

OU LDAP bevezetés OS és DB szinten telekommunikációs környezetben


Víg Pál

Senior rendszermérnök

Kóródi Ferenc

Senior adatbázis konzultáns

Budapest, 2018-11-13



Tartalomjegyzék

- Jelenlegi környezet és felhasználás
- Oracle Unified Directory
- OUD implementáció
- Kihívások
- Jövőbeli lehetőségek

Jelenlegi környezet


- Vállalati környezet
- Szerver környezet
 - Linux
 - Solaris
 - Oracle Database
 - DMZ
- Felhasználók száma

Jelenlegi környezet

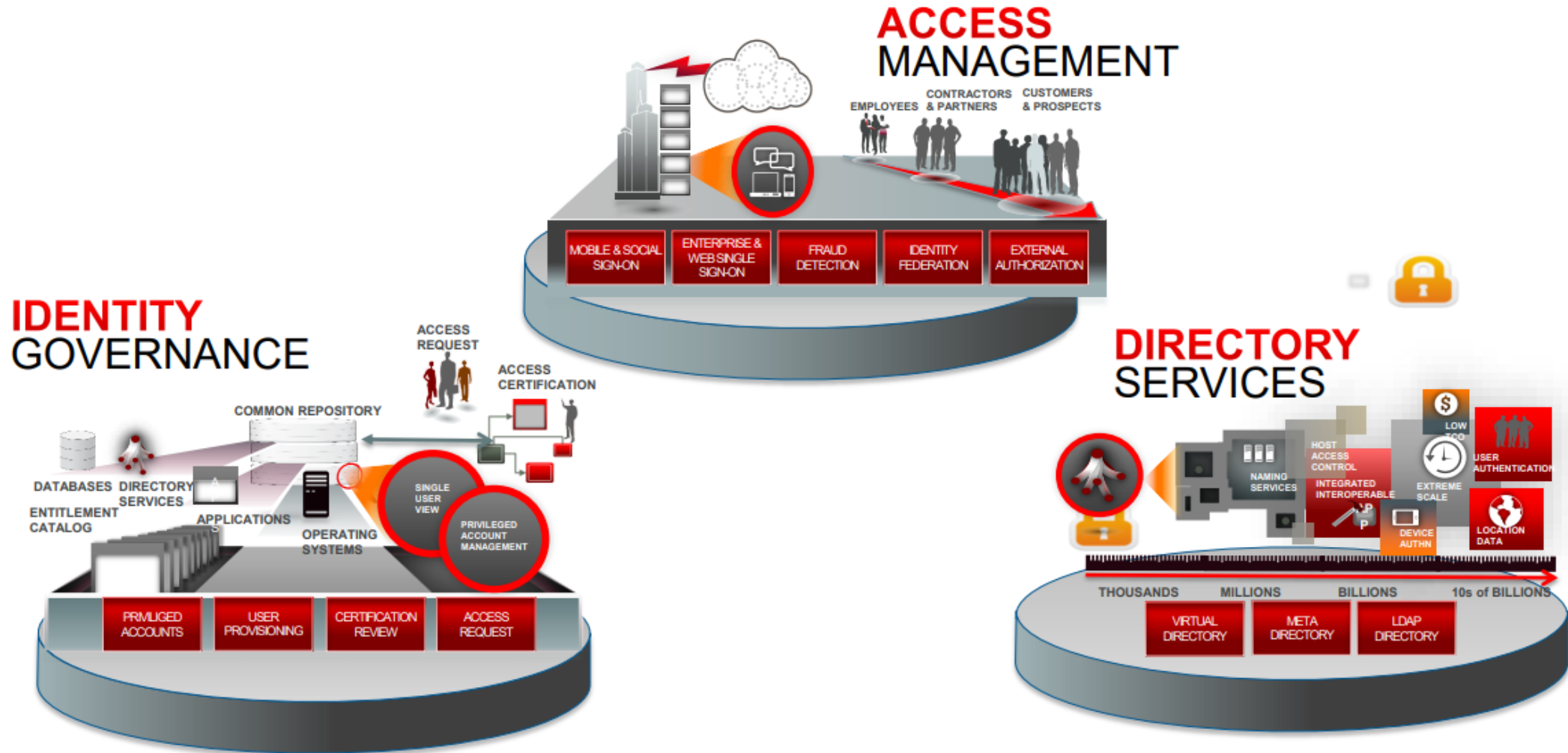
- Oracle Directory Server Enterprise Edition
 - Üzemeltetési problémák
 - Adminisztrációs nehézségek
- Sudo szabályok és script-ek
- ACL szabályok




Jelenlegi környezet

- Megvalósítandó feladatok:
 - Linux és Solaris OS szintű autentikáció és autorizáció
 - Linux és Solaris sudo jogosultság központosított menedzsment
 - Oracle Database autentikáció és opcionálisan autorizáció
 - High Availability megvalósítás
 - Security feltételeknek megfelelés
 - Felhasználók egységes forrása a központi Microsoft Active Directory
- 

