Oracle Unified Directory. Lessons learnt.

Is it worth moving from OID?

ANDREJS PROKOPJEVS
Lead Applications Database Consultant
Pythian

About me

Andrejs Prokopjevs

Lead Applications Database Consultant

At Pythian since 2011

Apps DBA from Riga, Latvia.

Speaking SQL since 2001.
In Oracle world since 2004.
“In love” with Oracle EBS since 2006.

@aprokopjevs

prokopjevs@pythian.com

https://www.pythian.com/blog/author/prokopjevs/

ABOUT PYTHIAN

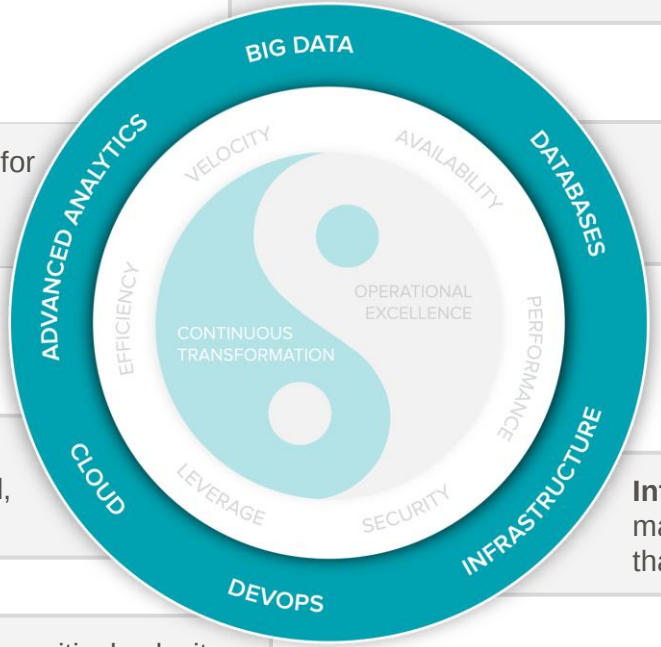
Pythian’s 400+ IT professionals help companies adopt and manage disruptive technologies to better compete

TECHNICAL EXPERTISE

Big Data: Harnessing the transformative power of data on a massive scale

Advanced Analytics: Mining data for insights & business transformation using data science

Databases: Ensuring databases are reliable, secure, available and continuously optimized



Cloud: Using the disruptive nature of cloud for accelerated, cost-effective growth

Infrastructure: Transforming and managing the IT infrastructure that supports the business

DevOps: Providing critical velocity in software deployment by adopting DevOps practices

EXPERIENCED

11,800

Systems currently managed by Pythian

GLOBAL

400

Pythian experts in 35 countries

EXPERTS

2

Millennia of experience gathered and shared over 19 years

Agenda

- What is Oracle Unified Directory?
- Quick overview of integration process with Oracle E-Business Suite R12.2.5.
- Issues faced while implementing OUD.
- Features that deserve a note.
- Performance tuning considerations.

What is Oracle Unified Directory?

What is Oracle Unified Directory?

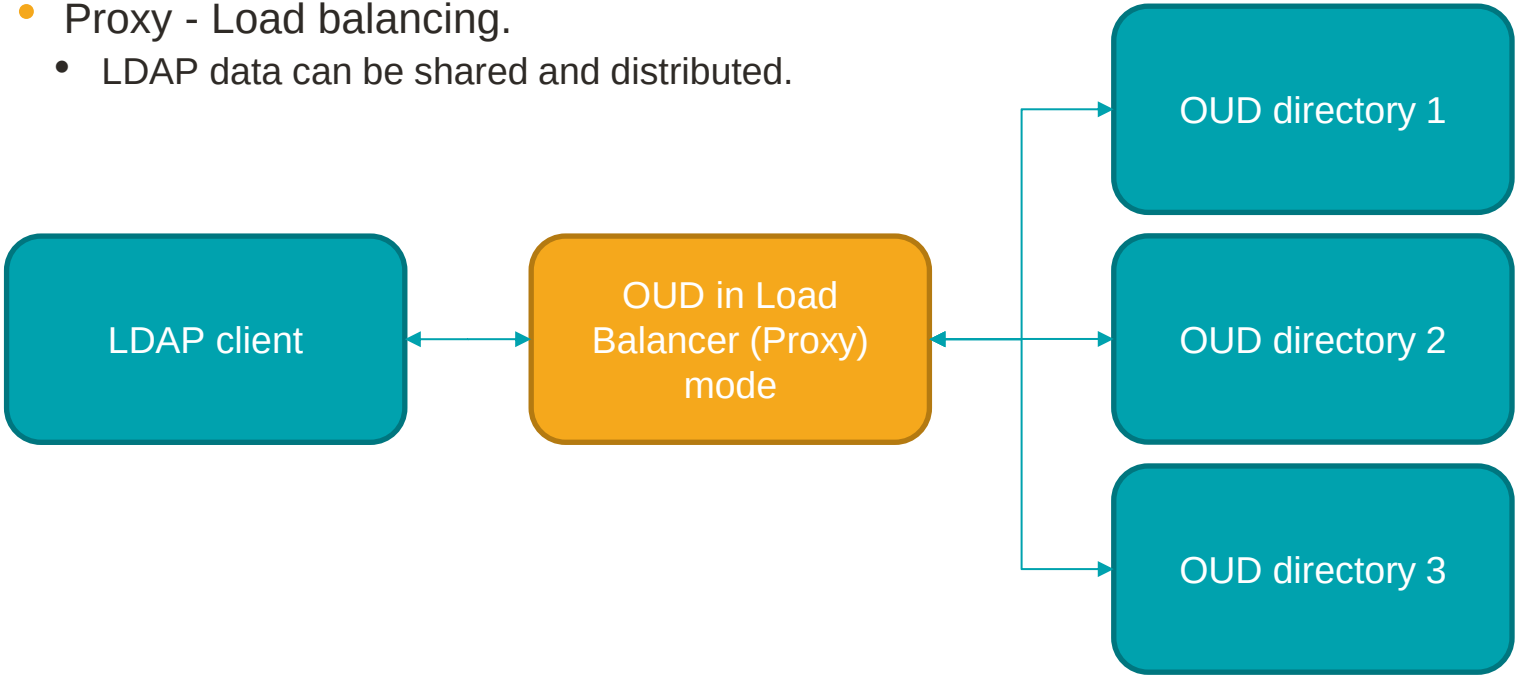
- LDAP v3 compliant directory. Ex Sun iPlanet Directory.
- Completely runs on Java.
- New generation of Oracle Directory Services since 11gR2.
- Announced product replacement of Oracle Internet Directory.

