Use ACI/ACL to move fast to a stronger and safer directory

Alban Meunier
SmartWave SA

LDAP ACIs,
Lab with ForgeRock OpenDJ
1h45

Agenda

5'

10'

90'

Requirements

- You laptop with a terminal (command prompt for Windows)
- a basic knowledge of LDAP filters
- a laptop with either Windows, OS X, or Linux
- JRE or JDK must be installed
- `OpenDJ-2.6.x.zip` stable downloaded but **not installed**
- https://forgerock.org/downloads/ ** registration required*

  Or Alternate URL for 4 days

http://shortlinks.smartwavesa.com/OpenDJ_forACI .

- Internet access to download hand-outs and data set
  - http://ldapcon.org/2015/?page_id=327 **HeavyMetal**
    - `_The_Power_of_ACI.zip`
    - Few minutes left to get the materials …..

What is this lab about

- **Secure a directory server using ACI**
- **Why ACI ?**
  - linked with business requirement
  - short time to implement
  - simple syntax
  - flexible and powerful
  - auditable
  - no workaround on application side

What to achieve

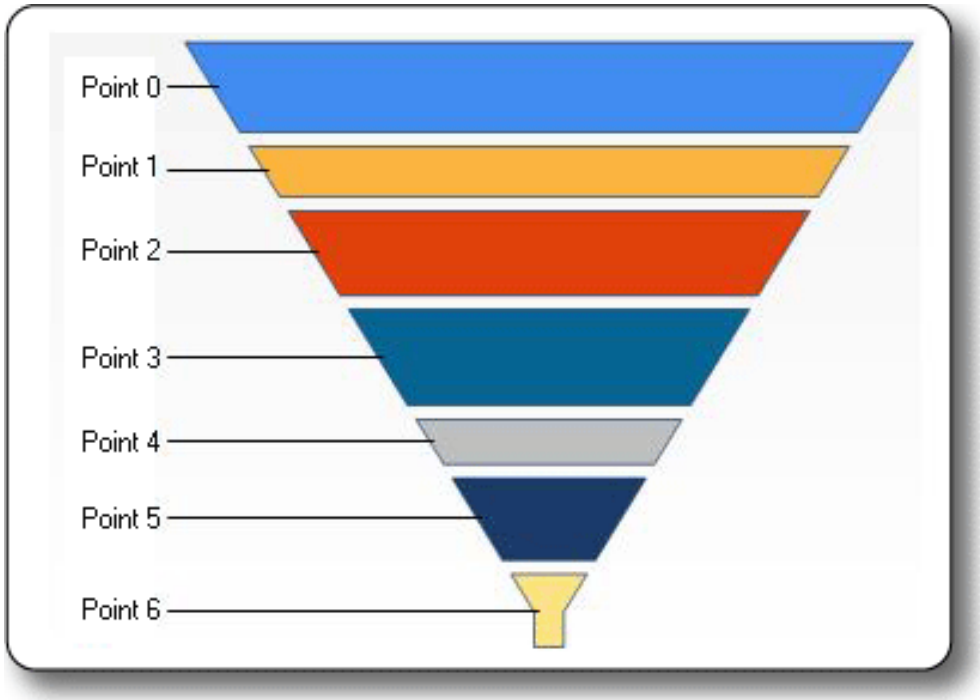
- Gather business requirement
- Install an LDAP directory with data set
- Configure as per IT best practices
- Configure as per Business requirement
- Test
- Plan to go live

Concept of ACI/ACL

- **RFC 2820: Access Control Requirements for LDAP**
  - *fundamental requirements of an access control list model*
  - *provide a simple, but secure, highly efficient access control model for LDAP*
  - *flexibility to meet the needs of both the Internet and enterprise environments and policies*
- **Access Control Instructions/Lists**

ACI/ACL evaluation

- **Inheritance from branched structure (target)**
- **Priority for Deny (permission)**
- **Inheritance from general to details (subject)**
  - Anonymous
  - Authenticated users
  - Self
  - Group membership
  - Authenticated entry



