talanx.
Systeme

Fun with OUD

Nürnberg 17.11.2016

Die Talanx Systeme ist an den Standorten Hannover, Köln, Hamburg und Hilden vertreten

Standorte

Hannover (Zentrale)
~ 550 Mitarbeiter

Köln
~ 300 Mitarbeiter

Hamburg
~ 80 Mitarbeiter

Hilden
~ 80 Mitarbeiter

Historie

Oracle Unified Directory (OUD)

- Basis OpenDS
- opends von Sun Mircosysten (2005)
- Kommerzielle Versions (Sun OpenDS Standard Edition) seit 2008
- OpenDS open Source Project
  - Neuste Version 3.5
- Weiterentwicklung OpenDS → OUD
- Strategisches Produkt
- Integration von anderen Produkte

Möglichkeiten

- Identification und Access Management
  - Cloud
    - IAAS
  - Internet
  - Intranet
  - Mobile
    - Provider
  - Applikationen
  - Datenbanken
    - **EUS**
- Konsolidierung von Directory Services
- Virtualisierung

Tipp:
Thema **EUS / OUD**
Vortrag Stefan Oehrli (Trivadis)

http://www.oradba.ch/download/DOAG__EUS_mit_OUD_Oehrli.pdf

talanx. Systeme

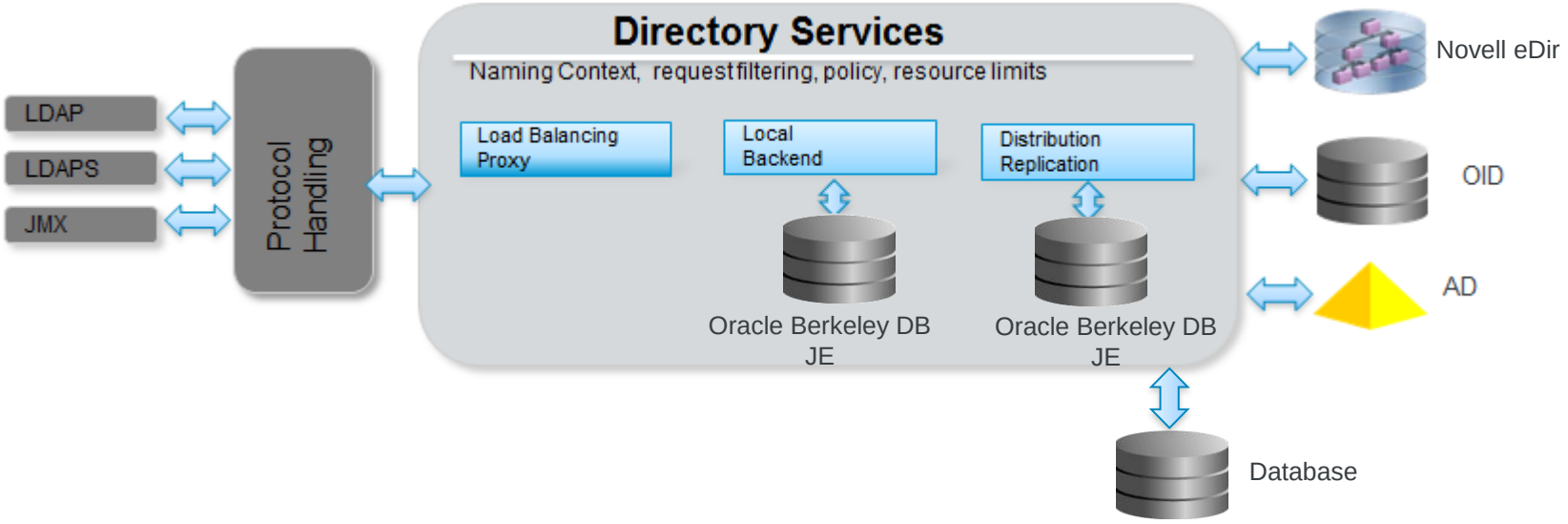
Was steckt drin…

- Handhabung mit Kommandozeile oder grafische Oberfäche
- Java pure
- Einfache Administration
- Schnelle und einfache Installation und Konfiguration
- Multimaster Replikation
- Virtual Attributes
- Attribute Encryption
- Load Balancing, Data Partitioning, Join Views
- Pass Through Authentication mit LDAP oder Kerberos (z.B. Active Directory)
- Data Transformation (Attribute / ObjectClass mapping, DN-Renaming)
- Gute Tuningmöglichkeiten
- Implementieren von eigenen Plugins
- Gute Wartbarkeit