- Features:
  - Storage
  - Proxy and Load Balancing
  - Virtualization
  - Synchronization and Replication

- Data is stored in JavaDB (Oracle Berkeley DB Java Edition).
- Licensed under Oracle Directory Services Plus license.
- Supports known features like Enterprise User Security and TNS store.

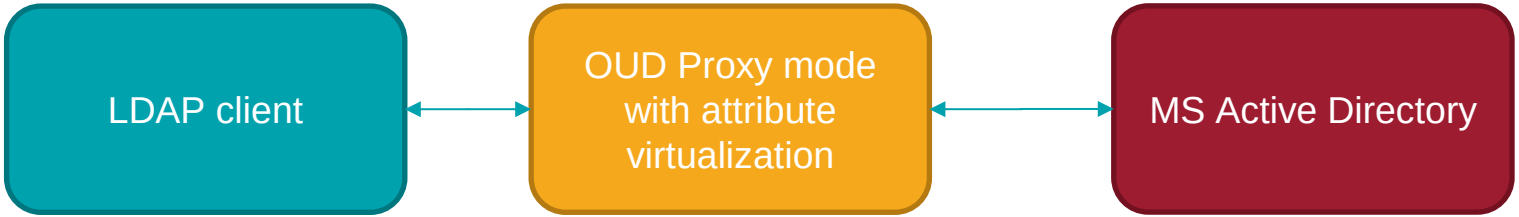
What is Oracle Unified Directory?

- Proxy - Load balancing.
  - LDAP data can be shared and distributed.



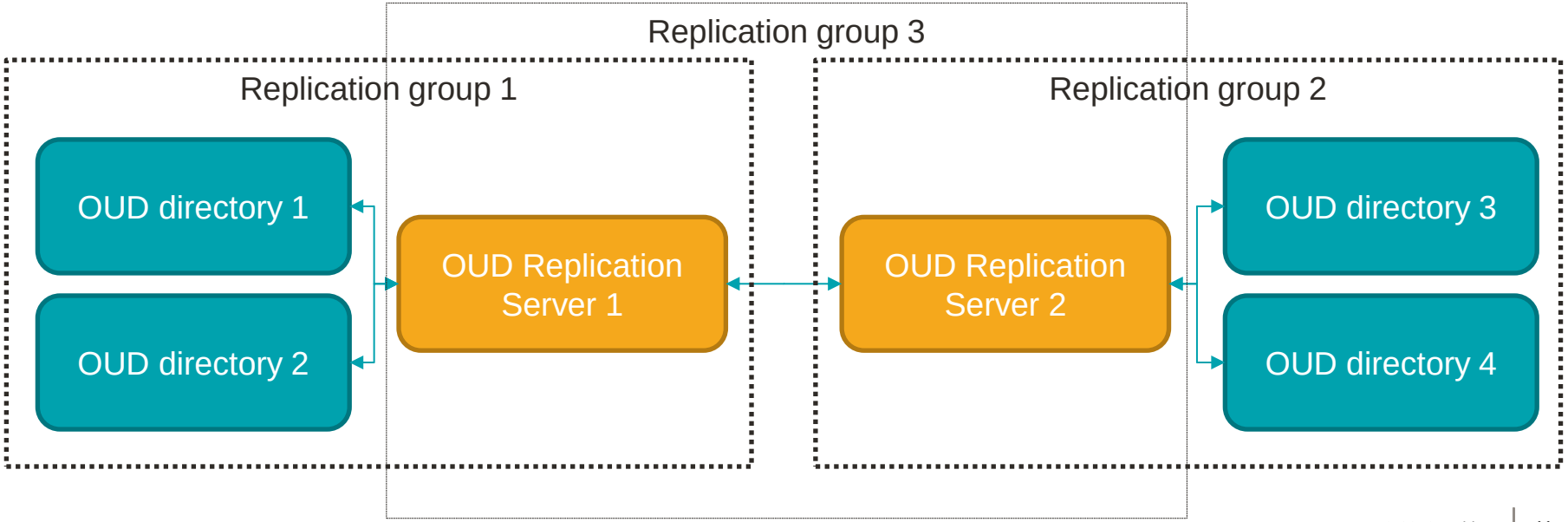
What is Oracle Unified Directory?