Overview of the syntax elements

- **Business specification**
- ***Protection of externals' email address : the email attribute of external users is searchable and readable by all members of HR when connecting from corporate network during business hours***

- **Technical syntax**
- **targets (version 3.0;acl "name";permissions subjects;)**

Overview of the syntax elements name

- **Business specification**

Protection of email address for external contacts

- **Technical syntax: text**
- **Result**

  targets (version 3.0;acl "Protection of email address for external contacts";permissions subjects;)

Overview of the syntax elements target

- **Business specification:** ***the email attribute of external users***
- **Technical ACI syntax: ldap filter like**
  - (target = "ldap:///uid=*,*,dc=ldapcon,dc=2015")
  - (targetscope = "base|onelevel|subtree|subordinate")
  - (targetfilter [!]= "ldap-filter")
  - (targetattr [!]= "attr-list")
  - (targattrfilters [!]= "expression") add/del=attr1:filter
  - (targetcontrol [!]= "OID")
  - (extop [!]= "OID")
- **Result**

(target=”ldap://ou=People,dc=ldapcon,dc=2015”) (targetscope=”one”) (targetfilter=”employeeType=external”) (targetattr=”mail”)

Overview of the syntax elements permission

- **Business specification**

is searchable and readable

- **Technical syntax**
  - allow/deny(read, search, compare, write, delete, all)
  - import, export
  - selfwrite, proxy

- **Result**

allow(read,search,compare)

Overview of the syntax elements subject

- **Business specification:** ***by all members of HR when connecting from corporate network during business hours***
- **Technical syntax**
  - userdn [!]= "ldap-url++[|| ldap-url++ …]"
    - ldap:///uid=user.01,ou=People,dc=ldapcon,dc=2015
    - ldap:///dc=ldapcon,dc=2015??sub?(uid=user.01)
    - ldap:///all anyone parent self
  - groupdn [!]= "ldap:///DN[|| ldap:///DN …]"
  - authmethod, dns, ip, dayofweek, timeofday, ssf
- **Result**

  groupdn=ldap:///cn=gu_hr,ou=Groups,dc=ldapcon,dc=2015
  ip=ldap://10.11.*.*
  dayofweek != sat,sun
  timeofday >= "0800" timeofday <= "2000"

Overview of the syntax elements summary

- **Business specification**

***Protection of externals' email address** : the email attribute of external users **is searchable and readable** by all members of HR when connecting from corporate network during business hours*

- **Result**

(target=”ldap://ou=People,dc=ldapcon,dc=2015”) (targetscope=”one”) (targetfilter=”employeeType=external”) (targetattr=”mail”) (version 3.0;acl "*Protection of email address for external contacts*" ;allow(read,search,compare) (groupdn=“ldap:///cn=gu_hr,ou=Groups,dc=ldapcon,dc=2015” *AND* ip=ldap://10.11.*.* *AND* dayofweek!=sat,sun *AND* timeofday>="0800" *AND* timeofday<="2000”);)