Aufbau

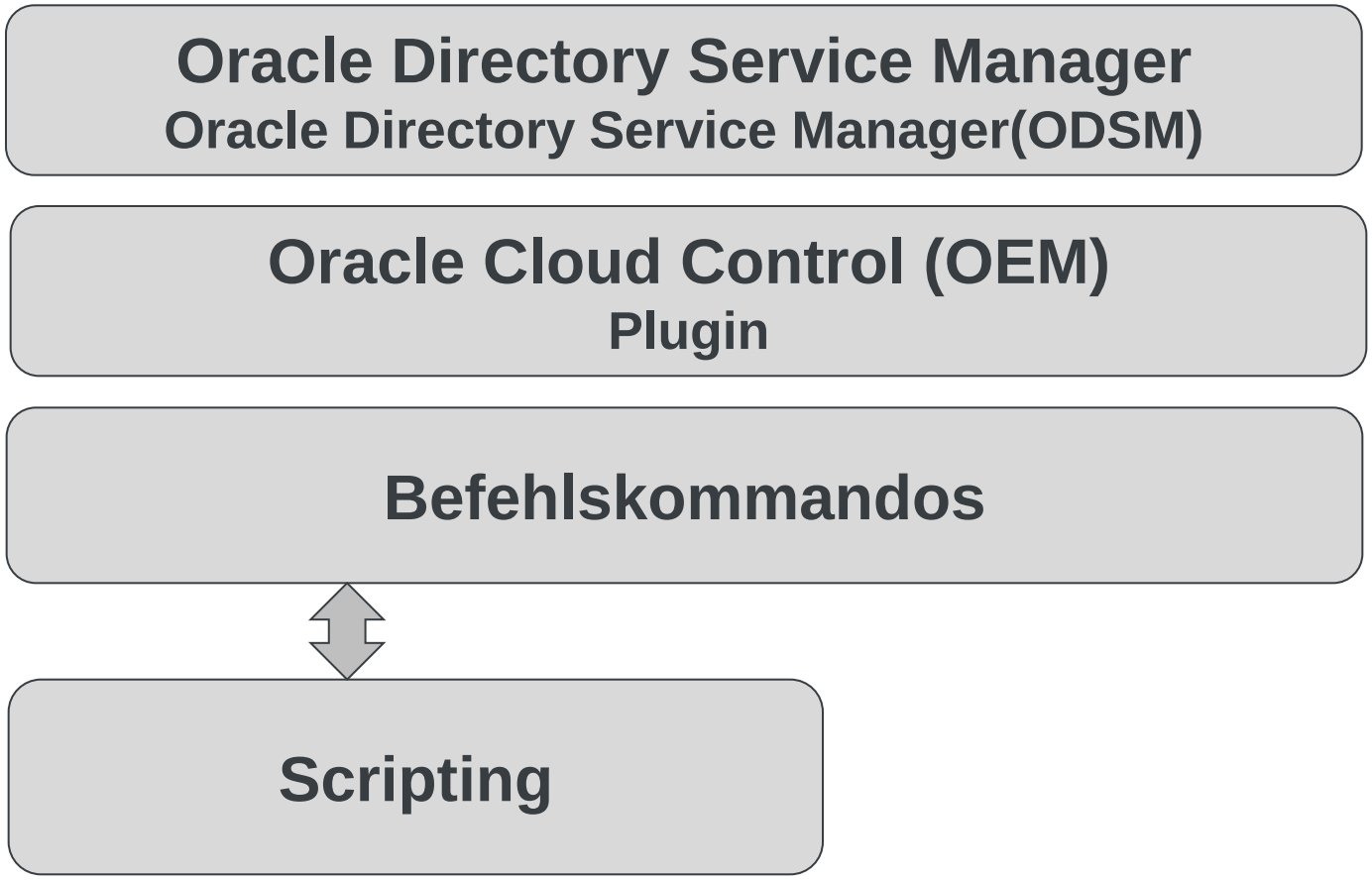
Tipp:
funktionale Erweiterungen berücksichtigen