- Proxy – mapping of external directories, like Active Directory.



What is Oracle Unified Directory?

- Replication and High Availability.
  - Same instance can share multiple roles like Storage and be a replication server.



Oracle Internet Directory comparison

- **Oracle Unified Directory**
  - Runtime
    - Java
  - Storage
    - JavaDB, local disk storage
  - Clustering concept
    - Multiple instances within replication group
  - Proxy / Virtualization
    - Native support
  - Tools
    - No ldapadd anymore, instead there is "ldapmodify --defaultAdd"
  - Backups
    - No PITR, full or incremental snapshots initiated by the backup utility.

- **Oracle Internet Directory**
  - Runtime
    - C
  - Storage
    - Oracle Database as metadata repository
  - Clustering concept
    - Multiple instances connected to one common Oracle database
  - Proxy / Virtualization
    - Not supported
    - Requires Oracle Virtual Directory
  - Tools
    - Standard set of tools (ldapadd, ldapmodify, ldapdelete, etc)
  - Backups
    - Full PITR supported by Oracle Database.

Oracle E-Business Suite integration overview

Software requirements

- E-Business Suite R12.2.5+
  - FMW 11.1.1.9
  - R12.AD.C.7+
  - Patches 22098300, 21229697, and 24008856
- Oracle Unified Directory 11.1.2.3
  - Being deployed into a separate Fusion Middleware Home.
  - Oracle Directory Services Manager (ODSM) 11.1.2.3
    - Weblogic Server 10.3.6
    - Oracle ADF 11.1.1.9
- Repository Creation Utility 11.1.1.9
- Oracle Directory Integration Platform 11.1.1.9
- Oracle Access Manager 11.1.2.3

Documentation reference

- Integrating Oracle E-Business Suite Release 12.2 with Oracle Unified Directory 11gR2 (Doc ID 2003483.1)
- Integrating Oracle E-Business Suite Release 12.2 with Oracle Access Manager 11gR2 (11.1.2) using Oracle E-Business Suite AccessGate (Doc ID 1576425.1)
- Installation Guide for Oracle Identity Management
  - https://docs.oracle.com/middleware/11119/core/INOIM/under_install.htm#INOIM1024

Configure OUD

- Create the OUD instance.

```
$ echo "welcome1" > /tmp/oud_pwd
$ ./oud-setup --cli \
--hostName myoud.domain.com --ldapPort 1389 --ldapsPort 1636 \
--adminConnectorPort 4461 \
--rootUserDN "cn=directory manager" --rootUserPasswordFile /tmp/oud_pwd \
--generateSelfSignedCertificate --enableStartTLS \
--baseDN dc=example,dc=com \
--integration generic \
--serverTuning 512m --offlineToolsTuning 512m \
--no-prompt
```

  - “generic” integration option creates the necessary naming context, required for EBS integration.

Configure Naming Context

- Modify the realm default user and group base DN references.
  - Very important as this will bring issues at later stages, if not executed.
  - Reference:
    - https://docs.oracle.com/cd/E52734_01/oud/OUDAG/eus.htm#BABGJFEE

  - Locate the LDIF template and edit the naming context you configured.
  - Execute it after correction.

```
$ ldapmodify -h localhost -p 1389 -D "cn=directory manager" -j pwd-file -f
$ORACLE_INSTANCE/config/EUS/modifyRealm.ldif
```

Configure DIP with OUD

- Enable the External Change Log

```
$ dsreplication enable-changelog -h localhost -p 4461 -D "cn=directory manager" -j /tmp/oud_pwd -r 8989 -b
dc=example,dc=com --trustAll --no-prompt
$ dsreplication enable-changelog -h localhost -p 4461 -D "cn=directory manager" -j /tmp/oud_pwd -r 8989 -b
cn=oraclecontext --trustAll --no-prompt
```

- Enforce Unique UID Attribute

```
$ dsconfig -p 4461 -h localhost -D "cn=directory manager" -j /tmp/oud_pwd -n --trustAll set-plugin-prop --
plugin-name "UID Unique Attribute" --set enabled:true
$ dsconfig -p 4461 -h localhost -D "cn=directory manager" -j /tmp/oud_pwd -n --trustAll set-plugin-prop --
plugin-name "UID Unique Attribute" --set base-dn:ou=people,dc=example,dc=com
```

- Configure DIP for OUD

```
$ $ORACLE_HOME/bin/dipConfigurator setup -wlshost localhost -wlsport 7001 -wlsuser weblogic -ldaphost
localhost -ldapport 1389 -ldapuser "cn=directory manager" -isldapssl false -ldapadminport 4461
```

Registration with Oracle EBS

- Start EBS Online Patching Cycle (adop phase=prepare)
- Run all the actions against patch filesystem
  - Register OUD:

```
$FND_TOP/bin/txkrun.pl -script=SetSSOReg -registerldap=yes -ldapadminuser="cn=directory manager"
```

  - Update EBS Profile Options
  - Autoconfig
- Cutover

- Side note:
  - You can do all this in hot mode directly on run file system.
  - Multi-node: This isn't required to be executed on all nodes as stated in the documentation.

