ou=LocalGroups**
 - Alle Unix groups
- **ou=automount**
 - Unix automount maps

NikIDM Directory Tree

- **ou=LocalUsers**

- Alle echte, menselijke gebruikers ('Users' in de policy)
- Bevat *alle* attributen van een persoon, zoals
Unix uid, uidNumber en primary gidNumber
voornaam, achternaam, common name, nickname
preferred emailadres (niet noodzakelijkerwijs Nikhef)
adressen Nikhef mailbox (mailacceptinggeneralid)
userPassword, sshPublicKeys
authorizedServices
allowed hosts
expiryDate, shadowLastChange
affiliate, gebruiksrechten, gebruikerstatus

NikIDM Directory Tree

- **ou=DirectoryGroups**
 - Gebruikerslijsten per login group
 - Te gebruiken om alleen bepaalde gebruikers inlog rechten te geven op machines
 - **Moet** gebruikt worden op **alle** machines
hoe dat te doen staat verderop in deze presentatie!
- **ou=OrganicUnits**
 - Nikhef organigram, nieuwe stijl
 - Automatisch gegenereerd uit PRIS

NikIDM Directory Tree

- **ou=GenericUsers**
 - De ‘generieke’ gebruikers uit de policy
 - Bijvoorbeeld
 - admin accounts (‘cyrus’, ‘nasadmin’, ‘dpmmgr’,)
 - Groepsaccounts (‘helpdesk’, ‘meet’, ‘pv’, ‘pz’, ‘sgmalice’)
 - Ook, voor de NDPF, de poolaccounts
 - *ou=pvier*, *ou=poolaccounts*, *ou=ndpf*, *ou=GenericUsers*, ...
 - Dus ook **geen** groeps of anonieme accounts onder ‘ou=LocalUsers’!
- **ou=Services**
 - Bv: *ou=aliases*, *ou=mail*, *ou=Services*, of de MAC adres registratie, of ...

Root of the DIT

- De wortel van de Directory Information Tree (DIT) wordt uiteindelijk

dc=nikhef, dc=nl

- Waarbij ‘dc’ is ‘domainComponent’
 - Unieke manier om globaal-niet-overlappende directories te maken
 - Originele X.500 naming (“O=Nikhef,C=NL”) deprecated, omdat het IJkwezen geen delegaties meer doet

User Account

- Users, real person, have a 'typical' account that derived from *inetOrgPerson* as structural class
 - Requires a `commonName`, allows a *uid*
 - Since `uid` is used for entry naming, *uid* is compulsory
- Additional object classes as needed
 - `posixAccount`, `shadowAccount`
 - `authorizedServiceObject`, `hostObject`
 - `mailAccount`
 - `eduPerson`
 - `schacUserEntitlements`
 - *Required managerial classes: schacEntryMetadata*

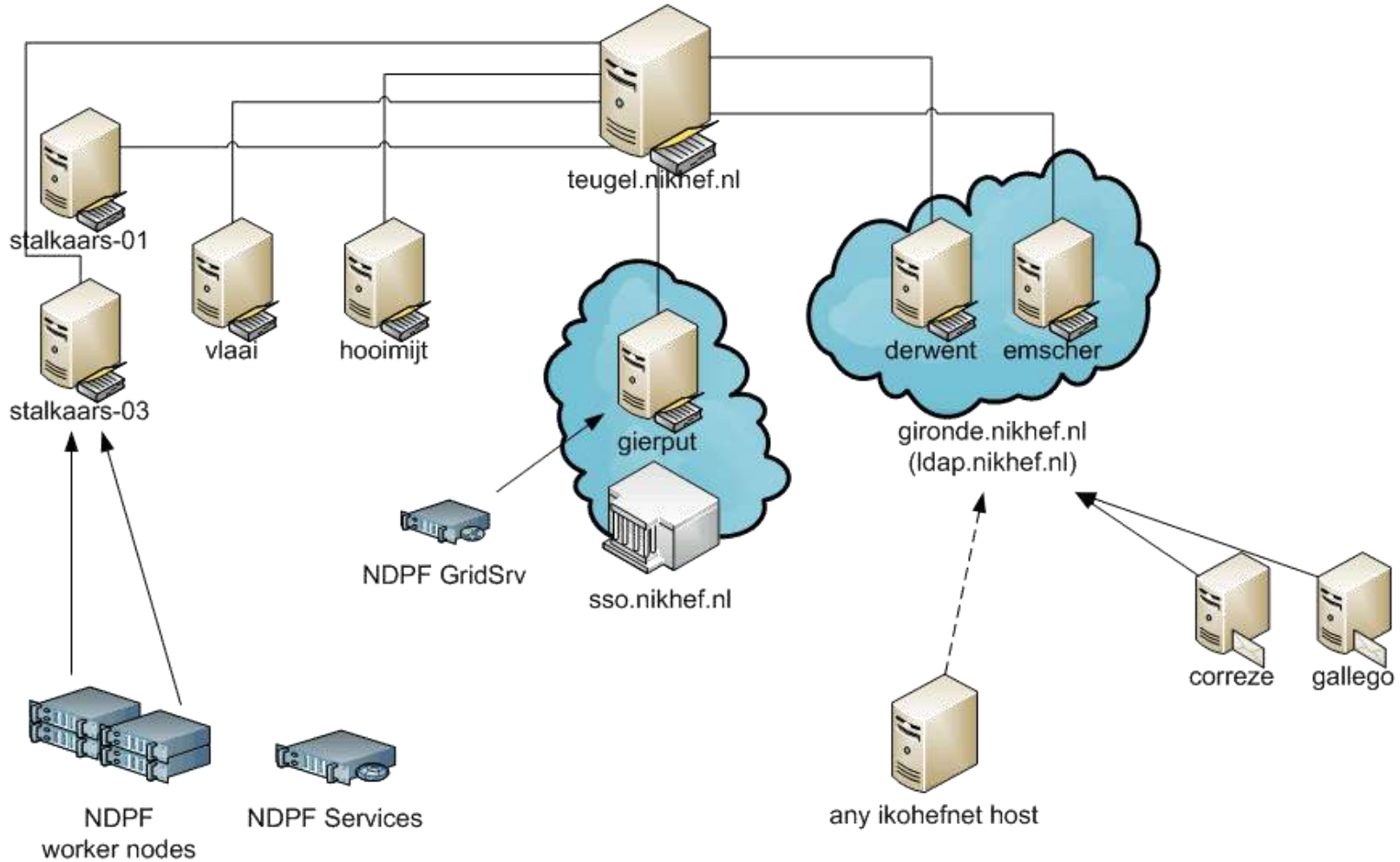
Generic accounts

- Can derive from other objectclass: account
- objectClass 'account' requires:
 - *uid* used for naming under 'ou=GenericAccounts'
- Caveat: 'account' is a structural class
(cannot be combined with *inetOrgPerson*)

Updates & changes to the directory

- Setup: single master, multiple slaves
- Master server: teugel.nikhef.nl
- Slaves: have *updateref* set to teugel.nikhef.nl
 - No changes can be made on the slaves
 - Proper clients will follow redirection
- Access **only** over secure LDAP (ldaps, port 636)
 - No START_TLS support (no port 389) since clients could unwittingly send password in plaintext anyway if they don't enforce STARTTLS ...