Release Notes beachten



talanx. Systeme

Administration

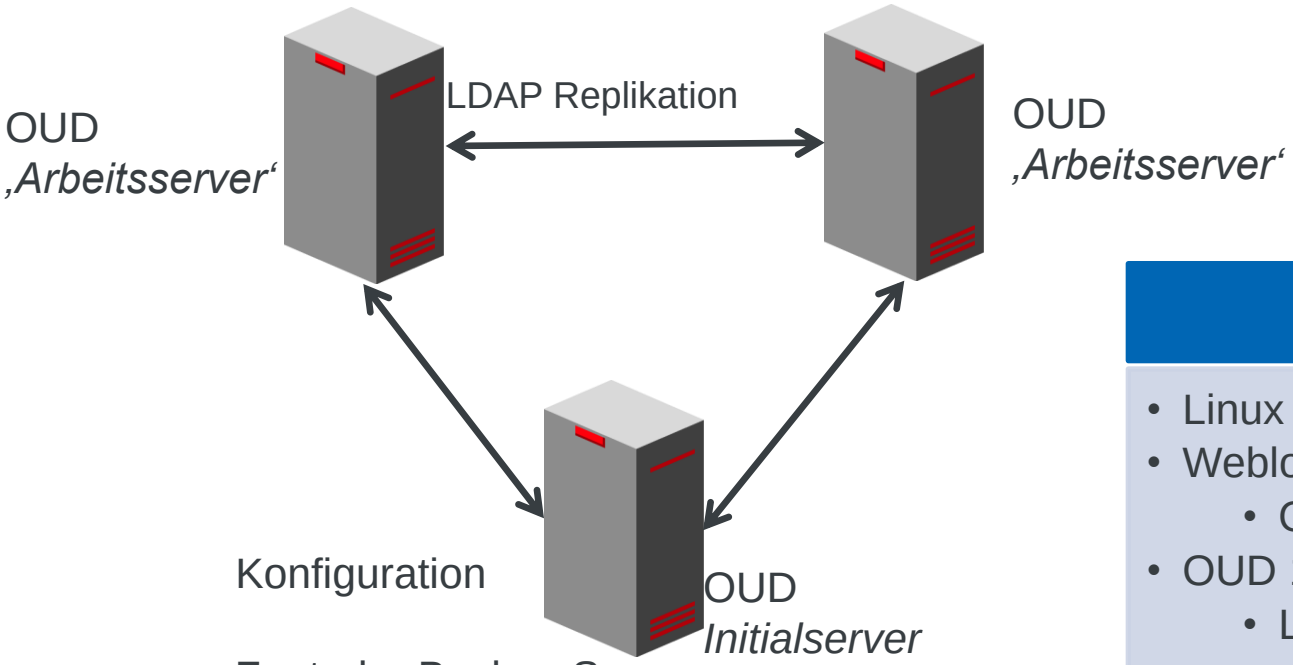


talanx. Systeme

Konzeptionierung

- Konzept erstellen
  - **Ein muss !!!!**
- Fragestellung (Checkliste)
  - Einsatzgebiet
    - Aufbau
  - Erweiterungen
  - Hochverfügbarkeit
  - Konsolidierung
  - Virtualisierung
  - Betrieb
    - Administration
    - Monitoring
    - Wiederherstellung

Konzept Talanx (Oracle Net Service)



Konfiguration

- Linux Server
- Weblogic
  - ODSM
- OUD 11gR2
  - LDAP Replikation Verbund

talanx. Systeme

Installation

Software Installation

Software download

Java Installation

ODSM Installation:

Weblogic
ADF
Konfiguration

OUD Installation

Directory Server Setup

Directory Server Instance erstellen

Directory Server ggf. konfigurieren

Tipp:
Die Vorgaben (Versionen etc.) sind genau nach dem jeweiligen Installation Guide einzuhalten
***Keine Experimente* !!!** ☺

Software Installation

Software download mit entsprechenden PSU‘s

Java Installation :
Beispiel: tar zxvf jdk-7u80-linux-x64.tar.gz

Tipp:
Bei der Weblogic Installation kann es zu Installationsprobleme geben

Wichtig vorab Variable setzen
JAVA_HOME !!!!
ORACLE_HOME
MIDDLEWARE_HOME
INSTANCE_NAME !!!!