What we want to achieve

- security best practices
- functional use cases
- no code

Install the environment

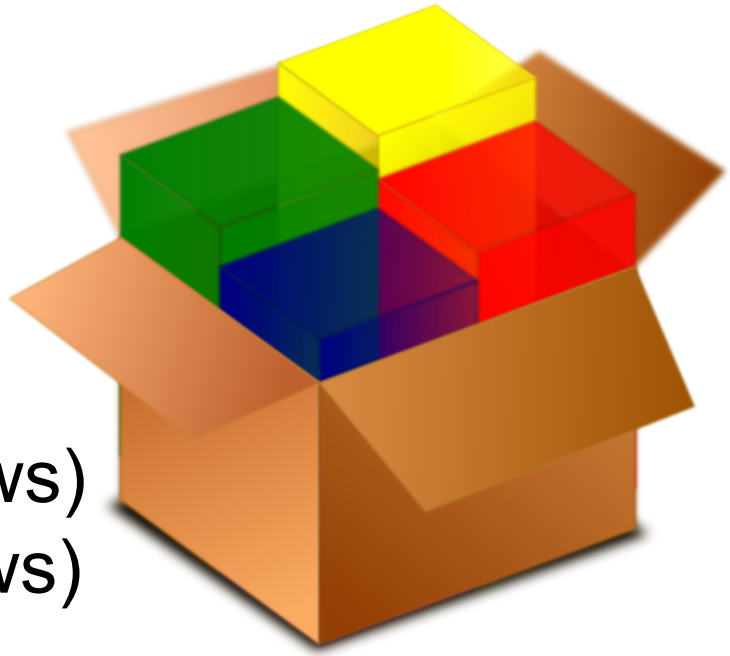
- **install a fresh OpenDJ for the LAB**

```
cd aci.lab
cp 00_The_Power_of_ACI.ldif opendj
unzip opendj-2.6.0.zip
cd opendj
echo password>dirman.pwd
setup ……
```

Refer to
The_Power_of_ACI.txt

What is implemented out of the box

- **understand**
  - 1 ldap server with default settings
  - 2 listeners, 3 protocols (LDAP, StartTLS, LDAPS)
  - 1 data set
  - 1 user set
  - 1 directory manager
  - Various admin tools
- **test ACI**
  - ldapsearch (both linux and Windows)
  - ldapmodify (both linux and Windows)



Secured communication only

① Understand

- user id and password are sent in clear text
- certificates as well …..

Note: we will not force to use StartTLS, but will reject all requests that have not established SSL with encryption

② Test default

- set variables for the Lab
- read with LDAP (anonymous and user.0)
- read with LDAPS
- read with StartTLS

③ Implement

OpenDj proprietary settings
- set require-secure-authentication:true

Option:
- ssf: security strength factor

④ Test after ACI implementation

- read with LDAP (anonymous and user.0)
- read with LDAPS
- read with StartTLS

Disable unauthenticated access

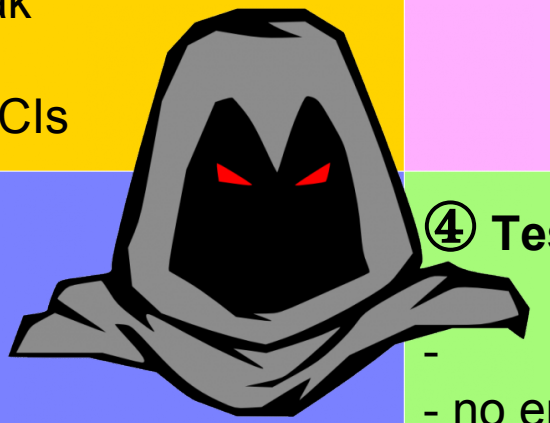
① Understand

- Anonymous access allows read all but pwd
- Common for testing
- Part of RFC to access rootDSE
- Widely used without reconsidering why
- Big opportunity for data leak

- And also remove default ACIs

② Test default

- search StartTLS anonymous and user.0
- objectclass=*
- return all allowed attributes



③ Implement

- reject unauthenticated req.

Note: OpenDJ 2.6.x specifics: use dsconfig and not ldapmodify

④ Test after ACI implementation

-
- no entry returned

Cleanup and no grant

① Understand

- Default ACIs exist
- Remove default ACIs
- Prepare your own ACIs

② Test default

- user.0
- objectclass=*
- all allowed attributes returned

③ Implement

- check existing/ remove ACI
- stop-ds
- global ACI -> ignore “anyone”
- start-ds

./dsconfig set-access-control-handler-prop --remove global-aci: \”escape characters\”

④ Test after ACI implementation

- no entry returned

Directory Administrators

① Understand

- don't use directory manager for operations

- can perform data management

- !!! reset password !!!