Servers



David Groep
Nikhef
Amsterdam
PDP & Grid

ACLs

- ACLs op de LDAP server (slapd) implementeren de policy van NikIdM
 - Alle servers hebben *dezelfde* policy
 - Want alle servers (ook de slaves) hebben alle data
 - Review ACLs tegen policy bij wijzigingen, of pas dan policy aan
 - Let op privacy/DPA/CBP aspecten, en op federatie contracten
- Distributie via RPM ‘ndpf-slapd-acls-1.X-R.noarch.rpm’
 - emscher en derwent hebben een extra ‘public-access’ ACL voor remote address book toegang
 - deze ‘slapd-acls-public.conf’ file zit ook in de RPM
- Voorbeeld LDAP config files (master en slave) in SVN

Interim bijzonderheden (technisch)

- De ‘echte’ top van de boom heet nog
dc=farmnet,dc=nikhef,dc=nl
- In ‘publieke’ LDAP server: alias ‘dc=nikhef,dc=nl’
 - Deze is *slecht* bruikbaar voor pam/nss lookup, omdat interne koppelingen verbroken kunnen worden!

Interim bijzonderheden (organiek)

- Koppeling PRIS met LDAP gaat via email adres
 - Niet iedereen heeft een email adres
 - Niet alle medewerkers hebben een computeraccount!
- PRIS bevat nog beperkte informatie
 - Status van medewerker/gast is niet zichtbaar
 - Heuristiek
 - Iedereen in een missiebudget groep is een medewerker
 - Anderen in pris zijn wel 'member' maar hebben verder geen status
 - Iemand die NIET in PRIS zit, is GEEN medewerker, GEEN lid, en GEEN (wetenschappelijke) staf

LDAP tools

- Web management (binnen Nikhef of via VPN)
 - <https://sso.nikhef.nl/pla/>
 - Web based access
 - Customisable user interface, but rather slow
- LDAP Browser\Editor 2.8.2b
 - <http://www.nikhef.nl/grid/ndpf/files/LDAPBrowser/>
 - Java browser
 - Needs installation on your system
 - Works on Linux, Windows and Mac
- Schrijftoegang (op teugel) vanaf
 - ikonet, hefnet, pcnet I & 2, guestnet, '186' net, en farmnet-public

Veranderingen

- Nieuwe users
 - Nu nog even: via `ndpfypimport` (zie later)
- Attribuut wijzigingen
 - Op user verzoek: **controleer** of wijziging mag, zo ja: log op nikidm-syslog@nikhef.nl (liefst in signed email)
 - Via PRIS: run `ndpfprismatch`
- DirectoryGroup
 - Owner kan het zelf
 - Anders: toevoegen en log naar `nikidm-syslog`
- OrganicUnits: alleen via PRIS
- Aliases: owner, of zoals gebruikelijk



Attributen en policy

David Groep
Nikhef
Amsterdam
PDP & Grid

Attributen

- Attributen zijn basis voor authorizatie
 - ‘foute’ attributen voor personen kunnen zeer ongewenste effecten geven!
 - Attributen alleen maar aanzetten of wijzigen in overeenstemming met de *NikIdM Policy*:
<https://sso.nikhef.nl/policy/>
 - en, waar nodig, na overleg met de service beheerder
- Overigens:
 - ook ‘directorygroups’ geven (extra) rechten
 - graag overleg met de groep-eigenaar

Unix attributen: users

- posixAccount, shadowAccount

```
loginShell: /bin/bash
uidNumber: 5903
gidNumber: 6900
uid: ronalds
gecos: Ronald Starink,5180,wvengen@nikhef.nl,+31201234567
cn: Ronald Starink
homeDirectory: /user/ronalds
shadowLastChange: 59522
userPassword:: e2NyeXB0fSQxJG1CZjJWNDFlJF11Mi9vNnZuekFTa2xLd1JKWDAyWDE=
```

- Attributes vervangen alles uit NIS/YP en /etc/passwd
- Bij gebrek aan GECOS wordt cn gebruikt
- Geen autosync tussen gecoss en andere velden
 - telephoneNumber, homePhone, mail
- shadowLastChange in *dagen na 1 januari 1970*
- userPassword: base64 encoded ‘{crypt}passwordhash’

Unix attributen: groepen

- posixGroup

```
memberUid: davidg  
memberUid: templon  
gidNumber: 6900  
cn: datagrid  
objectClass: posixGroup  
objectClass: top
```

- memberUid attribuut van posixGroup bevat strings: *uid* attribuutwaarden uit posixAccount
- Dit is *anders dan bij de DirectoryGroups*
 - *uniqueMember* attribuut uit *groupOfUniqueNames* is een *DistinguishedName*, géén string

Mail

- Er zijn verschillende mail attributen
 - inetOrgPerson::mail
 - voorkeursemailadres waarop deze gebruiker elektronische post ontvangt
 - Dit is, toevallig, ook het adres dat aan federaties wordt gegeven
 - {virtualaccount,mailaccount}::mailacceptinggeneralid
 - adressen waaronder deze gebruiker mail ontvangt binnen de Nikhef email dienst
 - mailaccount::maildrop – bestemming voor door Nikhef ontvangen email
- Let op: sommige federatieve diensten gebruiken ‘mail’ als een gebruikersidentificatie:
‘Too bad for them’

Status attributen

- eduPerson::eduPersonAffiliation
 - Wat voor ‘soort’ relatie heeft de User met Nikhef
 - **Alleen** instellen voor LocalUsers, met relatie Nikhef
 - Gebruikte waarden
 - **member** – iedereen die bij PZ geregistreerd is
 - **employee** – *iedereen* met een arbeidscontact met een van de Nikhef partners (FOM, RU, UU, UvA, VU)
 - **staff** - alle wetenschappelijk personeel
 - **student** – HBO, bachelor en master studenten, waarvan wij *met zekerheid* kunnen vaststellen dat ze student zijn
 - Nikhef is **contractueel verantwoordelijk** voor de juistheid van dit attribuut, dus *alleen* toekennen na verificatie bij PZ (en automatisch op basis van PRIS)

Status attributen

- eduPerson::eduPersonEntitlement
 - Rechten van een gebruiker in het kader van een overeenkomst met een dienstverlener ('SP')
 - Geldige waarden op basis van overeenkomst, en **alleen** binnen licentie of contractvoorwaarden
 - Nikhef-interne rechten via Nikhef 'name space'
<http://sso.nikhef.nl/entitlements/...> (dit is **geen** URL)
 - Voorbeelden
 - urn:maceterena:tcs:user – gebruiker voldoet aan eisen van het TERENA eScience Personal CA TCS contract
 - <http://sso.nikhef.nl/entitlements/hrenrolment> - gebruiker mag nieuwe medewerkers voor-registreren via de web site

Status attributen

- schacUserEntitlements::schacUserStatus
 - Bepaald of account actief, suspended of expired is
 - Waarde
 - ***urn:mace:terena.org:schac:userStatus:nikhef.nl:affiliation:expired***
gebruiker is *niet meer zichtbaar* en echt overall uitgezet
 - Alleen registrars en de PZ enrolment tool zien 'm nog
 - Voor controle of oude userID namen niet hergebruikt worden
 - ***urn:mace:terena.org:schac:userStatus:nikhef.nl:affiliation:suspended***
van gebruik zijn allen unix NIS attributen over,
 - Gebruiker kan niet meer inloggen en heeft geen services meer
 - Gebruiker kan dus ook geen mail meer lezen
 - Maar een 'ls' op het systeem laat nog wel zien van wie files zijn

Status attributen

- schacUserEntitlements::schacUserStatus
 - ***urn:mace:terena.org:schac:userStatus:nikhef.nl:affiliation:active***
gebruiker is actief en heeft zijn volledige rechten
 - Maar zonder authorizedServices is de gebruiker niks ...