ODSM Installation:
Weblogic: $JAVA_HOME/java –d64 –jar wls1036_generic.jar
ADF: ./runInstaller -jreloc $JAVA_HOME
Konfiguration: $MIDDLEWARE_BASE/oracle_common/common/bin/config.sh

OUD Installation:
./runInstaller -jreLoc $JAVA_HOME

talanx. Systeme

Directory Server Setup

Directory Server Instance erstellen

- Kommando oud-setup
  - Pfad direkt im OUD
  - Variable INSTANCE_NAME(Instance-Verzeichnis)
- Kommandoausführung
  - Grafisch (out of the box)
  - Interaktiv
  - Kommandozeile
- Vorkonfiguration
  - Replikation
  - Zertifikate
  - Tuning Parameter

Tipp:
Zertifikate sollten möglichst vorhanden sein
Die Maßnahme erspart eine Nachkonfiguration

Vorab ein zentrales Verzeichnis für Passwortdateien und Zertifikate einrichten

Directory Server Setup

Beispiel :

```
oud-setup
        --cli
        --baseDN dc=doag
        --addBaseEntry
        --adminConnectorPort 4444
        --ldapPort 1389
        --integration no-integration
        --rootUserDN "cn=Directory Manager"
        --rootUserPasswordFile /u00/app/oracle/.pwfiles/pwfile
        --ldapsPort 1636
        --generateSelfSignedCertificate
        --hostname oudserver1
        --serverTuning -Xms871m -Xmx871m -d64 -XX:+UseCompressedOops -server -
XX:MaxTenuringThreshold=1 -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=55
        --no-prompt \
        --noPropertiesFile
```

Hinweis:
Wenn Zertifikate (z.B.JKS) vorhanden sind
--useJavaKeystore
--keyStorePasswordFile
--certNickname

Wenn EUS verwendet werden soll
--integration eus

Bei Netservices (tnsnames)
--integration generic

talanx. Systeme

Directory Server konfigurieren

Allgemein

- Grundstruktur
  - **Network Group**
    - Einstiegspunkt aller Client Request
  - **Workflow**
    - Aufgabe den Naming Context (BaseDN) zu definieren
  - **Workflow Elemente**
    - verschiedene Elementtypen die bestimmte Aufgaben haben
- ***Workflow Extension***
  - Optional
  - besondere Aufgaben (z.B. AD-Kopplung)

talanx. Systeme

Directory Server konfigurieren

Hinweis:
dsconfig ist das wichtigste Konfigurationskommando

Kommandoüberblick

Kommando	Beschreibung
start-ds	Starten der OUD-Instance
stop-ds	Stoppen der OUD-Instance
dsconfig	**Konfigurationswerkzeug, wichtig für alle OUD-Komponenten**
manage_suffix	Strukturen mit einen Backend anlegen.
dsreplication	Überprüfung und Konfiguration von Replikationseinstellungen
backup	OUD Backup bzw. Backup der OUD-Backends
restore	OUD Restore bzw. restore der OUD-Backends
ldapmodify	LDAP Daten ändern
ldapsearch	LDAP Daten suchen
ldapdelete	LDAP Daten löschen
status	Überprüfung des OUD-Status
dstune	Tuning Utility

Directory Server konfigurieren

Struktur erstellen (DIT)

- Teilschritte
  - Worklflow Element
  - Workflow
  - Network Group
- ODSM
- Komplett mit einer Ausführung
  - Kommando
    - Manage-suffix

Tipp:
Möglichst früh die Replikation aufbauen, dass erleichtert die Konfiguration
Nach jeden Aufbauphase eine Offlinesicherung(generell)

Directory Server konfigurieren

Beispiel :

```
manage-suffix create
        --baseDN  dc=tnsnames,dc=doag
        --entries base-entry
        --integration generic
        --networkGroup network-group
        --workflowElement local_anwendungen_doag_DB
        --dbPath db
        --hostname oudserver1
        --port 4444
        --bindDN "cn=Directory Manager"
        --bindPasswordFile /u00/app/oracle/.pwfiles/pwfile
        --trustAll
        --no-prompt
```