Oracle Unified Directory



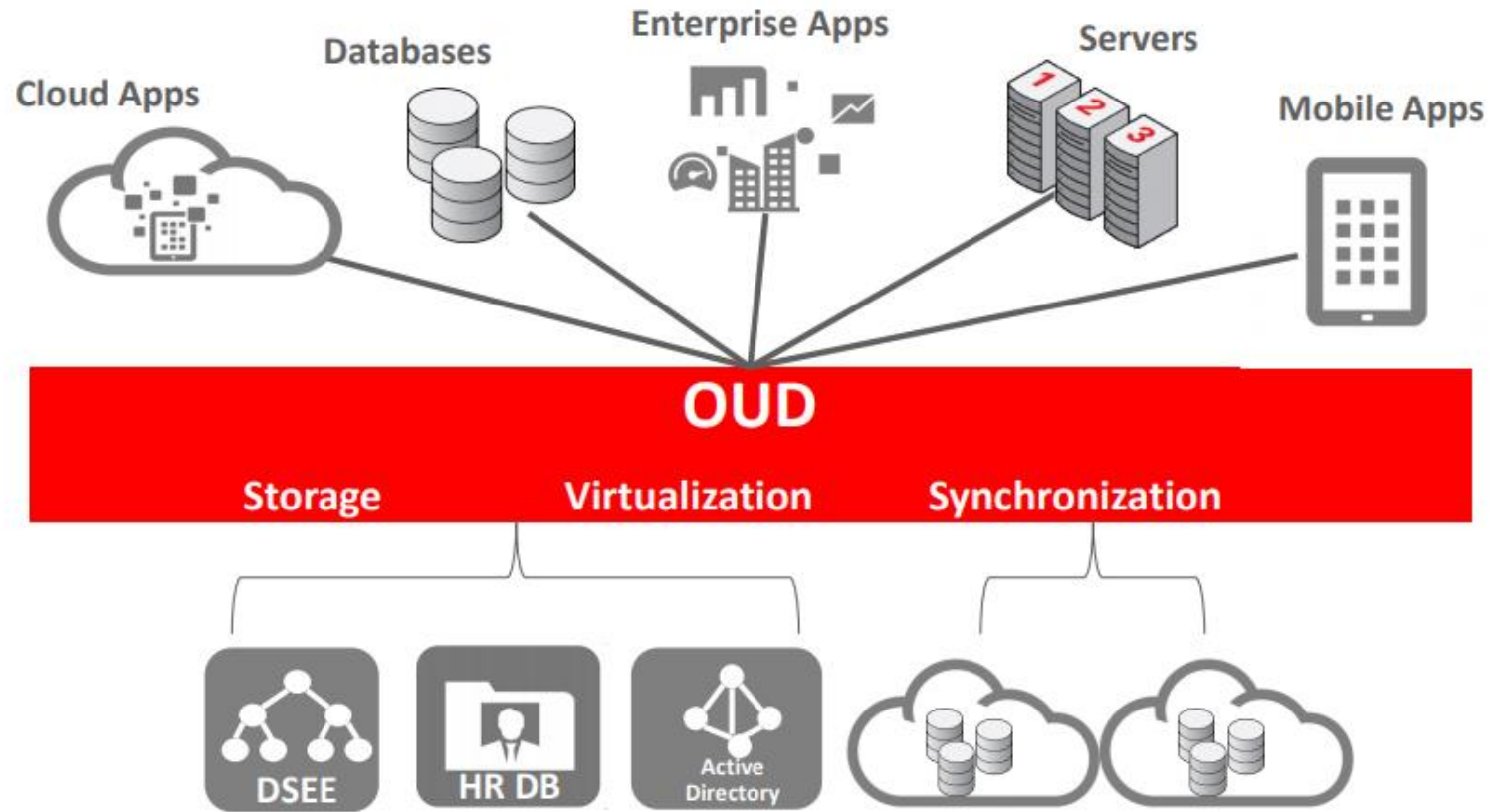
Oracle Unified Directory

- ODSEE és OID utóda
 - Java alkalmazás (11g - JDK7 és 12c - JDK8)
 - BerkleyDB
 - ODSM/OUDSM WebLogic alkalmazás - menedzsment
 - LDAP szerver funkcionalitás
 - Oracle környezet szinergiái
 - Enterprise User Security
- 