Account expiry

- schacEntryMetadata::schacExpiryDate
 - vervaldatum van het account in ISO8601 full format
 - ‘ndpfcheckdir’ script zoekt naar (bijna) verlopen accounts en stuurt dan mail
 - Iedere non-dry run levert een mailtje op naar gebruikers
 - Waarschuwingen vanaf 30 dagen voor vervaldatum
 - Mails gaan naar ‘primaire’ mail adres (‘mail’ attribuut), niet noodzakelijkerwijs Nikhef email account
 - Na vervaldatum: account is ‘expired’ en niet meer zichtbaar
 - Recovery?
 - Opnieuw aanmelden via PZ of sponsorende medewerker bij Nikhef moet account opnieuw bevestigen
 - **Pas daarna** schacUserStatus weer op ‘..:affilaition:active’ zetten

Password expiry

- shadowAccount::shadowLastChange
 - Laatste wijziging van wachtwoord
 - 'ndpfcheckdir' script zoekt naar account waarbij deze langer dan 365 geleden is en stuurt waarschuwingen
 - Mail gedrag als bij schacExpiryDate, andere inhoud
 - Na vervaldatum: account is 'suspended', beperkt zichtbaar
 - User kan nog wel mail ontvangen (maar uiteraard niet lezen)
 - Helpdesk reset password zet shadowLastChange
 - Maar schacUserStatus moet expliciet worden teruggezet
 - Via LDAPBrowser\Editor of <https://sso.nikhef.nl/pla/>

Andere attributen

- eduPerson::eduPersonPrincipalName
 - Unieke naam van entiteit binnen de instelling
 - Voor ons: deze is *persistent* en *niet-hetbruikbaar!*
 - Format voor NikIDM: *uid@nikhef.nl*
 - Dus voor ons mag ook *uid* **nooit** herbruikt worden
 - Automatisch gegenereerd uit uid door SSPHP
 - Onderdeel SURFfederatie en andere contracten (TCS)
- eduPerson::eduPersonTargettedID
 - Privacy-preserving naam van entiteit voor iedere instelling-dienstverlenings combinatie
 - Automatisch gegenereerd uit uid door SSPHP
 - Nog niet in SURFfederatie, wel b.v. Elsevier, Kluwer

Compromises

- Wanneer er iets mis is met een user account
 - Password gekraakt?
 - Password vergeten en gereset?
- Dan:
 - Password reset via **<http://sso.nikhef.nl/passwd>**
 - **Account suspenden** via LDAP browser: vervang ***[urn:mace:terena.org:schac:userStatus:nikhef.nl:affiliation:active](#)*** door ***[urn:mace:terena.org:schac:userStatus:nikhef.nl:affiliation:suspended](#)***
 - Via TCS eScience portal:
revoke alle certificates van deze user
 - **<https://tcs-escience-portal.terena.org/>**



Authenticatie en authorisatie

Unix login

Apache configuratie

Mail configuratie en aliases

Attributen voor gebruikers

- NIS schema (RFC2307 “An Approach for Using LDAP as a Network Information Service”)

```
objectclass ( 1.3.6.1.1.1.2.0 NAME 'posixAccount'  
  DESC 'Abstraction of an account with POSIX attributes'  
  SUP top AUXILIARY  
  MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )  
  MAY ( userPassword $ loginShell $ gecos $ description ) )
```

```
objectclass ( 1.3.6.1.1.1.2.1 NAME 'shadowAccount'  
  DESC 'Additional attributes for shadow passwords'  
  SUP top AUXILIARY  
  MUST uid  
  MAY ( userPassword $ shadowLastChange $ shadowMin $  
    shadowMax $ shadowWarning $ shadowInactive $  
    shadowExpire $ shadowFlag $ description ) )
```

/etc/ldap.conf

```
$ cat /etc/ldap.conf
```

```
base dc=farmnet,dc=nikhef,dc=nl
timelimit 120
bind_timelimit 120
idle_timelimit 3600
nss_initgroups_ignoreusers
root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mailman
uri ldaps://teugel.nikhef.nl/ ldaps://hooimijt.nikhef.nl/ ldaps://stalkaas-
01.farm.nikhef.nl/ ldaps://stalkaas-03.farm.nikhef.nl/ ldaps://vlaai.nikhef.nl/
ssl on
tls_cacertdir /etc/openldap/cacerts
pam_password md5
pam_groupdn cn=SystemAdministrators,ou=DirectoryGroups,dc=farmnet,dc=nikhef,dc=nl
pam_check_service_attr yes
```

David Groep
Nikhef
Amsterdam
PDP & Grid

```
echo "Enabling authConfig options"
/usr/sbin/authconfig --kickstart \
    --enablemd5 --enablesshadow --enablecache \
    --enableldap --enableldaps
```

Toegangsbeperking

- Directory bevat *alle* gebruikers, externen, email-only accounts, SVN gebruikers, grid users, ...
- Rechten worden bepaald door
 - Attributen
 - Groeps-lidmaatschappen ('rollen')
- **Deze moeten dan ook afgedwongen worden in de verschillende diensten**
- **Let op:**
userPassword zegt *niks* over login-capabilities

authorizedService

- `authorizedServiceObject::authorizedService`
 - Attribueert voor alle accounts (LocalUsers en GenericUsers)
 - Bevat de PAM service naam van alle diensten waartoe gebruiker toegang heeft
 - In enkele gevallen een *quasi-service* naam (b.v.: 'svn')

/etc/ldap.conf

```
pam_check_service_attr yes
```

cyrus.conf en ldap filters

```
(&(|(authorizedService=imap)())() (...))
```

AuthorizedService

- Gangbare waarden
 - sshd toegang via ssh login (password of pubkey)
 - login toegang via console
 - svn opname in ssh key-based NDPF SVN dienst
dit is een quasi-service attribuut
 - imap } cyrus-imap client connect
 - sieve } sieve script filter daemon
 - pop } cyrus-pop3 client
 - smtp } versturen van mail via onze smtp gateway
 - csync internal cyrus cross-synchronisation
alleen voor het interne 'cyrus' admin account

host

- hostObject::host
- Beperking hosts voor (pam_ldap/unix) toegang
- ‘moeilijk’ inzetbaar
 - Is multi-valued, maar geen fnmatch of regex support
 - Lijst met *alle* hosts moet worden opgenomen, of een ‘*’ (maar *niet* ‘*.farm.nikhef.n’, of ‘login*.nikhef.nl’ ☹)
- Staat *niet* in /etc/ldap.conf voorbeeld
- Alternatief: pam_groupdn ‘group-based’ access

Group-based access

- Afdwingbaar in `ldap.conf`, `httpd.conf`, en `.htaccess` files

`pam_groupdn`

`cn=SystemAdministrators,ou=DirectoryGroups,dc=farmnet,dc=nikhef,dc=nl`

- Alleen accounts met een DN die in de groep zit worden toegelaten
 - Heeft dus niks met de unix groep te maken
- In NikIDM zijn deze groepen ondergebracht bij *ou=DirectoryGroups, dc=...*
 - Groepen kunnen owner-editable worden gemaakt (b.v. voor gebruik op de Nikhef web site)
 - In principe zijn ook de OrganicUnits zo te gebruiken ...