Hinweis:
-- integration no_integration
generic
eus
--workflowElement Verzeichnis für die Berkley DB

--networkGroup network-group ist die Default Networkgroup

talanx. Systeme

Directory Server konfigurieren

Replikation erstellen

- Verschiedene Konfigurationsarten
- Erhöht die Ausfallsicherheit

- Vorgehensweise
  - Replikation enable
  - Replikation initialisieren

- Kommandos
  - dsconfig / dsreplication
  - ODSM (grafisch)

Tipp:
Generell muss bei der Replikation das Backup und das Restore wegen der Synchronisation berücksichtigt werden

Directory Server konfigurieren

Bespiel Replikation:

```
dsreplication enable --host1 oudserver1
                     --port1 4444
                     --bindDN1 "cn=Directory Manager"
                     --bindPasswordFile1/u00/app/oracle/.pwfiles/pwfile
                      --trustAll
                     --host2 oudserver2
                     --port2 4444
                     --bindDN2 "cn=Directory Server"
                     --bindPasswordFile2 /u00/app/oracle/.pwfiles/pwfile1
                     --trustAll
                     --replicationPort2 8989
                     --secureReplication2
                     --baseDN  dc=tnsnames,dc=doag
                     --adminUID admin
                     --adminPasswordFile /u00/app/oracle/.pwfiles/rep_pwfile
                     --trustAll
                     --no-prompt
                     --noPropertiesFile
```

Hinweis:
Vorab die Variablen setzen

Skriptschritte:
1.Replikation enable
2.Replikation initialisieren
3.Replikationsstatus

Abschalten einer Replikation mit dsreplication –disable …

Wiedereinschalten einer Replikation mir dsreplication –enable …..

Kein initialisieren notwendig

```
dsreplication initialize -all -h oudserver1 -p 4444 --baseDN dc=tnsnames,dc=doag --adminUID admin
--adminPasswordFile /u00/app/oracle/.pwfiles/rep_pwfile -X -n

dsreplication status -h oudserver1 -p 4444 --adminUID admin
--adminPasswordFile  /u00/app/oracle/.pwfiles/rep_pwfile  -X -n
```


talanx. Systeme

Directory Server konfigurieren

Lokalen User erstellen / konfigurieren

- Freischaltung von importierenden Passwörter
- User anlegen
  - verschiedene Möglichkeiten
    - Kommando
      - LDIF-Dateien
    - Interaktiv
    - ODSM
- User konfigurieren
  - Expire-Time
  - Passwortkomplexität
  - Lifetime

Tipp:
Beim Importieren von verschlüsselten Passwörtern muss diese Möglichkeit separat freigeschaltet werden

User möglichst per Skript anlegen

talanx. Systeme

Directory Server konfigurieren

Beispiel Freischaltung zum Importieren von verschlüsselten Passwörtern:

Tipp:
Sollten generell eingeschaltet werden
Muss pro Instance ausgeführt werden

```
dsconfig -h oudserver1 -p 4444  -D "cn=Directory Manager" -j /u00/app/oracle/.pwfiles/pwfile
-X -n set-password-policy-prop  --policy-name "Default Password Policy" --set allow-pre-
encoded-passwords:true
```


talanx. Systeme

Directory Server konfigurieren

Beispiel lokalen User anlegen:

```
ldapmodify -h oudserver1  -p 1389 -D "cn=Directory Manager"  -j /u00/app/oracle/.pwfiles/pwfile <<'EOF'
dn: cn=O_4711,cn=people,ou=oracle_admins,o=local_users
changetype: add
postalCode: 30549
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
userPassword: pwneu_04711
ou: DOAG_Konferenz
uid: O_4711
mail: mhp@xxxx.com
cn: O_4711
o: DOAG GmbH
st: Niedersachsen
l: Hannover
postalAddress: Hannover
sn: Hoppe
ds-rlim-size-limit: 3000
ds-rlim-time-limit: 300
ds-rlim-lookthrough-limit: 3000
EOF
```

Tipp:
Die direkte Eingabe mit <<'EOF' muss getestet , z.T. verschiedenes Verhalten

Die Struktur zur Ablage der User muss vorhanden sein

Die Parameter ds-rlim-* sind wichtig für die spätere Anzeige(z.B. netmanager) , weil sonst nur die Einträge teilweise zu sehen sind