Oracle Unified Directory

■ OUD szerepkörök

- Directory
- Proxy
- Replication

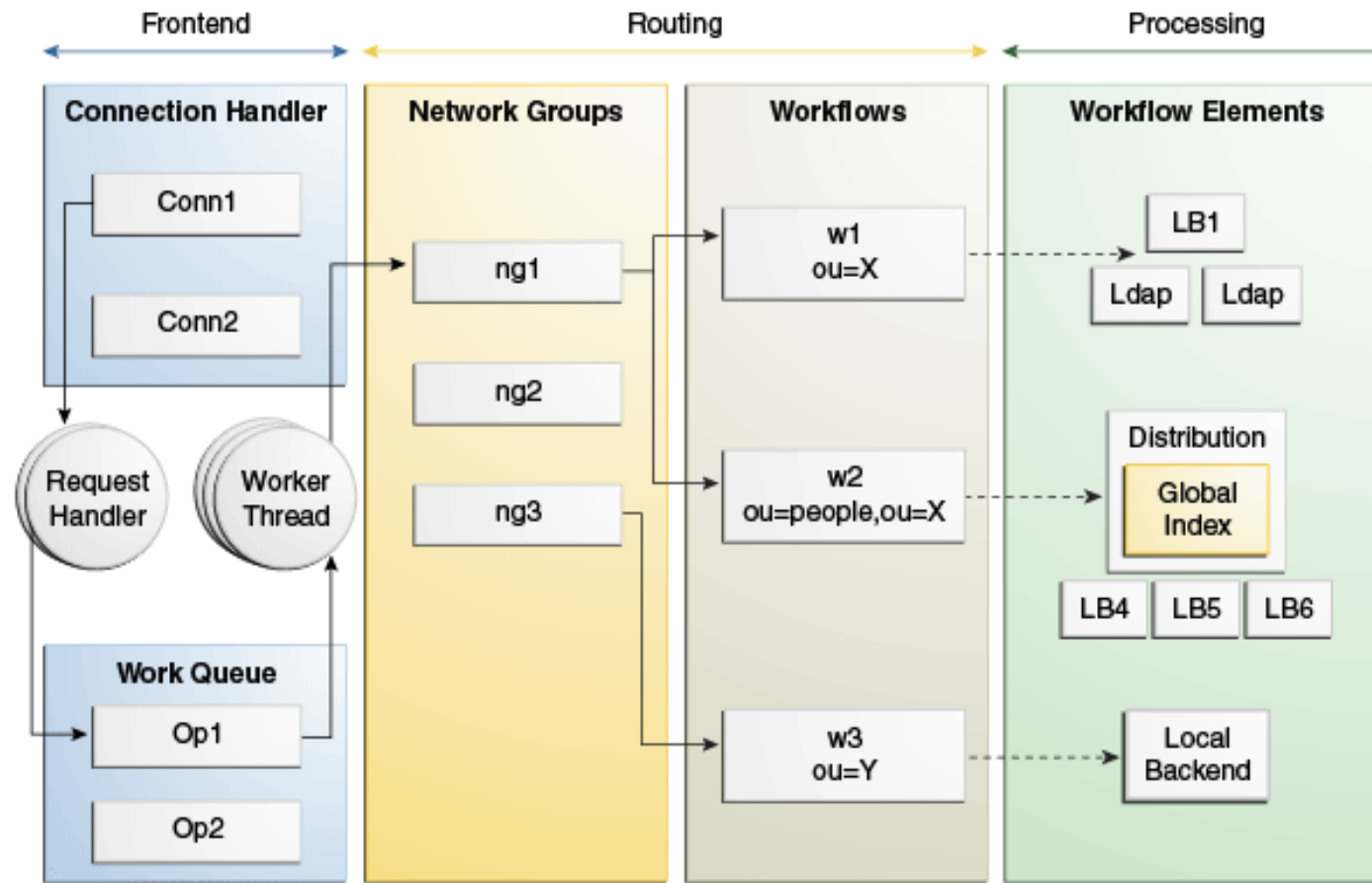


OU D - megvalósítás

- LDAP séma felépítése
 - Objectclass és Attributes
- LDAP séma bővítése
 - Egyéni célok → Sudo objektumok

```
objectClass: subschema
cn: schema
attributetypes: ( 1.3.6.1.4.1.15953.9.1.1 NAME 'sudoUser' DESC 'User(s) who may run sudo' EQUALITY caseI
attributetypes: ( 1.3.6.1.4.1.15953.9.1.2 NAME 'sudoHost' DESC 'Host(s) who may run sudo' EQUALITY caseI
attributetypes: ( 1.3.6.1.4.1.15953.9.1.3 NAME 'sudoCommand' DESC 'Command(s) to be executed by sudo' EQ
attributetypes: ( 1.3.6.1.4.1.15953.9.1.4 NAME 'sudoRunAs' DESC 'User(s) impersonated by sudo' EQUALITY
attributetypes: ( 1.3.6.1.4.1.15953.9.1.5 NAME 'sudoOption' DESC 'Options(s) followed by sudo' EQUALITY
attributetypes: ( 1.3.6.1.4.1.15953.9.1.6 NAME 'sudoRunAsUser' DESC 'User(s) impersonated by sudo' EQUAL
attributetypes: ( 1.3.6.1.4.1.15953.9.1.7 NAME 'sudoRunAsGroup' DESC 'Group(s) impersonated by sudo' EQU
objectclasses: ( 1.3.6.1.4.1.15953.9.2.1 NAME 'sudoRole' SUP top STRUCTURAL DESC 'Sudoer Entries' MUST
```