RedHat Oops

- RedHat 7+ reserveert uidNumbers onder de 500 voor systeemaccounts
 - Accounts met uidNumber < 500 uit LDAP worden dan ook standaard *gewijgerd!*
 - Wij hebben een aantal end-user accounts met uidNumber < 500, b.v. users uit de ‘computer’ groep
 - Vooral: account computergroep met origine H (aXX series) en nieuwe CT-B accounts tussen 1997 en ~ 2007
 - Oplossing: edit /etc/pam.d/system-auth.conf
 - Op 2 plaatsen ‘500’ vervangen door ‘100’

Apache authorization?

```
LoadModule ldap_module modules/mod_ldap.so
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
```

```
SSLRequireSSL
SSLOptions +StrictRequire
ErrorDocument 403 /to-https.php
```

```
AuthType Basic
AuthBasicProvider ldap
AuthName "NDPF Realm"
AuthLDAPURL
"ldaps://ldap.nikhef.nl/dc=farmnet,dc=nikhef,dc=nl?uid?sub?(objectClass=*)"
Require ldap-group
cn=nDPFPrivilegedUsers,ou=DirectoryGroups,dc=farmnet,dc=nikhef,dc=nl
```

David Groep
Nikhef
Amsterdam
PDP & Grid

- **But please beware of the PHP_AUTH_PW variable!**
- **we need a way to prevent user scripts from becoming phishing sites**

Mail aliases

- Aliases in LDAP also work
 - Owners can manage their mail alias destinations
 - Owner cannot change the name of the alias
 - But you can: adding aliases to the alias

```
dn: cn=Davids Test Aliases,ou=aliases,ou=mail,ou=Services,dc=...
cn: Davids Test Aliases
objectClass: top
objectClass: virtualaccount
objectClass: mailAccount
owner: uid=davidg,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
mailacceptinggeneralid: test-alias@nikhef.nl
maildrop: casper@groep.net
maildrop: marianne@pitnet.nl
maildrop: davidg@nikhef.nl
```



Gebruikers aanmaken

In het primaire LDAP systeem

David Groep
Nikhef
Amsterdam
PDP & Grid

ndpfuseradd (v1.19-2)

- Creating new users from scratch
 - In LDAP only
 - With needed attributes, to be asserted in compliance with the Policy
- Documentation
 - https://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/Adding_local_users
 - and of course at <http://www.nikhef.nl/nikhef/departments/ct/wiki/index.php/NikIDM>

Using the tool

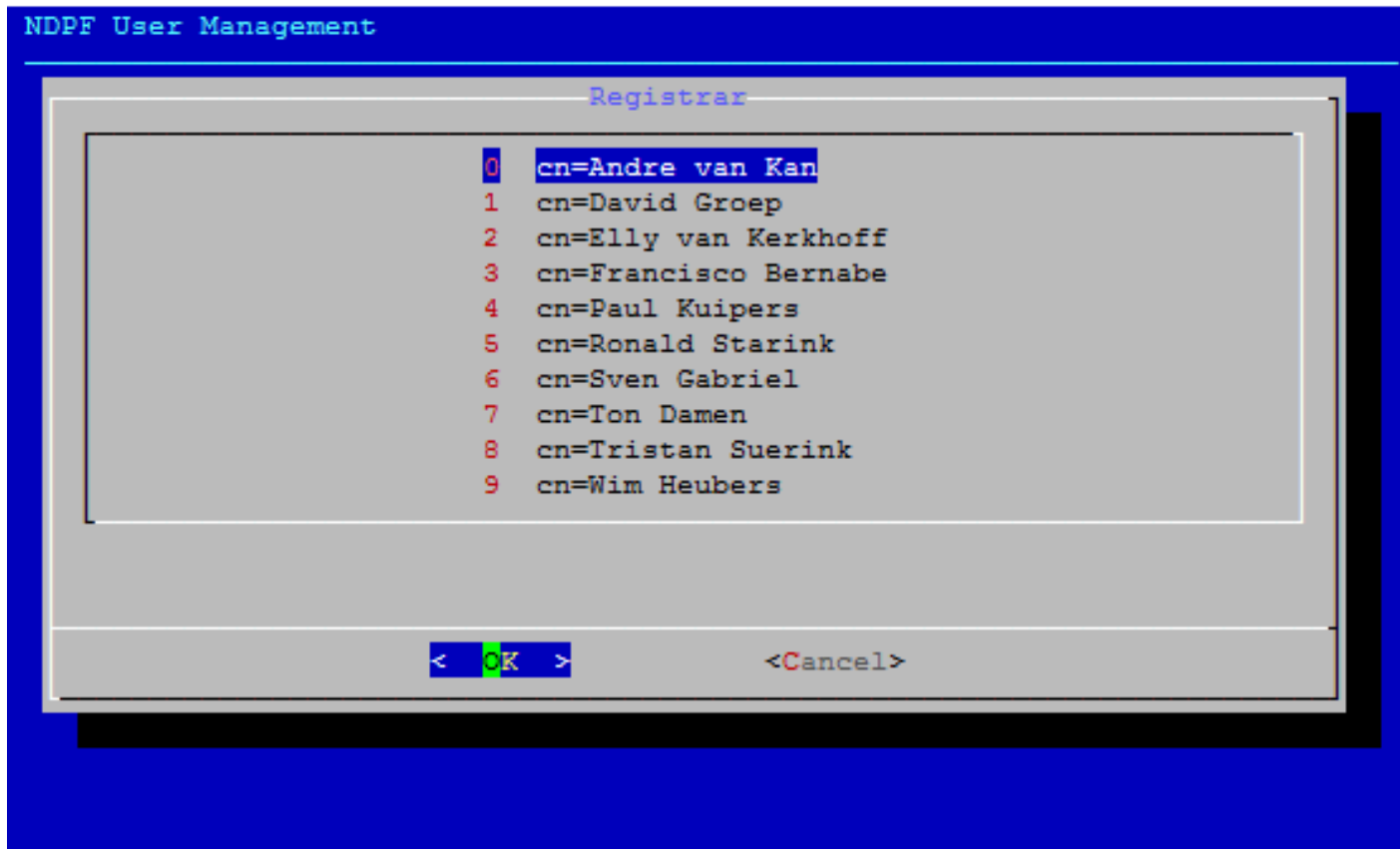
- Requirement
 - Enrolment as an Administrator in LDAP the 'Registrar' in the Policy
 - SSH public key in an agent
 - (root) access to the file servers via ssh key

```
login as: davidg
Authenticating with public key "imported-openssh-key" from agent
Last login: Thu Jan 21 19:32:07 2010 from schrepel.nikhef.nl
[davidg@mestkar ~]$ /usr/local/sbin/ndpfuseradd █
```