Directory Server konfigurieren

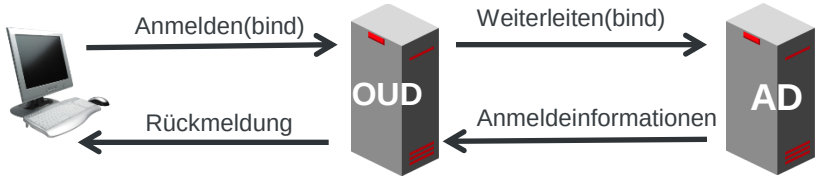
Remote User Authentifizierung

- Authentifizierung auf einem Directory Service
  - Beispiel Active Directory (Mircosoft)
- Pass-Through Authentication (PTA)
- Konfiguration
  - Workflow Element Extension
  - Workflow Element (Bind + Join)
  - Workflow
  - Networkgroup(Zuordnung)

Tipp:
Konfigurationsinformationen: Oracle® Fusion Middleware Administrator's Guide for Oracle Unified Directory

oder

Performing OUD PTA against AD (OUD R2PS2+) (Doc ID 1555227.1)



talanx. Systeme

Directory Server konfigurieren

Beispiel Workflow Extension :

```
dsconfig -h oudserver1 -p 4444 -D "cn=Directory Manager" -j /u00/app/oracle/.pwfiles/pwfile   -X –n create-extension --type ldap-server --extension-name  extension_pta_ad_oud
   --set remote-ldap-server-address:ad_server
   --set remote-ldap-server-port:  388
   --set enabled:true
```

Beispiel Workflow Element (Bind)

```
dsconfig -h oudserver1-p 4444 -D "cn=Directory Manager" -j  /u00/app/oracle/.pwfiles/pwfile -X -n create-workflow-element
        --set client-cred-mode:use-client-identity
        --set enabled:true
        --set ldap-server-extension: extension_pta_ad_oud
        --set remote-root-dn:"cn=ADMASTER,ou=users,ou=system_administration,dc=doag"
        --set remote-root-password:AD_Meister_007
        --type proxy-ldap
        --element-name we_pta_oud_ad
```


talanx. Systeme

Directory Server Monitoring / Überwachung

- SMNP-Schnittstelle
- Cloud Control (OEM)?
  - Plugin
- Eigene Lösung
  - Nagios Überwachung
    - Shell- Skripte (Verfügbarkeit)
  - Splunk Überwachung
    - Shell- Skripte (Replikation)
  - Check-Skripte bei Problemstellungen

Zertifikate

- Zertifikate (keystore / trustedstore)
  - LDAPS
  - Replikation
  - Administration
- Konfiguration
  - dsconfig
  - ODSM
- Administrationskonfiguration
  - dsconfig (interaktiv !!!!)

Tipp:

Replikation berücksichtigen, ggf. abschalten

Vorab die OUD-Instance sichern !

Zertifikatskonfiguration für die Administration nur dsconfig interaktiv benutzen

Directory Server konfigurieren

Beispiel Konfiguration(JKS) auslesen:

```
dsconfig -h oudserver1 -p 4444 -D " cn=Directory Manager " -j /u00/app/oracle/.pwfiles/pwfile get-key-manager-provider-prop --provider-name "JKS" -X -n
```

Beispiel JKS-Keystore erstellen:

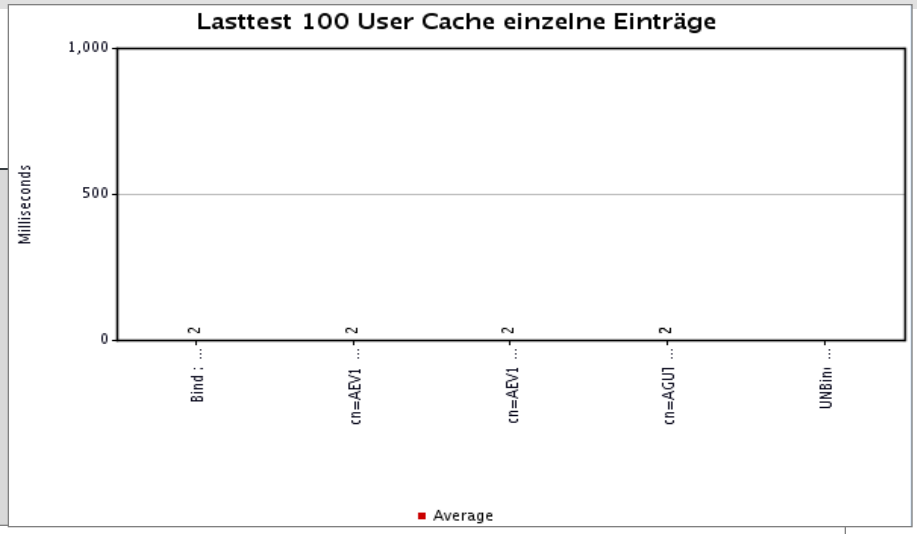
```
dsconfig -h oudserver1 -p 4444 -D " cn=Directory Manager " -j /u00/app/oracle/.pwfiles/pwfile
set-key-manager-provider-prop
--provider-name "JKS"
--set enabled:true
--set "key-store-type:JKS"
--set "key-store-pin: /u00/app/oracle/.keystore/jks_store.jks"
--set "key-store-pin-file /u00/app/oracle/.keystore/jks_store_pin.pin" -X –n
```

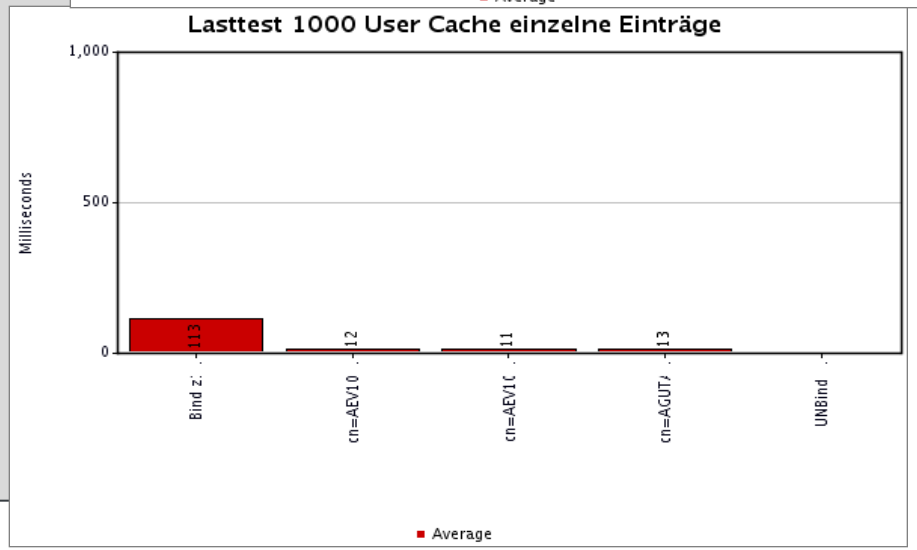

talanx. Systeme

Performance

Lasttest

- Apache Jmeter
  - LDAP-Komponente
- Konfiguration
  - Verschiedene Anzahl von User
  - Auslesen von allen Attributen
- Methode
  - Werte ‚gecacht'
  - Werte ‚ungecacht'





talanx. Systeme

Performance

- Überwachung
  - ODSM (einfach)
  - Cloud Control 12c (12.2.4)
- Überprüfen / Einstellen
  - dstune
    - Interaktiv
    - Memory Einstellungen
- Preload
  - ***InMemory***
    - Datenbank ins Memory

Tipp:

OUD Administration Guide

Database Cache Tuning - Heap Size Doc ID 1944247.1

OUD performance Tuning - Using DBCache Doc ID 1527016.1

talanx. Systeme

Mandantenfähigkeit

- Strukturen anlegen
  - Administratoren
  - User
    - Rollen
      - Leserolle
      - Administrationsrolle
- Überprüfen / Einstellen
- Lese und Administratorenzugriffe steuern
  - ACI (Zugriffskontrolle)
    - Gruppensteuerungen