Registration with Oracle EBS

- Start EBS Online Patching Cycle (adop phase=prepare)
- Run all the actions against patch filesystem
  - Install WebGate
    - Recommendation: Apply WebGate latest BP patch
  - Deploy AccessGate

```
perl $AD_TOP/patch/115/bin/adProvisionEBS.pl ebs-create-oaea_resources -deployApps=accessgate
```

  - Register OAM

```
$FND_TOP/bin/txkrun.pl -script=SetOAMReg -registeroam=yes -ldapProvider=OUD
```

  - Autoconfig
- Cutover

Registration with Oracle EBS

- Side note:
  - You can do all this in hot mode directly on run file system.
  - But beware of Bug 19817016 **!!!**
    - oaea_server1 (AccessGate) port conflict between run and patch during the fs_clone.

  - Solution:
    - Stop oaea_server1.
    - Run fs_clone.
    - Restart oaea_server1.
    - Next fs_clone executions will not have this conflict anymore.

Issues faced while implementing OUD

Issue #1: Configure Naming Context

- $ORACLE_INSTANCE/config/EUS/modifyRealm.ldif

```
$ ls -l $ORACLE_INSTANCE/config/EUS/modifyRealm.ldif
ls: cannot access /u01/app/oracle/product/fmw11g_oud/instances/OUD_instance/config/EUS/modifyRealm.ldif: No
such file or directory
$ ls -l $ORACLE_HOME/config/EUS/modifyRealm.ldif
-rw-r-----. 1 oracle oinstall 1608 Nov 15  2013
/u01/app/oracle/product/fmw11g_oud/Oracle_OUD1/config/EUS/modifyRealm.ldif
$
```

- Documentation bug.
  - Is deployed only with “--integration EUS”, but still available under Oracle Home

Issue #1: Configure Naming Context

- What does it fix?

```
# cn=Common,cn=Products,cn=OracleContext
orclSubscriberSearchBase: dc=com
orclSubscriberNickNameAttribute: dc
orclDefaultSubscriber: dc=example,dc=com

# cn=Common,cn=Products,cn=OracleContext,dc=example,dc=com
orclCommonUserSearchBase: ou=people,dc=example,dc=com
orclCommonGroupSearchBase: ou=groups,dc=example,dc=com
```

- Side note: Handled automatically since 11.1.2.3.161018 BP

Issue #2: No Subscriber found

- Let’s query the naming context we created.

```
$ ldapsearch -h localhost -p 1389 -D "cn=directory manager" -j /tmp/oud_pwd -b "dc=example,dc=com" -s one
"(objectclass=*)" "dn"
dn: cn=OracleContext,dc=example,dc=com

$
```

- Where is my naming context base entry?

```
$ ldapsearch -h localhost -p 1389 -D "cn=directory manager" -j /tmp/oud_pwd -b "dc=example,dc=com" -s base
"(objectclass=*)" "dn"
SEARCH operation failed
Result Code:  32 (No Such Entry)
Additional Information:  The entry dc=example,dc=com specified as the search base does not exist in the
Directory Server
$
```

Issue #2: No Subscriber found

- Fix: Manually create the Naming Context base DN as subscriber.

```
$ ldapmodify -h localhost -p 1389 -D "cn=directory manager" -j /tmp/oud_pwd –defaultAdd

dn: dc=example,dc=com
objectClass: top
objectClass: domain
objectclass: orclSubscriber
dc: example
orclversion: 90600
orclsubscriberfullname: example
aci: (targetattr != "userpassword || authpassword || aci") (version 3.0; acl "Anonymous read access to
dc=example, dc=com"; allow (read,search,compare) userdn = "ldap:///anyone";)
```

- Optional: Add read-only ACI permission for non-super-user access (except password attributes).

Issue #3: User and Group Base DNs

- Let’s query the naming context again.

```
$ ldapsearch -h localhost -p 1389 -D "cn=directory manager" -j /tmp/oud_pwd -b "dc=example,dc=com" -s one
"(objectclass=*)" "dn"
dn: cn=OracleContext,dc=example,dc=com

$
```

- Where are my user and group base DNs?

Issue #3: User and Group Base DNs

- Fix: Manually create the base DN entries.

```
$ ldapmodify -h localhost -p 1389 -D "cn=directory manager" -j /tmp/oud_pwd –defaultAdd

dn: ou=people,dc=example,dc=com
ou: people
objectClass: top
objectClass: organizationalUnit

dn: ou=groups,dc=example,dc=com
ou: groups
objectClass: top
objectClass: organizationalUnit
```

Issue #4: Write permissions for DIP profiles

- Documentation states that we need to apply these ACIs:

```
dn: dc=example,dc=com
changetype: modify
add: aci
aci: (target=" ldap:///dc=example,dc=com" )(version 3.0; acl "Entry-level DIP permissions"; allow
(all,proxy) groupdn=" ldap:///cn=odisgroup,cn=DIPadmins,cn=Directory Integration
platform,cn=Products,cn=oraclecontext"; allow (all,proxy) groupdn="
ldap:///cn=dipadmingrp,cn=DIPadmins,cn=Directory Integration Platform,cn=Products,cn=oraclecontext";)
-
add: aci
aci: (targetattr="*")(version 3.0; acl "Attribute-level DIP permissions"; allow (all,proxy) groupdn="
ldap:///cn=odisgroup,cn=DIPadmins,cn=Directory Integration Platform,cn=Products,cn=oraclecontext"; allow
(all,proxy) groupdn=" ldap:///cn=dipadmingrp,cn=DIPadmins,cn=Directory Integration
Platform,cn=Products,cn=oraclecontext";)
```

- But DIP runtime still fails on writes.