- For ikohefnet
ndpfuseradd --minuid=8000 -u 'Klaas Wit'
- Or: create NIS entry and use *ndpfypimport*

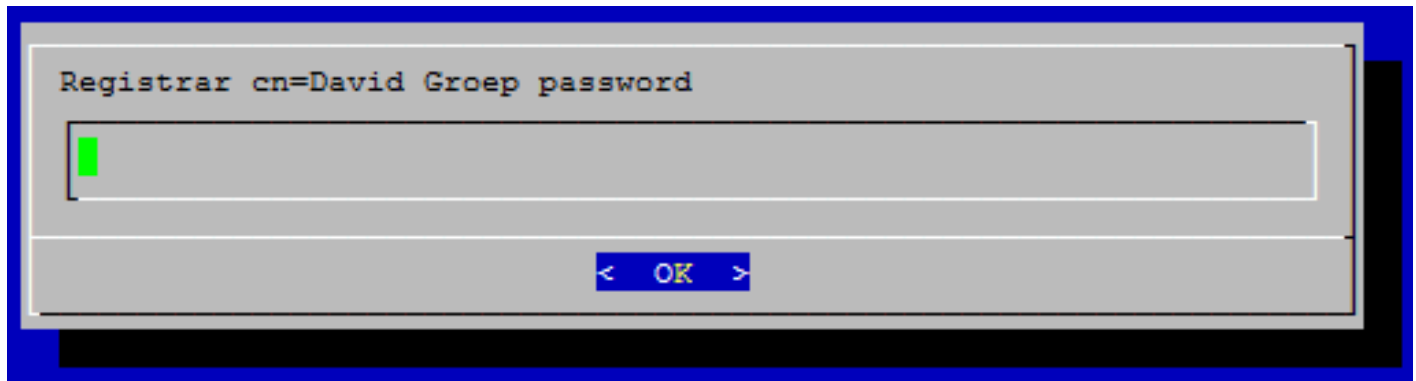
Identifying yourself

- From menu or with '-u "Klaas Wit" '



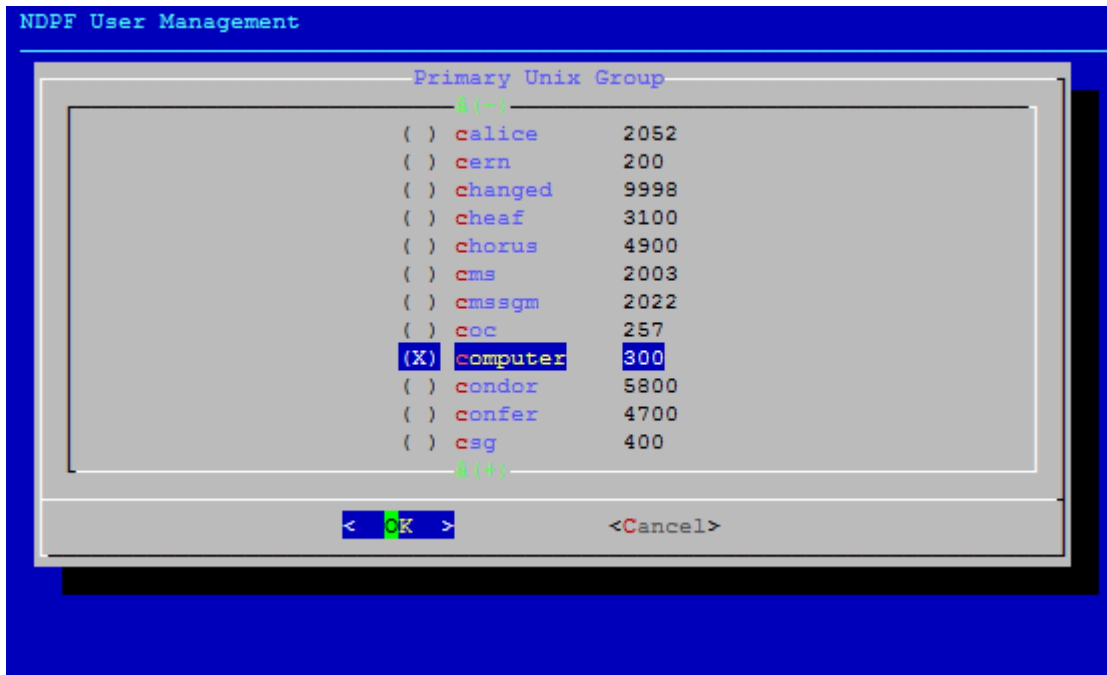
Registrar password

- This is the password for your *ou=Managers* account in LDAP, **not** your SSO password