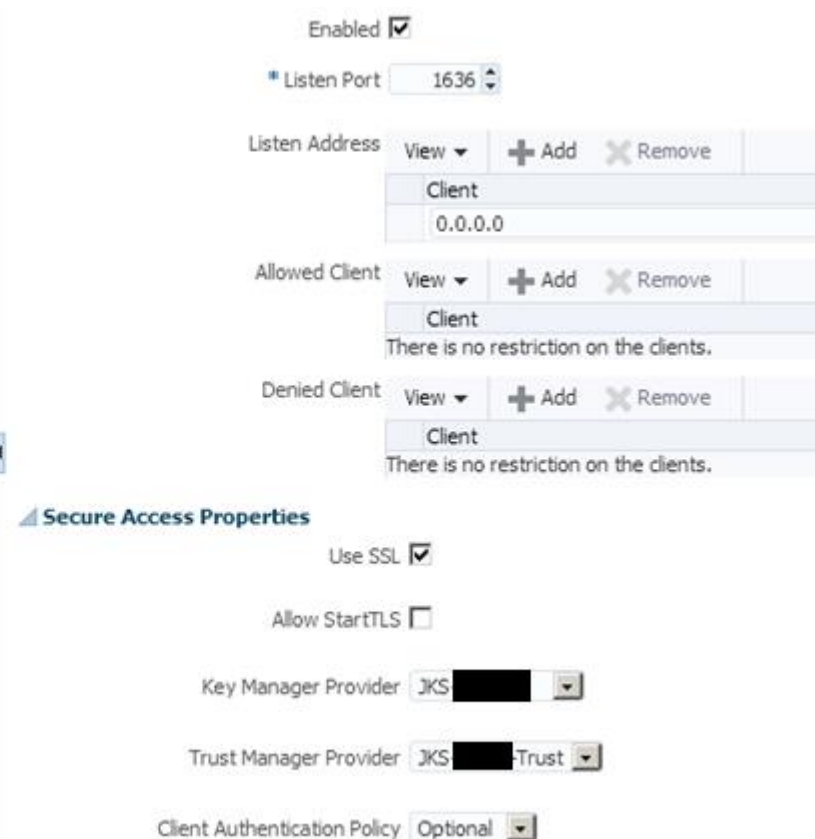
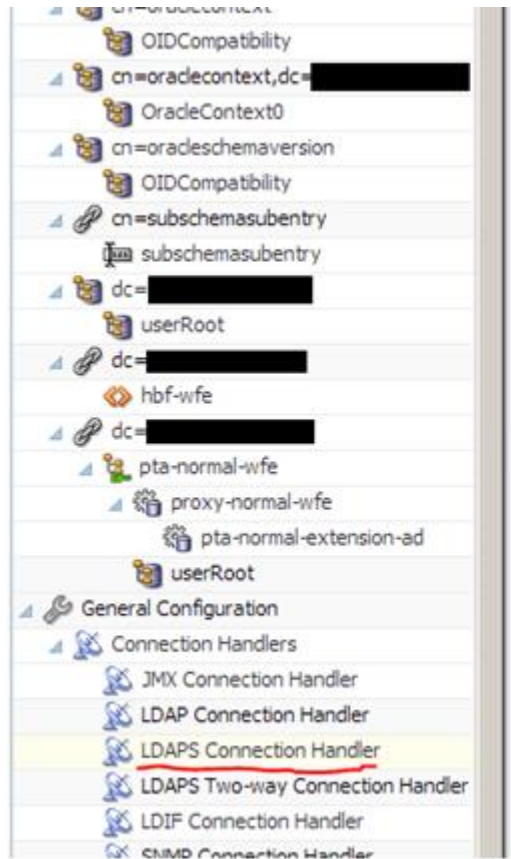
OOD - megvalósítás



OID - megvalósítás

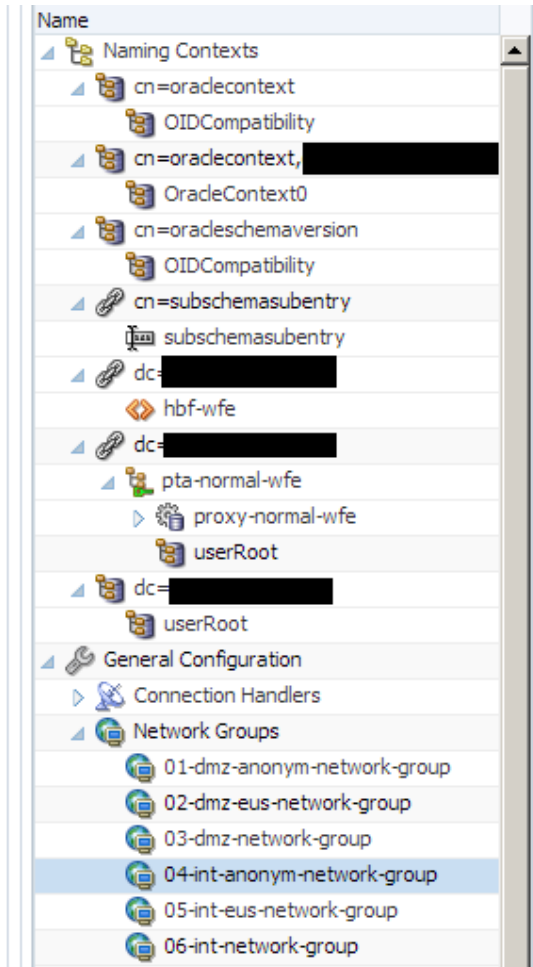
■ Connection Handlers

- Portok
- SSL



OOD - megvalósítás

- Network Groups
 - Funkcionalitás
 - Workflow-k



Basic Properties

Name 04-int-anonym-network-group

Enabled

* Priority 3

Workflow View

Name

OracleContext0

Root DSE to Expose Local Root DSE

Criteria

Security Mandatory

Allowed Auth Method Anonymous Sasl Simple

Allowed Protocol LDAP LDAPS

Allowed Bind DN View

DN

All bind DN's are allowed.