② Test default

- user.0
- read all
- write entry
- search entry
- delete entry
- search entry
- reset password

③ Implement ACI

- gm_ldap_Administrators
- all rights + aci + unidexed search

*On OpenDJ, Reset password is a privilege

④ Test after ACI implementation

- can read all
- can write entry
- can write ACI
- can reset password

Directory Operators

① Understand

similar to administrators but
- not authorized to modify ACIs and no rights for proxy authentication
- no reset password
- no right to create new branches on first level
- rights on ou=people
- rights on ou=groups

② Test default

- user.1
- read
- write
- delete
- aci
- reset password

③ Implement ACI

- gm_ldap_Operators
- all rights on ou=people & ou=groups

④ Test after ACI implementation

- can read all
- can write entry
- cannot write ACI
- can reset password

Externals users

① Understand

- can just access personal record
- can modify email, postal address, mobile, password

② Test default

- user.2
- read
- write
- self update

③ Implement ACI

- cn=gu_externals
- or employeeType=external

④ Test after ACI implementation

- Just replay the tests above

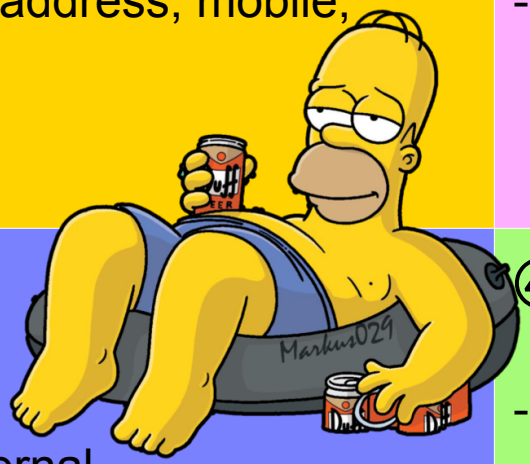
Internals users

① Understand

- can read people entries (limited set of attributes) and groups
- can access personal record
- can self modify postal address, mobile, password

② Test default

- user.3
- read
- write
- self update



③ Implement ACI

- cn=gu_externals
- or employeeType=internal

④ Test after ACI implementation

- Just replay the tests above

HR members*

① Understand

- same as internals
- can create and update internals but not delete them

② Test default

- user.9
- read
- add
- write
- delete
  self update

③ Implement ACI

- cn=gu_hr

④ Test after ACI implementation

- Just replay the tests above

Application account

① Understand

- minimum lookup (uid, email, cn, tel)
- limited write access on tel
- no self update
- group update

② Test default

- ga_app01
- read people
- self update
- group membership update

③ Implement ACI

- uid=ga_app01

* some application can perform proxy authentication

④ Test after ACI implementation

- Just replay the tests above

Export agent

① Understand

- must export all including password hash
- no restore

② Test default

- ga_export
- read
- write

③ Implement ACI

- uid=ga_export

④ Test after ACI implementation

- Just replay the tests above

Get effective rights

① Understand

- checking, assessment, audit
- OID 1.3.6.1.4.1.42.2.27.9.5.2
- No standard on implementation side

② Test basic

- ldapsearch
- Standard ldap request
- Request the OID (*--control effectiverights*)
- Return attribute *aclrights*

③ Implement ACI

- Global ACI: allow OID

See details on the web
http://opendj.forgerock.org/opendj-server/doc/bootstrap/admin-guide/#get-effective-rights

④ Test advanced

Same as basic plus

- Return attribute *aclRightsInfo* (why)
- *--getEffectiveRightsAuthzid*: DN of another user (*"dn:"* for anonymous)
- *--getEffectiveRightsAttribute* for attribute not present on a target entry

Conclusion

- ACl implementation and syntax depends on vendor
- A mandatory effort to secure data store
- Other ACIs can be implemented
- Imagine your owns