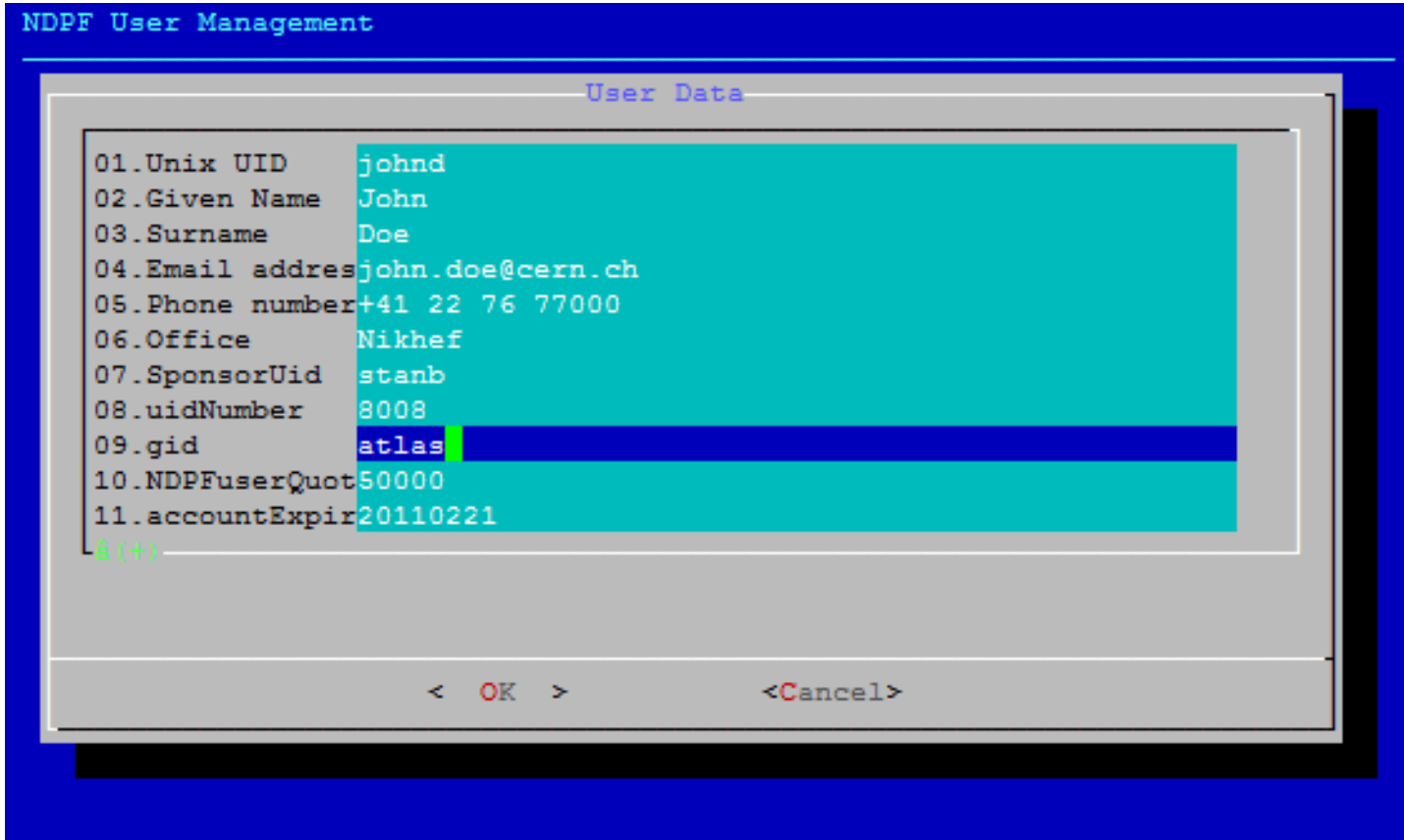
Primary group membership

- Selected from the full list of all Unix groups



- can be changed in the user attribute screen

User attribute screen



The screenshot shows a terminal window titled "NDPF User Management" with a sub-window titled "User Data". The user data is displayed as a list of attributes and values. The attribute "09.gid" is highlighted with a blue bar. At the bottom of the window, there are navigation buttons: "< OK >" and "<Cancel>".

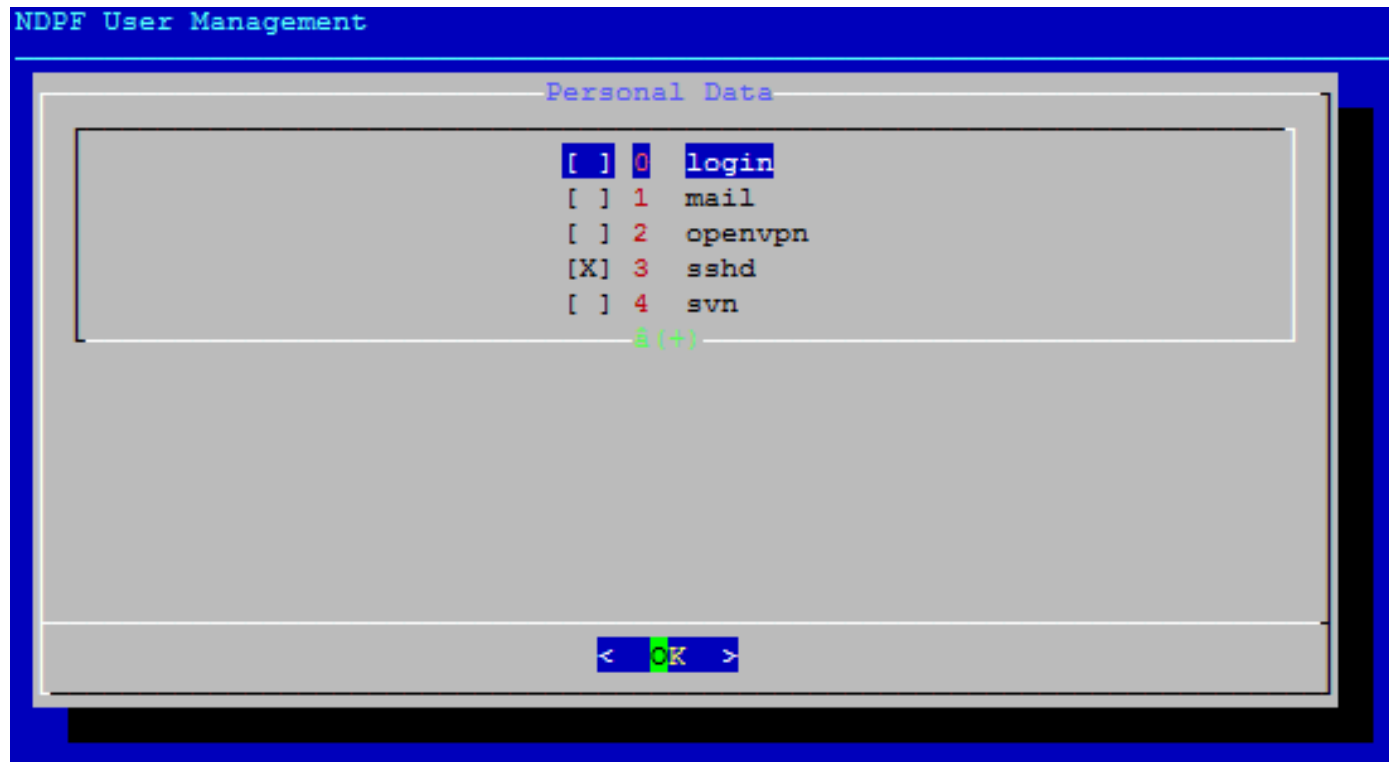
Attribute	Value
01.Unix UID	johnd
02.Given Name	John
03.Surname	Doe
04.Email address	john.doe@cern.ch
05.Phone number	+41 22 76 77000
06.Office	Nikhef
07.SponsorUid	stanb
08.uidNumber	8008
09.gid	atlas
10.NDPFuserQuot	50000
11.accountExpires	20110221

David Groep
Nikhef
Amsterdam
PDP & Grid

- uidNumber: first free uid $>$ minuid, **can be overwritten!**
- accountExpires is in YYYYMMDD, Quota in MByte