Allowed Client View

Address

All clients with addresses that do not match an address on the d

Denied Client View

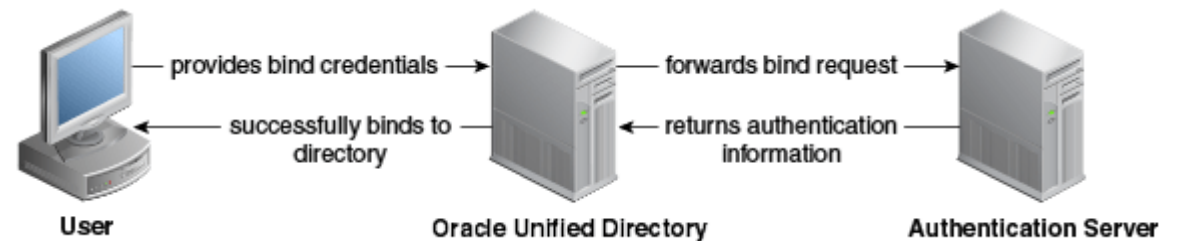
Address

172.21.71.*

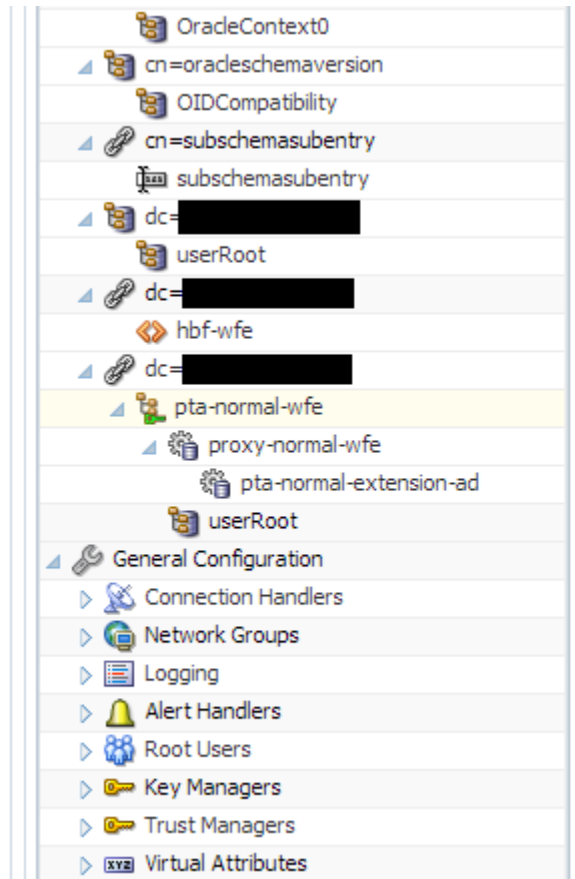
Qos Policy

ODU - megvalósítás

- Workflow-k és Workflow Element-ek
 - Pass Trough Authentication workflow element
 - Hide Entries by Filter workflow element
- Extensions
 - Microsoft Active Directory



OID - megvalósítás



Name pta-normal-wfe
Enabled

* User Provider Workflow Element userRoot

* Authentication Provider Workflow Element proxy-normal-wfe

Advanced Properties

Password Attribute userpassword

Save Password on successful bind

Pass Through Authentication Suffix ou=People,dc=example,dc=com

User Suffix ou=People,dc=example,dc=com

Authentication Suffix OU=Users,OU=HU,DC=internal,DC=exi

Pass Through Authentication Join Rule

Specify how an Auth entry associates with a User entry, by choosing an Auth entry property to map to a User entry property.