Issue #4: Write permissions for DIP profiles

- Fix: Add few more ACI permissions.
- DIP profiles are actually running with “odipgroup” App DN members.

```
dn: dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///dc=example,dc=com" )(version 3.0; acl "Entry-level DIP permissions"; allow (all,proxy)
groupdn=" ldap:///cn=odipgroup,cn=DIPadmins,cn=Directory Integration
platform,cn=Products,cn=oraclecontext";)
-
add: aci
aci: (targetattr="*")(version 3.0; acl "Attribute-level DIP permissions"; allow (all,proxy) groupdn="
ldap:///cn=odipgroup,cn=DIPadmins,cn=Directory Integration Platform,cn=Products,cn=oraclecontext";)
```

Issue #5: OUD restrictions on unindexed search

- There are limits when OUD allows non-super-user to do unindexed searches.
- None of OID specific attributes are indexed by default.

- Example: search per “orcguid” attribute filter.

```
[27/Apr/2016:01:25:45 -0700] SEARCH RES conn=381168 op=514 msgID=515 result=50 message="You do not have
sufficient privileges to perform an unindexed search  Operation 'SEARCH' failed in participant 'user' for
entry 'ou=people,dc=example,dc=com'  Operation 'SEARCH' failed in participant 'user' for entry
'ou=people,dc=example,dc=com'" nentries=0 authzDN="orclodipagentname=AD_DIP_PROFILE,cn=subscriber
profile,cn=changelog subscriber,cn=directory integration platform,cn=products,cn=OracleContext" etime=0
```

Issue #5: OUD restrictions on unindexed search

- Fix: Give a permission to your required non-super-user.
- For DIP – required for each subscriber app DN.
- Example:

```
$ ldapmodify -h localhost -p 1389 -D "cn=directory manager" -j /tmp/oud_pwd

dn: orclodipagentname=AD_DIP_PROFILE,cn=subscriber profile,cn=changelog subscriber,cn=directory integration
platform,cn=products,cn=OracleContext
changetype: modify
add: ds-privilege-name
ds-privilege-name: unindexed-search
-
add: ds-privilege-name
ds-privilege-name: proxied-auth
```

Issue #6: cn=changelog data timeout

- By default, purge delay for replication in OUD is set to 1 day.
- Set it to 1 week, at least.

```
$ dsconfig -h localhost -p 4461 -D "cn=directory manager" -w password -n get-replication-server-prop \
--provider-name "Multimaster Synchronization" --advanced --property replication-purge-delay
Property                : Value(s)
------------------------:---------
replication-purge-delay : 1 d
$ dsconfig -h localhost -p 4461 -D "cn=directory manager" -w password -n set-replication-server-prop \
--provider-name "Multimaster Synchronization" --set replication-purge-delay:1w
```

- Historical replication data retention also can be tuned.

```
$ dsconfig -h localhost -p 4461 -D "cn=directory manager" -w password -X -n \
set-replication-domain-prop --provider-name "Multimaster Synchronization" \
--domain-name dc=example,dc=com --set conflicts-historical-purge-delay:7200m
```

Issues faced while implementing OAM with OUD

Issue #1: EBS registration

- Test connection to identity server is failing.
- But network is fine, LDAP connection is working.

```
$ txkrun.pl -script=SetOAMReg -registeroam=yes -ldapProvider=OUD

...

Failed while doing policy configurations

In the log file this will be the only actual information.

<class>oracle.apps.fnd.txk.oam.UserIdentityStoreConf</class>
<message>Test connection to identity server is failed. Please verify the settings and try again.</message>

<class>oracle.apps.fnd.txk.oam.RegisterOAM</class>
<message>Failed while updating the configurations in OAM console</message>
```

Issue #1: EBS registration

- Only LDAP trace helped.

```
[25/Nov/2016:13:50:35 +0200] CONNECT conn=1939 from=10.10.10.187:13771 to=10.10.10.160:1389 protocol=LDAP...
[25/Nov/2016:13:50:35 +0200] UNBIND REQ conn=1939 op=1 msgID=2...
[25/Nov/2016:13:50:36 +0200] CONNECT conn=1940 from=10.10.10.160:63638 to=10.10.10.160:1389 protocol=LDAP...
[25/Nov/2016:13:50:36 +0200] SEARCH REQ conn=1940 op=1 msgID=2 base="ou=people,dc=example,dc=com" scope=sub
filter="(uid=*)" attrs="ALL"
[25/Nov/2016:13:50:36 +0200] SEARCH RES conn=1940 op=1 msgID=2 result=0 nentries=0 etime=1
[25/Nov/2016:13:50:36 +0200] SEARCH REQ conn=1940 op=2 msgID=3 base="ou=groups,dc=example,dc=com" scope=sub
filter="(cn=*)" attrs="cn"
[25/Nov/2016:13:50:36 +0200] SEARCH RES conn=1940 op=2 msgID=3 result=0 nentries=0 etime=0
```

Issue #1: EBS registration

- Fix: User Base DN and Group Base DN should have at least 1 user and 1 group created.
- In OID cn=orcladmin and cn=public are being seeded by default.