Services

- Sets AuthorizedServices and DirectoryGroups



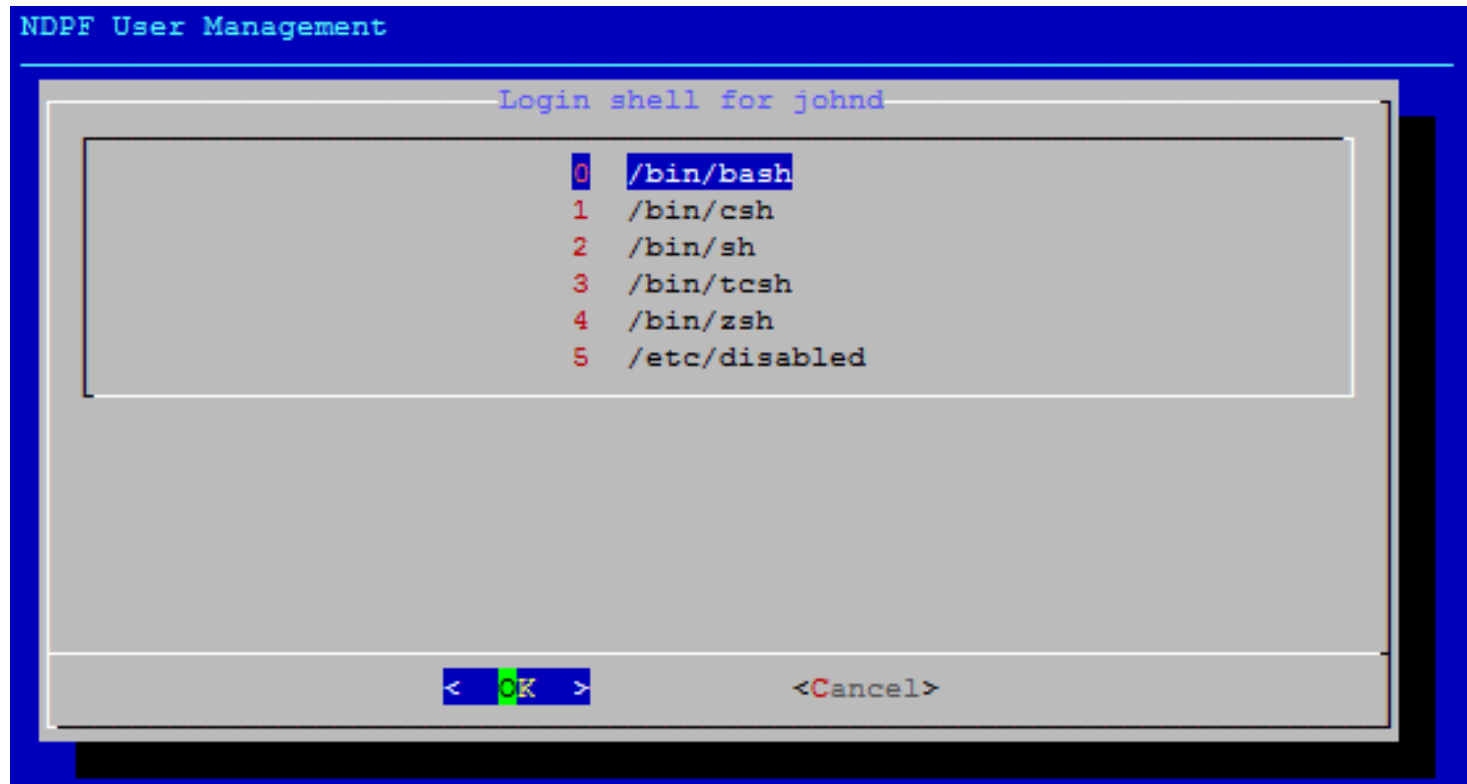
The screenshot shows a terminal window titled "NDPF User Management". Inside, there is a section titled "Personal Data" which contains a list of services. Each service is preceded by a checkbox. The services listed are: login (checkbox []), mail (checkbox []), openvpn (checkbox []), sshd (checkbox [X]), and svn (checkbox []). Below the list is a green prompt character followed by a plus sign in parentheses. At the bottom of the terminal window, there is a navigation bar with a left arrow, a green cursor, the letter 'K', and a right arrow.

Service	Selected
login	[]
mail	[]
openvpn	[]
sshd	[X]
svn	[]

- mail = imap | sieve | smtp | pop3
- Selecting sshd or svn triggers the ssh-key entry box

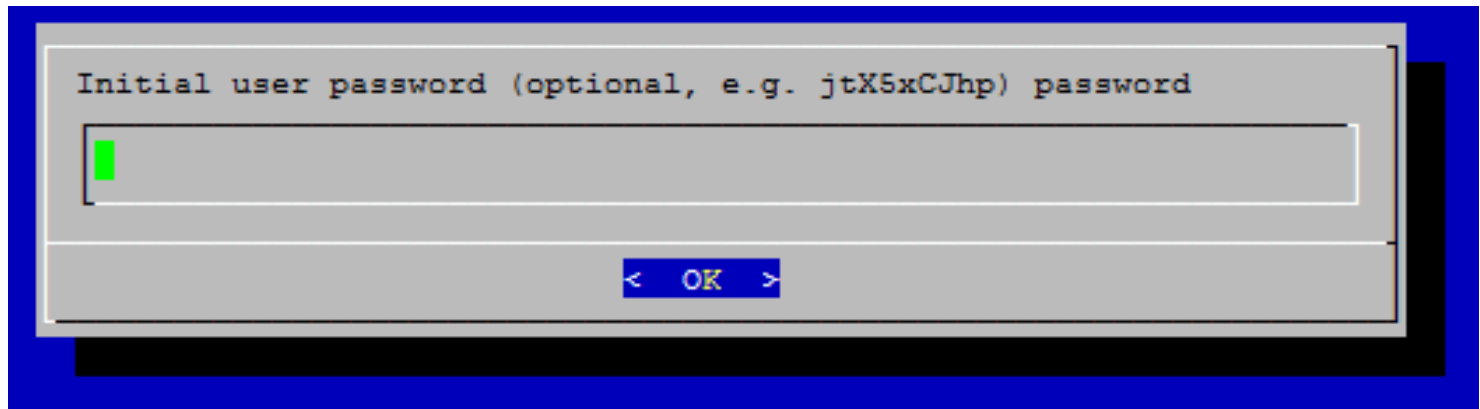
Default login shell

- One must be chosen, even for mail-only accounts (to fill posixAccount objectclas)



Initial user password

- unique random initial password suggestion given (here “jtX5xCJhp”)