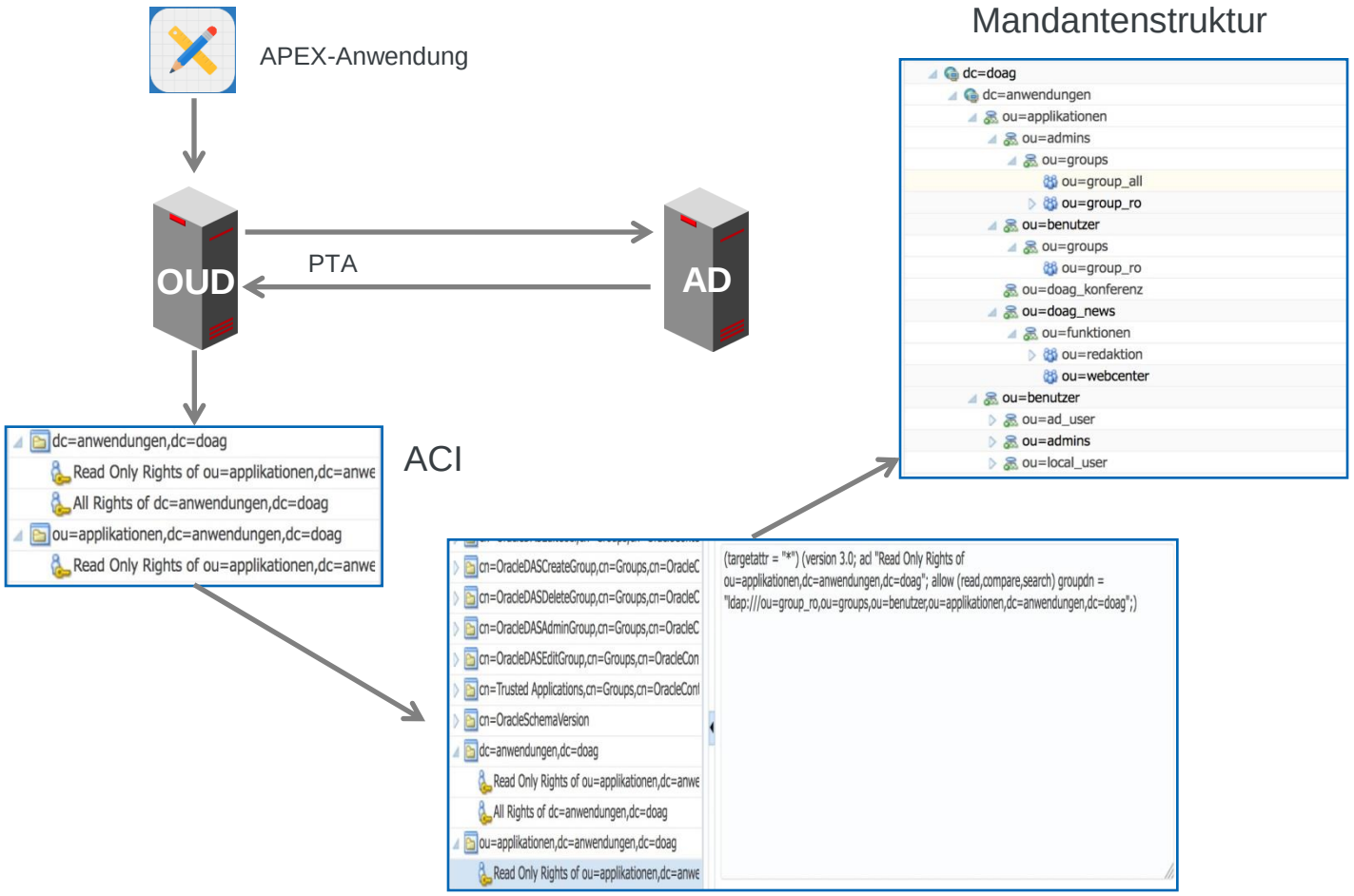
Tipp:

Abstimmung mit den Applikationen (Konzept)

Übersichtlichkeit beim Strukturaufbau berücksichtigen

Standards definieren

Mandantenfähigkeit (Beispiel)



talanx. Systeme

have fun……

Useful Infos:

Information Center : Overview Oracle Unified Directory (OUD) (Doc ID 1418884.2)

Master Note for Oracle Unified Directory (OUD) (Doc ID 1401023.1)

Master Note for OUD-EUS integration (Doc ID 1592446.1)

OUD Dokumentation

https://blogs.oracle.com/sduloutr