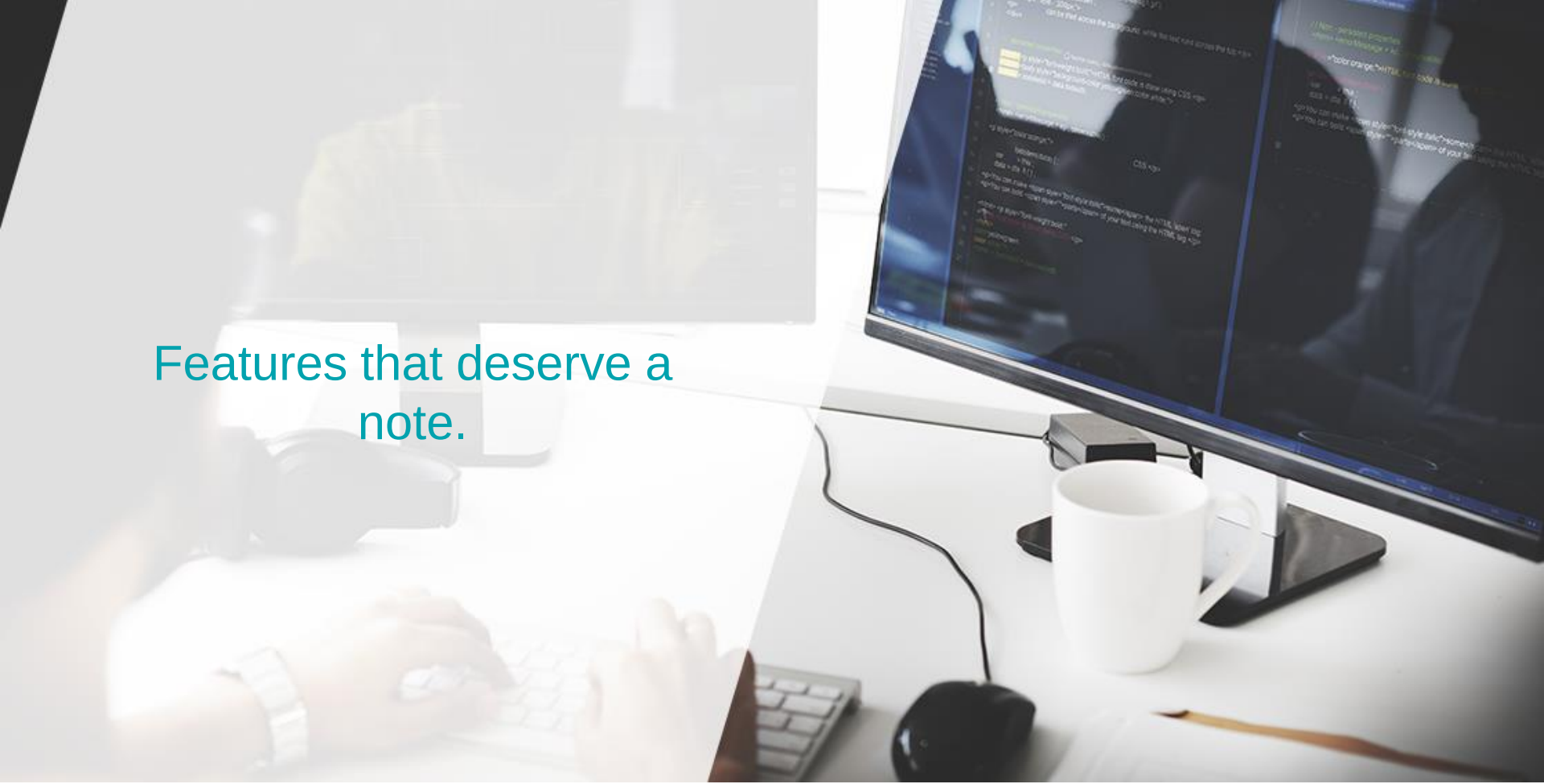
```
dn: cn=testuser1,ou=people,dc=example,dc=com
objectClass: person
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: top
givenName: John
sn: Testercn: testuser1
uid: testuser1
userpassword: welcome1
mail: test@test.com

dn: cn=admins,ou=groups,dc=example,dc=com
objectClass: groupOfNames
objectClass: top
cn: testgroup
```

Issue #2: Configuration of the User Identity Store

- Not an issue, actually. More a recommendation.

- These parameters are not set by default.
  - User Filter Object Classes: person
  - Group Name Attribute: cn
  - Group Filter Classes: groupofnames
  - Inactivity Timeout (in seconds): 60



Features that deserve a note.

SSL

- RIP SSL no-auth mode

- Only SSL server or client-server authentication.
- JSSE - Java Secure Socket Extension.

- And this is good !

- Default keystore: $ORACLE_INSTANCE/OUD/config/keystore

SSL - small comment about DIP

- By default, DIP is configured with non-SSL.