Initial user password (optional, e.g. jtX5xCJhp) password

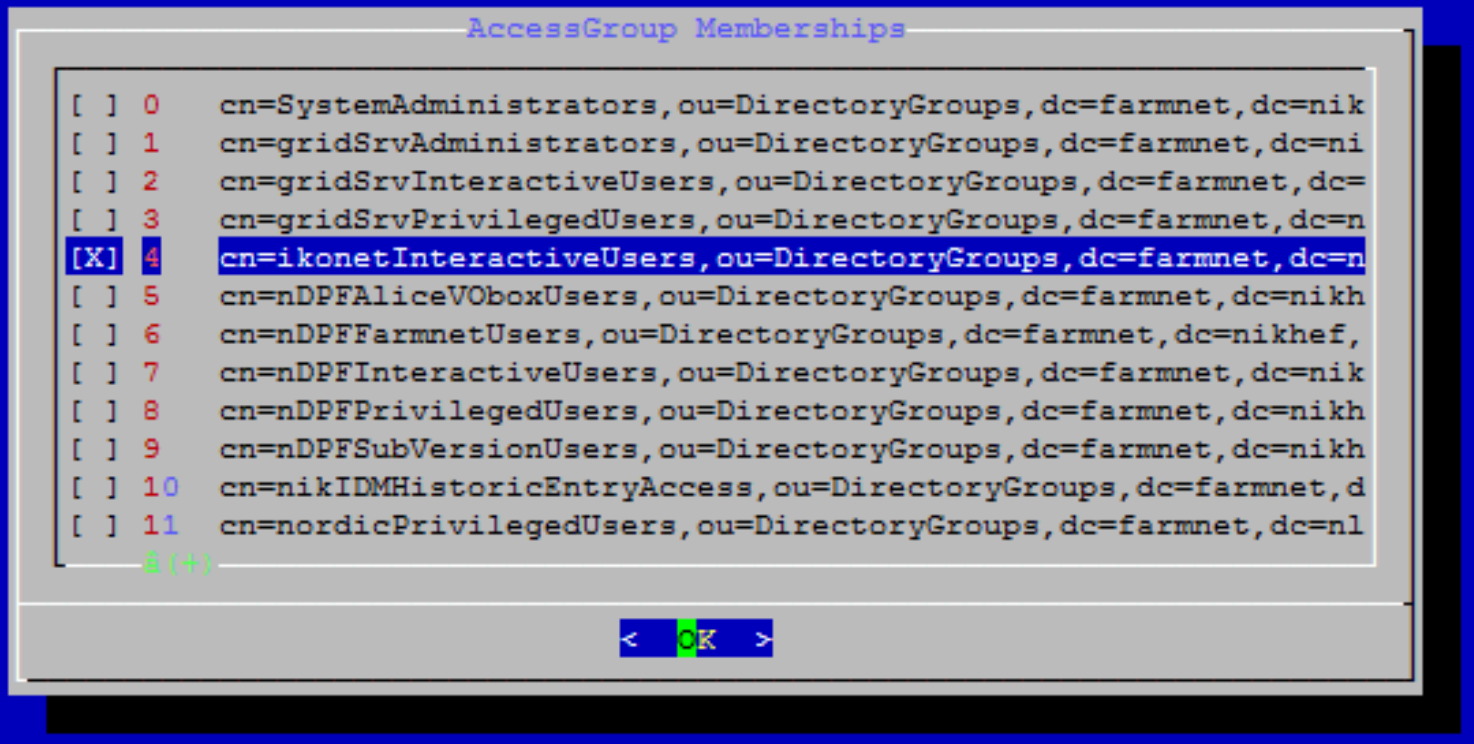
< OK >

Affiliation and userStatus

- By default no attributes assigned
- When a registration form is signed and a password checked by the helpdesk, assert 'F2F
- Affiliation is synched with PRIS anyway!

```
Affiliation and ID Quality
[ ] 0 Affiliation-Affiliate
[ ] 1 Affiliation-Employee
[ ] 2 Affiliation-Member
[ ] 3 Affiliation-Staff
[ ] 4 Affiliation-Student
[ ] 5 Enrolled-Only
[X] 6 Identity-not-vetted
[ ] 7 Identity-recorded-via-F2F
[ ] 8 Identity-vetting-by-acquaintance
  (+)
< OK >
```

- DirectoryGroups for login/ssh/http access
- Please check with the service manager
- For login on desktops: 'ikonetInteractiveUsers'



```
AccessGroup Memberships

[ ] 0  cn=SystemAdministrators,ou=DirectoryGroups,dc=farmnet,dc=nik
[ ] 1  cn=gridSrvAdministrators,ou=DirectoryGroups,dc=farmnet,dc=ni
[ ] 2  cn=gridSrvInteractiveUsers,ou=DirectoryGroups,dc=farmnet,dc=
[ ] 3  cn=gridSrvPrivilegedUsers,ou=DirectoryGroups,dc=farmnet,dc=n
[X] 4  cn=ikonetInteractiveUsers,ou=DirectoryGroups,dc=farmnet,dc=n
[ ] 5  cn=nDPFAliceVOboxUsers,ou=DirectoryGroups,dc=farmnet,dc=nikh
[ ] 6  cn=nDPFFarmnetUsers,ou=DirectoryGroups,dc=farmnet,dc=nikhef,
[ ] 7  cn=nDPFInteractiveUsers,ou=DirectoryGroups,dc=farmnet,dc=nik
[ ] 8  cn=nDPFPrivilegedUsers,ou=DirectoryGroups,dc=farmnet,dc=nikh
[ ] 9  cn=nDPFSubVersionUsers,ou=DirectoryGroups,dc=farmnet,dc=nikh
[ ] 10 cn=nikIDMHistoricEntryAccess,ou=DirectoryGroups,dc=farmnet,d
[ ] 11 cn=nordicPrivilegedUsers,ou=DirectoryGroups,dc=farmnet,dc=nl

  & (+)

< OK >
```

Review LDAP data

- User entry and attributes

```
â(-)
authorizedService: smtp
authorizedService: pop3
authorizedService: mail
authorizedService: sshd
authorizedService: imapd
authorizedService: sieve
cn: John Doe
eduPersonPrincipalName: johnd@nikhef.nl
gecos: John Doe,Nikhef,+41 22 76 77000,
gidNumber: 4600
homeDirectory: /user/johnd
loginShell: /bin/bash
mail: john.doe@cern.ch
mailacceptinggeneralid: johnd@nikhef.nl
â(+)
```

26%

< EXIT >

- *Scroll down for ...*

User attributes (cntd)

- Automount and DirectoryGroups LDIF

```
â (-)
uid: johnd
uidNumber: 8008
userPassword: {crypt}$1$QSTSQ7TX$/zBgdqBmVAn11ANbEGO76/

dn: cn=johnd,ou=local,ou=auto.home,ou=automount,dc=farmnet,dc=nikh
automountInformation: vlaai.nikhef.nl:/export/perm/share/home/john
cn: johnd
objectClass: top
objectClass: automount

dn: cn=ikonetInteractiveUsers,ou=DirectoryGroups,dc=farmnet,dc=nik
modify: add
uniqueMember: uid=johnd,ou=LocalUsers,dc=farmnet,dc=nikhef,dc=nl
```

100%

< EXIT >

Help?!

- If you don't like the entry, press **^C now**
- **If you press “Enter”, the entry process exits and the account is created**
- To clean up:
 - Remove user entry from `ou=LocalUsers`
 - Remove *single uniqueMember* from `DirectoryGroups`
 - Remove the automount entry
 - Clean up file system(s)

UserAdd tools

- Non-LDAP acties: via shell code plug-ins
 - Alle acties en copies worden gedaan via ssh
 - Via ssh pubkey en ssh-agent kan dit zonder password
 - Actief op verschillende target hosts mogelijk vanaf eigen desktop of install server

UserAdd: customisations

- Default versie gaat uit van de NDPF
 - Home directory en quota op vlaai
 - Alleen automount point `/user/uid` in ndpf automount wordt gemaakt, en wijst ook naar vlaai
- Alle shell-code routines zijn run-time pluggable
 - Als de plug-in routine gedefinieerd is wordt deze, en *niet* de standaard uitgevoerd
 - Invoegbaar via `$HOME/.ndpfpooladdrc` perl code
 - Ook de plaats om per-user default te zetten
 - *lkohefnet scripts moeten nog gemaakt worden, op basis van huidig user-add script*

Andere utilities in 1.19-4

- ndpfypimport
- ndpfypexport
- ndpfcheckdir
- ndpfuserattribute
- ndpfprismatch
- ndpfpooladd