Auth Entry Property DN Attribute samaccountname

User Entry Property DN Attribute uid

OUD - megvalósítás

- ACL szabályok

- Kinek / mihez / milyen jogosultsága van

- Speciális jogosultságok

- DNS

- Attribútum

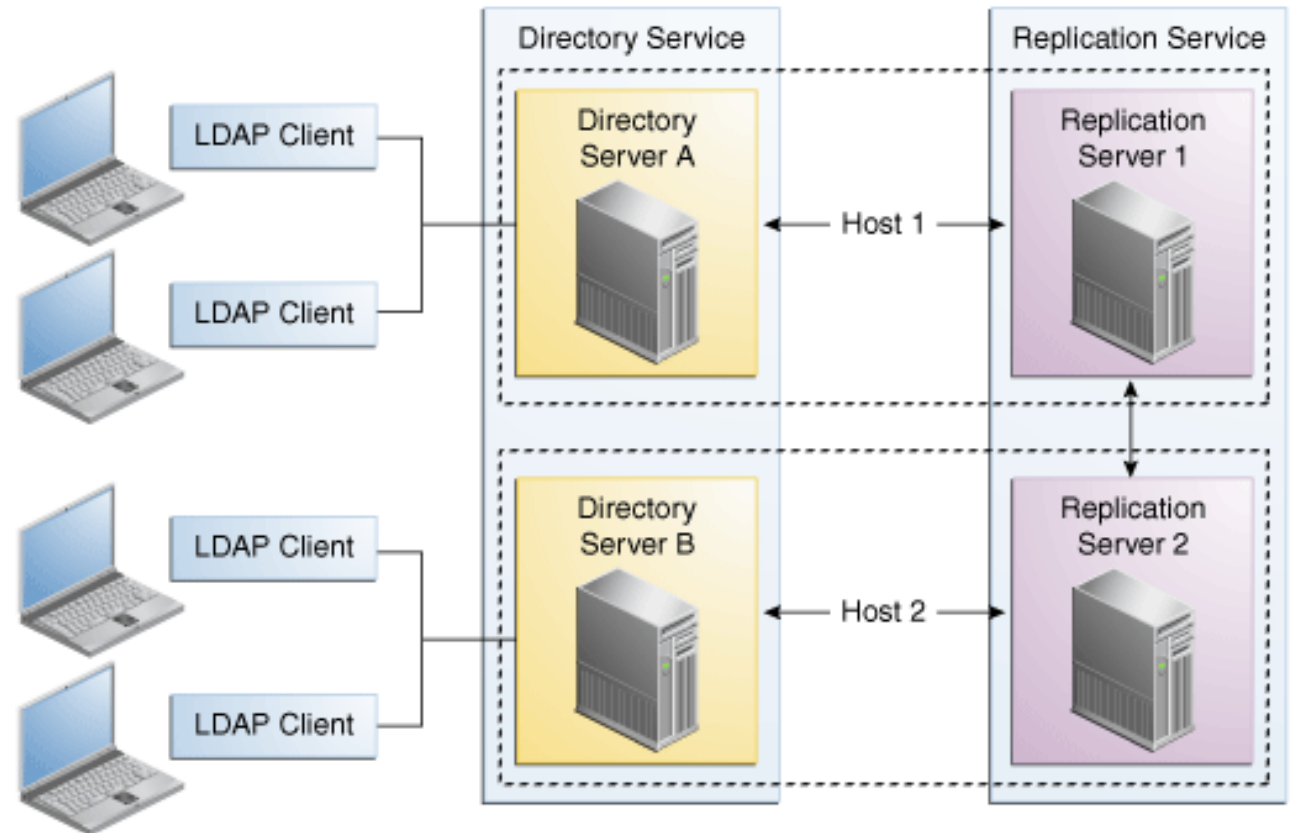
- Time of day

```
(target = "ldap:///uid=pal.vig,ou=People,dc=example,dc=com") (targetattr = "host") (targetscope = "base") (version 3.0; acl "UNIX Read pal.vig scope host1"; allow (read,search) (userdn = "ldap:///cn=tech_user,ou=TechUsers,dc=example,dc=com" and dn = "host1.example.com");)
```

OOD - megvalósítás

■ Replikáció

- Multi-master replikáció
- dc=example,dc=com
- cn=OracleContext,dc=...



OS - megvalósítás

- Linux - sssd.conf
- Solaris - ldapclient

```
sssd  
sssd-common  
sssd-common-pac  
sssd-ldap  
sssd-tools  
sssd-client  
sssd-proxy
```


```
[domain/default]  
  
enumerate = True  
autofs_provider = ldap  
ldap_search_base = dc=example,dc=com  
id_provider = ldap  
auth_provider = ldap  
access_provider = ldap  
sudo_provider = ldap  
ldap_tls_cacertdir = /etc/openldap/cacerts  
ldap_search_base = dc=example,dc=com  
ldap_schema = rfc2307bis  
ldap_tls_reqcert = never  
  
ldap_uri = ldaps://oudprod1:636/  
ldap_backup_uri = ldaps://oudprod2:636/  
  
ldap_default_bind_dn = cn=tech_user,ou=TechUsers,dc=example,dc=com  
ldap_default_authtok = AAAQXAMdWE4BZ1Dnpj/aejFtiKCii+6dEC1bBo5D+  
ldap_default_authtok_type = obfuscated_password  
  
ldap_user_search_base = ou=People,dc=example,dc=com?sub?host=itdevcrepol  
ldap_group_search_base = ou=Groups,dc=example,dc=com  
ldap_sudo_search_base = ou=Sudoers,dc=example,dc=com  
  
ldap_sudo_full_refresh_interval = 60  
ldap_sudo_smart_refresh_interval = 60  
  
cache_credentials = False  
ldap_access_filter = isMemberOf=cn=SystemSupportUnix,ou=Groups,dc=example,dc=com  
filter_users = root, admin
```