- SSL only mode is required if passwords are provisioned from external directories.
- Requires a JKS keystore configuration with OUD server certificate imported.

```
$ keytool -importcert -trustcacerts -alias OUD -file /tmp/oud_server_certificate_b64.txt -keystore
$ORACLE_INSTANCE/config/DIP_JKS/dip.jks

$ wlst.sh
> connect('t3://localhost:7001')
> createCred(map="dip", key="jksKey", user="jksuser", password="changeit")

$ $ORACLE_HOME/bin/manageDIPServerConfig set -h localhost -p 7005 -D weblogic -attribute keystorelocation -
val /u01/app/oracle/product/fmw11g/dip_inst1/config/DIP_JKS/dip.jks
$ $ORACLE_HOME/bin/manageDIPServerConfig set -attribute sslmode -val 2 -h localhost -p 7005 -D weblogic
$ $ORACLE_HOME/bin/manageDIPServerConfig set -attribute backendhostport -val localhost:1636 -h localhost -p
7005 -D weblogic
```

External password plugins in OUD

- Use case: Active Directory – passwords are not directly synced by DIP.
- OID has a cool feature – external password plugin.
  - Java based module which forwards the BIND requests to external LDAP directories for authentication.
- OUD does not have these kind of modules, however there are alternatives.
  - Pass Through Authentication (OUD 11.1.2.2+)
  - On-Demand Password and Password Translate (OUD 11.1.2.3+)
  - OUD / DIP Synchronization with Active Directory (Doc ID 1534241.1)

Pass Through Authentication

- How it works: Proxy mode workflow.
- You have your Local Naming Context “dc=example,dc=com” with synced user entries by DIP (no userpassword / orclpassword attributes).
- New Proxy Workflow is configured to mount external LDAP Base DN.
- A Workflow Element will merge both sources and use local context as user provider and external proxy context as authentication provider.

Pass Through Authentication

- Configure OUD LDAP extension.

```
$ dsconfig -h localhost -p 4461 -D "cn=directory manager" -j /tmp/oud_pwd -X -n create-extension \
--type ldap-server \
--extension-name proxy_extension_pta_ext_ldap \
--set remote-ldap-server-read-only:true \
--set remote-ldap-server-address:myad.example.com \
--set remote-ldap-server-port:389  \
--set remote-ldap-server-ssl-port:636 \
--set remote-ldap-server-ssl-policy:always \
--set ssl-trust-all:true \
--set ssl-trust-manager-provider:JKS \
--set enabled:true
```

Pass Through Authentication

- Configure OUD Proxy Workflow elements.

```
$ dsconfig -h localhost -p 4461 -D "cn=directory manager" -j /tmp/oud_pwd -X -n create-workflow-element \
--set client-cred-mode:use-specific-identity \
--set enabled:true --set ldap-server-extension:proxy_extension_pta_ext_ldap \
--set remote-ldap-server-bind-dn:cn=system_user,ou=ad_system_accounts,dc=example,dc=com \
--set remote-ldap-server-bind-password:password \
--set remote-root-dn:cn=system_user,ou=system_accounts,dc=ad,dc=example,dc=com \
--set remote-root-password:password \
--type proxy-ldap \
--element-name wf_element_auth_pta_ext_ldap

$ dsconfig -h localhost -p 4461 -D "cn=directory manager" -j /tmp/oud_pwd -X -n create-workflow-element \
--set auth-provider-workflow-element:wf_element_auth_pta_ext_ldap \
--set enabled:true --set user-provider-workflow-element:userRoot \ # our default naming context created
--set pta-suffix:ou=people,dc=example,dc=com \
--set pta-auth-suffix:ou=people,dc=example,dc=com \
--set pta-user-suffix:ou=people,dc=example,dc=com \
--type pass-through-authentication \
--element-name wf_element_pta_ext_ldap
```

Pass Through Authentication

- Configure OUD Proxy Workflow.

```
$ dsconfig -h localhost -p 4461 -D "cn=directory manager" -j /tmp/oud_pwd -X -n create-workflow \
--workflow-name pta_ext_ldap_wf \
--set base-dn:ou=people,dc=example,dc=com \
--set enabled:true \
--set workflow-element:wf_element_pta_ext_ldap
```

- Enable the new configuration.

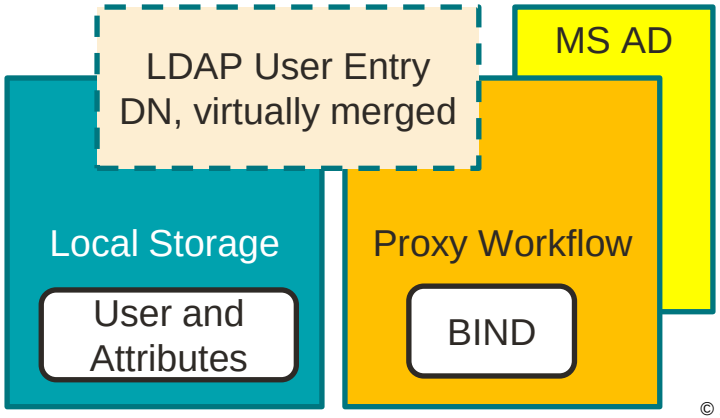
```
$ dsconfig -h localhost -p 4461 -D "cn=directory manager" -j /tmp/oud_pwd -X  -n set-network-group-prop \
--group-name network-group \
--set enabled:true \
--add workflow:pta_google_openldap_wf
```

Pass Through Authentication

- It works.

```
$ ldapsearch -h localhost -p 1389 -D "cn=user1,ou=people,dc=example,dc=com" -b
"cn=user1,ou=people,dc=example,dc=com" -s base "(objectclass=*)" "orclSourceObjectDN"
Password for user 'cn=user1,ou=people,dc=example,dc=com':
dn: cn=user1,ou=people,dc=example,dc=com
orclSourceObjectDN: cn=user1,ou=People,dc=example,dc=com
$
```

- Some illustration.



OUD Access Log

- OUD has access log tracing similar to Apache.
- It tracks everything and YOU SHOULD LOVE IT!

- $ORACLE_INSTANCE/OUD/logs/access

```
[25/Nov/2016:13:50:35 +0200] CONNECT conn=1939 from=10.10.10.187:13771 to=10.10.10.160:1389 protocol=LDAP
[25/Nov/2016:13:50:35 +0200] BIND REQ conn=1939 op=0 msgID=1 type=SIMPLE dn="cn=directory manager" version=3
[25/Nov/2016:13:50:35 +0200] BIND RES conn=1939 op=0 msgID=1 result=0 authDN="cn=Directory Manager,cn=Root
DNs,cn=config" etime=1
[25/Nov/2016:13:50:35 +0200] UNBIND REQ conn=1939 op=1 msgID=2
[25/Nov/2016:13:50:35 +0200] DISCONNECT conn=1939 reason="Client Disconnect”
[25/Nov/2016:13:50:36 +0200] CONNECT conn=1940 from=10.10.10.160:63638 to=10.10.10.160:1389 protocol=LDAP
[25/Nov/2016:13:50:36 +0200] BIND REQ conn=1940 op=0 msgID=1 type=SIMPLE dn="cn=directory manager" version=3
[25/Nov/2016:13:50:36 +0200] BIND RES conn=1940 op=0 msgID=1 result=0 authDN="cn=Directory Manager,cn=Root
DNs,cn=config" etime=0
[25/Nov/2016:13:50:36 +0200] SEARCH REQ conn=1940 op=1 msgID=2 base="ou=people,dc=domain,dc=com" scope=sub
filter="(uid=*)" attrs="ALL”
[25/Nov/2016:13:50:36 +0200] SEARCH RES conn=1940 op=1 msgID=2 result=0 nentries=0 etime=1
[25/Nov/2016:13:50:36 +0200] SEARCH REQ conn=1940 op=2 msgID=3 base="ou=groups,dc=domain,dc=com" scope=sub
filter="(cn=*)" attrs="cn”
[25/Nov/2016:13:50:36 +0200] SEARCH RES conn=1940 op=2 msgID=3 result=0 nentries=0 etime=0
```

Virtual Attributes

- An attribute which is more like a function.
- The best example: isMemberOf
  - Is true if a user is a member of a defined group
  - The most useful place to use: LDAP filters

- Example: OAM User Identity Store filter to allow only specific group to access your application.
  - KEY_LDAP_FILTER: (&(uid={KEY_USERNAME})(isMemberOf=cn=ebs_sso_allowed_users,ou=groups,dc=example,dc=com))

Performance tuning considerations

Overview

- Performance is a feature. ☺
- Overall the OUD performance is good.

- The more memory you configure – the more you get into the cache.

- Always try to apply the latest PSU BP. Many performance related bugs are resolved per the change log in every bundle.

- Some real problems to look at may start only when your data size exceeds hundreds of thousands, like 400 000 user accounts.

Indexes

- OUD is not indexing by default most of the common OID attributes.
- Example: DIP ApplicationToOID profile is doing Root DN sub-search looking for entries with required orclGUID, to confirm it exists.
  - With large directories it can spin the CPU a lot. Can be indexed.

```
$ dsconfig -h localhost -p 4461 -D "cn=directory manager" -j /tmp/oud_pwd -X -n create-local-db-index --
element-name userRoot --index-name orclguid --set index-type:equality
$ rebuild-index -h localhost -p 4461 -D "cn=directory manager" -j /tmp/oud_pwd -X -b "dc=example,dc=com" -
i orclguid
```

- If DIP bootstrap has synchronized a huge amount of new user accounts (ex from external directory) – full index rebuild is highly recommended.

```
$ rebuild-index -b "dc=example,dc=com" --rebuildAll
```

Root DN based search

- Same use case: DIP ApplicationToOID

```
$ ldapsearch -h localhost -p 1389 -D "cn=directory manager" -j /tmp/oud_pwd -b ""
"(orclguid=XXXXXXXXXXXXXXXXXXXXX)" "*"
```

- OUD will also look into “cn=changelog” as it interprets it as non-hidden naming context.
- This is how OUD works.
- Recommendation: evaluate the data size, and put the memory enough to cache as maximum as possible.
  - https://blogs.oracle.com/sduloutr/entry/oud_external_change_log_and
  - OUD - Bad Performance of a Subtree Search on the Root DSE if the External Changelog is Enabled. (Doc ID 1676998.1)
- With PTA add here your external Proxy Workflow Element as well.

Data cache tuning

- If your LDAP data is 1 GB in size, you can configure your OUD instance to 2 GB memory and set data cache to utilize 50 %.

```
$ dsconfig -h localhost -p 4461 -D "cn=directory manager" -w password set-workflow-element-prop --element-name userRoot --set db-cache-percent:50
```

- Cache as much as possible **!!!**

Summary

- OUD is an interesting lightweight product.
- Hard to say if it’s better or worse than OID. Both OUD and OID have their own pros and cons.
- OUD – is a replacement product. OID is going away soon (Dec 2018 / Dec 2021).
- Comparing to 11gR1, where OUD was not usable at all for all main integration use cases, it is now more less ready. Of course, with some nuances mentioned.
- Simplified setup and configuration.
- It takes time to tune everything. Let us be patient. There is a potential.

THANK YOU

Q & A