OS - megvalósítás

- Solaris megvalósítás natív ldapclient segítségével
 - Egyéb konfiguráció: pam.conf, ldap.conf, nsswitch

```
ldapclient -v manual \  
-a defaultServerList=oudprod1:636,oudprod2:636 \  
-a bindTimeLimit=5 \  
-a authenticationMethod=simple:tls \  
-a credentialLevel=proxy \  
-a proxydn=cn=tech_user_os,ou=TechUsers,dc=example,dc=com \  
-a proxypassword=XXX \  
-a defaultSearchBase=dc=example,dc=com \  
-a defaultSearchScope=sub \  
-a "serviceSearchDescriptor=group:ou=Groups,dc=example,dc=com" \  
-a "serviceSearchDescriptor=shadow:ou=People,dc=example,dc=com?sub?objectClass=shadowAccount" \  
-a "serviceSearchDescriptor=passwd:ou=People,dc=example,dc=com?sub?(&(objectClass=posixAccount)(ismemberof=cn=SolarisGroup,cn=OperatingSystems,ou=Groups,dc=example,dc=com)(host=soltst11))"
```

OS - Sudo és ACL keretrendszer

 cn=rule1

Distinguished Name cn=rule1,ou=Sudoers,dc=

Created by cn=admin

Modified by cn=admin


Created at September 18, 2017 9:39:13 PM CEST



Modified at November 12, 2018 1:13:22 PM CET

Attributes

▲ Mandatory Attributes

Object Class  Add  Delete

Name
top 
sudoRole 

cn  Add  Delete

Value
rule1

▲ Optional Attributes

sudohost  Add  Delete

Value
ldapcdev1


sudorunas  Add  Delete

Value
ALL

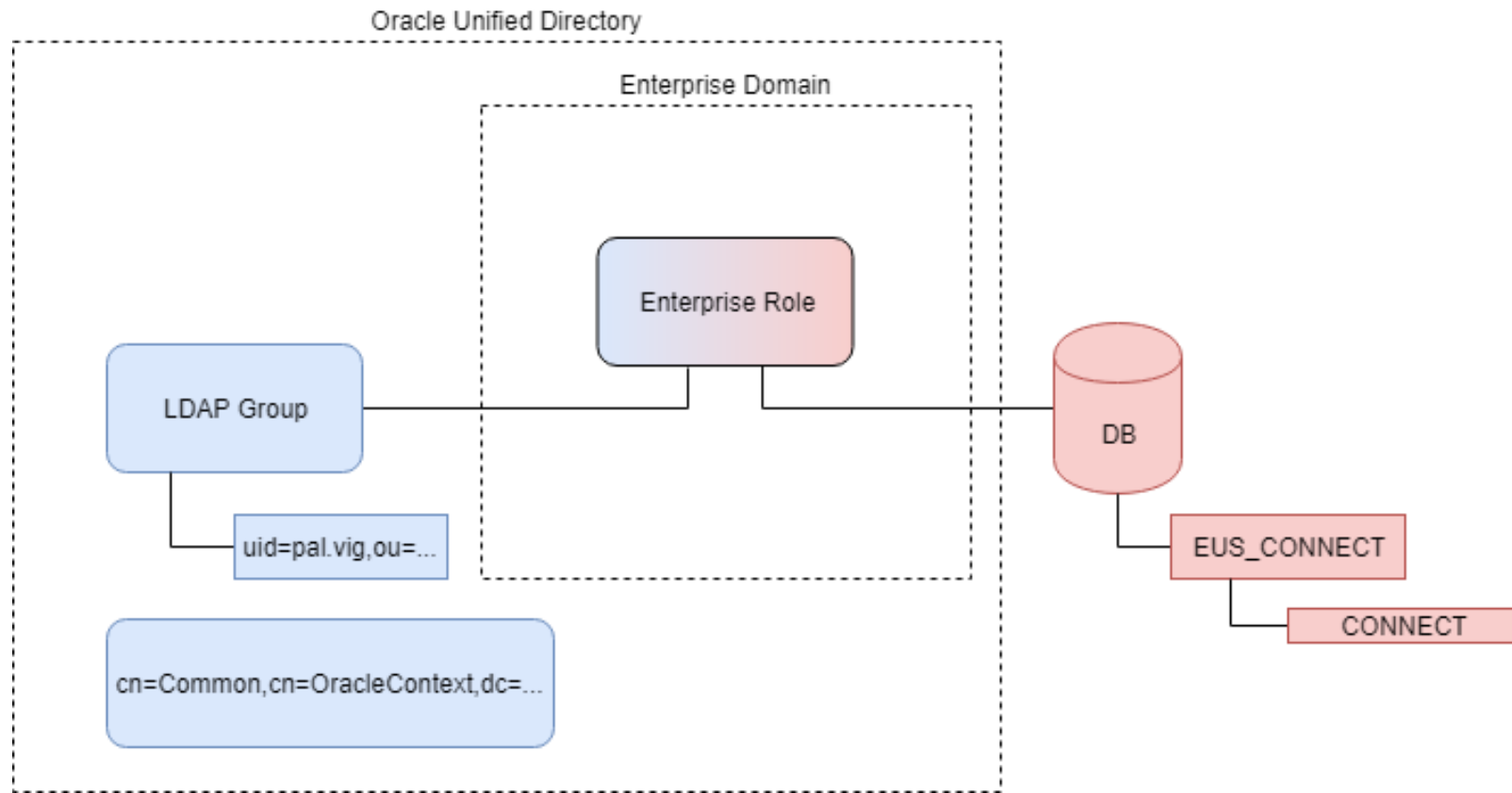
sudouser  Add  Delete

Value
%group1
pal.vig

EUS - megvalósítás

- DB regisztráció
 - dbca
 - Wallet konfiguráció
 - orapki
 - Enterprise Domian-ek és Role-ok létrehozása
 - eusm
 - DB konfiguráció
 - ldap_directory_access='SSL'
 - alter user pal_vig identified globally as 'uid=pal.vig,ou=People,dc=...';
- 

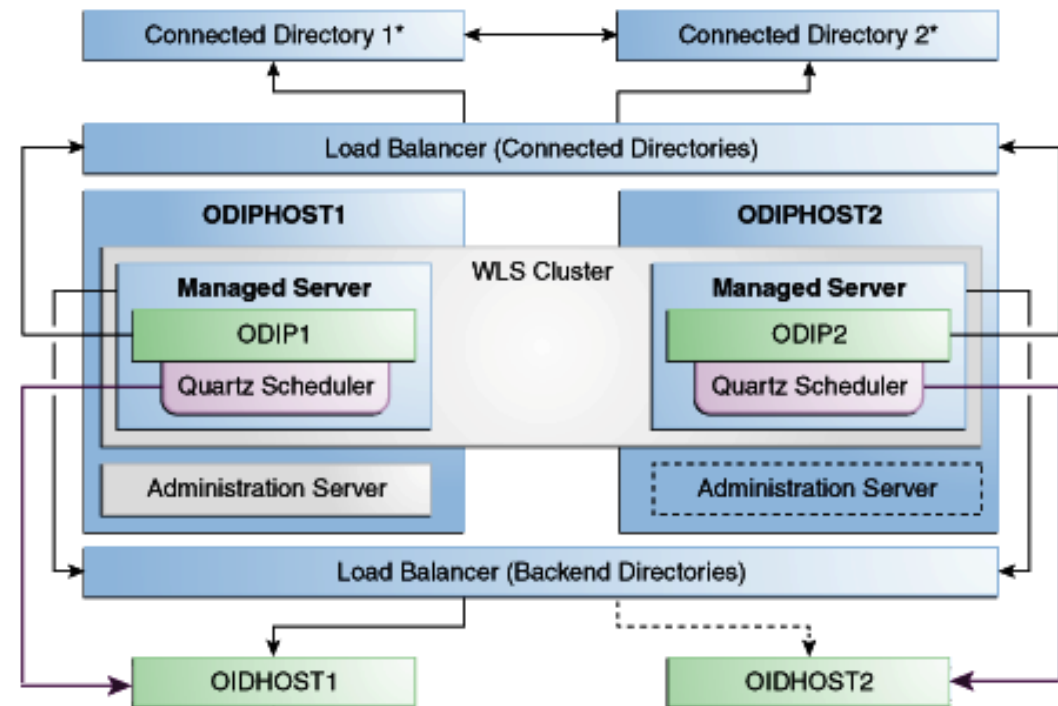
EUS - autorizáció



Adatszinkronizáció

■ Directory Integration Platform

- HA és SSL konfiguráció
- Synchronization Profile
 - Domain rules
 - Attribute rules
 - Filtering



Adatszinkronizáció

DIP(11.1.1.2.0)

DIP Server ▾

DIP Server > Synchronization Profiles >

Edit Synchronization Profile - profile_users

General **Mapping** Filtering Advanced

Source Container	DIP-OU Container	DN Mapping Rule
cn=████████,cn=users,dc=example,...	cn=users,dc=████████	uid=%,cn=users,dc=████████

Columns Hidden 1

Attribute Mapping Rules

Create... Edit... Delete...

View ▾

Source Container			DIP-OU Container		
ObjectClass	Attribute(s)	Attribute Required	ObjectClass	Attribute	Attribute Mapping Expression
container	cn		orclContainer	cn	
domain	dc		domain	dc	
person	usncreated		posixaccount	loginshell	"/bin/bash"
person	usncreated		posixaccount	gidnumber	"5001"
person	cn		person	cn	
person	cn		account	description	
person	usncreated		posixaccount	homedirectory	"/export/home"
top	distinguishedname		orclADObject	orclSourceObjectDN	
user	useraccountcontrol	✓	top	ds-pwp-account-disabled	AccountDisable(userAccountControl)
user	samaccountname		person	sn	
user	samaccountname		inetorgperson	uid	

Kihívások

- DMZ - Internal sík szétválasztása
- EUS - PTA autentikáció
- uidnumber attribútum töltése



Köszönjük a figyelmet!

