DOAG 2010

Kerberos für die Datenbank

Dr. Günter Unbescheid
Database Consult GmbH
Jachenau

Database Consult GmbH

- Gegründet 1996
- Kompetenzen im Umfeld von ORACLE-basierten Systemen
- Tätigkeitsbereiche
  - Tuning, Installation, Konfiguration
  - Security, Identity Management
  - Expertisen/Gutachten
  - Support, Troubleshooting, DBA-Aufgaben
  - Datenmodellierung und –design
  - Datenbankdesign, Systemanalysen
  - Programmierung: SQL,PL/SQL,Java, JSP, ADF, BC4J
  - Workshops
  - www.database-consult.de

Kerberos

- Verteilter Autentifizierungsdienst – SSO Prinzip
  - Basis symmetrische Kryptografie
  - Kerberos 5 Netzwerkdienst als „trusted third party“
- Von Microsoft genutzt als Standardprotokoll für die Authentifizierung
- Ideale Benutzerbasis in Windowsnetzwerken
- Tools zur Nutzung unter Unix & CO.
- Anmeldung als `/@zieldb`
- Verbunden mit gleichnamigem externen Benutzer

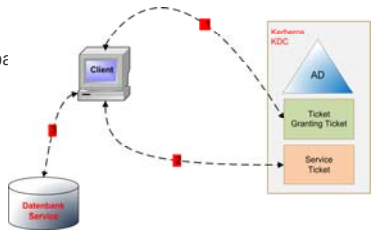
Kerberos Ablauf

	Benutzer	KDC Ticket Granting Server (TGS) Authentication Server (AS)
	> Authentication Request	> *AS
		< Response mit TGT, Sitzungsschlüssel
	> Anforderung Service Ticket (Ressource,TGT,Authent.)	> *TGS
Resource	< Ticket mit Auth. an Service	< Ticket, Sitzungsschlüssel
	> Service bestätigt	
	Weitere Kommunikation	verschlüsselt oder nicht

Tickets sind immer nur vom *Target* lesbar

Kerberos

- okinit testuser
- sqlplus /@zieldb
- Oracle-User: testuser@DBC.DE (entsprechend Principa Name)



Kerberos


```
okinit testuser
Kerberos Utilities for Solaris: Version 10.2.0.1.0 –
Production on 03-MAY-2010 16:57:49
Copyright (c) 1996, 2004 Oracle. All rights reserved.

Password for testuser@DBC.DE:

oklist

Kerberos Utilities for Solaris: Version 10.2.0.1.0 –
Production on 03-MAY-2010 16:59:46
Copyright (c) 1996, 2004 Oracle. All rights reserved.

Ticket cache: /opt/oracle/1020client/network/krb5/krbcache
Default principal: testuser@DBC.DE

   Valid Starting           Expires          Principal
03-May-2010 16:58:04 04-May-2010 00:57:49
krbtgt/DBC.DE@DBC.DE

sqlplus /@zieldb
```

Kerberos-Konfiguration

- Lizenz: Advanced Security Option
- Anlegen Principal User, anhängen Service Principal Name (AD)
- Konfigurationsdateien sqlnet.ora und krb5.conf (Client/Server) unter Windows: krb5.ini
- Keyfile auf den/die DB-Server kopieren – enthält Credentials
- Datenbank-User mit entsprechendem Principal Name

```
ktpass -princ oracle/testserver01@DBC.DE -mapuser testserver01
-pass password123 –DesOnly
-crypto des-cbc-crc -ptype KRB5_NT_PRINCIPAL –kvno 1
–out C:\Users\keytab.testserver01
--------------------
CREATE USER "TESTUSER@DBC.DE" IDENTIFIED EXTERNALLY;
```


Kerberos-Konfiguration


```
CLIENTSEITE sqlnet.ora
NAMES.DIRECTORY_PATH= (TNSNAMES)
SQLNET.AUTHENTICATION_SERVICES = (kerberos5)
# Erreichbarkeit KDC
SQLNET.KERBEROS5_CONF = c:\windows\krb5.ini
# Credential Cache (TPT usw.)
SQLNET.KERBEROS5_CC_NAME = OSMSFT://
# SQLNET.KERBEROS5_CC_NAME = /opt/oracle/1020client/network/krb5/krbcache
SQLNET.KERBEROS5_CONF_MIT = true
# SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle

SERVERSEITE sqlnet.ora
NAMES.DIRECTORY_PATH= (TNSNAMES)
SQLNET.AUTHENTICATION_SERVICES = (kerberos5)
SQLNET.KERBEROS5_CONF = /u01/oracle/1020client/network/krb5/krb5.conf
SQLNET.KERBEROS5_CC_NAME = /opt/oracle/1020client/network/krb5/krbcache
SQLNET.KERBEROS5_CONF_MIT = true
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
SQLNET.KERBEROS5_KEYTAB = /u01/oracle/product/krb5/keytab.testserver01
```

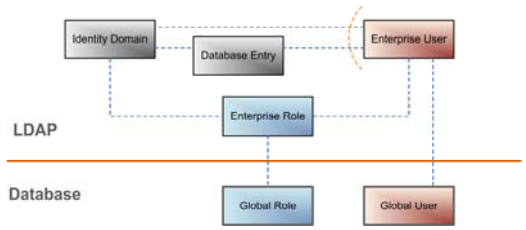

Kerberos

- Kerberos authentifiziert. Authorisierung erfolgt separat.
- Weitere Konfigurationsmöglichkeiten:
  - Kombination mit Enterprise Usern: Kerberos User „mapped“ auf *shared schema*
  - Umleitung auf *proxy user*
- Tool/API Unterstützung, u.a.
  - SQL Developer (über OCI/thick driver)
  - JDBC thin und thick

Enterprise User/Roles

- LDAP-Verzeichnisdienst
  - Benutzer (*enterprise user*), Rollen (*enterprise roles*)
  - registrierte Datenbanken, „Mappings“
  - Authentifizierung über PW, Zertifikat, Kerberos
- Datenbank(en)
  - Globale Benutzer, Globale Rollen
  - Verbindung zum Verzeichnisdienst (ldap.ora)
- Motivation
  - Zentralisierung der Benutzerverwaltung
  - Reduktion der lokalen DB-Administration

Enterprise Benutzer



Komponenten

- Produkte/Lizenzen
  - Enterprise Edition
  - ASO für Authenfitizierungen ausser Password
  - OID/OVD – Bestandteil von „Identity Management“ von OFM
- Verzeichnisdienst
  - Oracle Internet Directory (OID) + Repository
  - Active Directory (AD) – alternativ/zusätzlich
  - ggf. Oracle Virtual Directory als „Frontend“ zur Integration
- Weblogic Server – Admin Oberflächen OID/OVD

Kurzinfo Directory

- „spezialisierte“ Datenbanken
  - Leseorientiert
  - Kurze Transaktionen
  - Kompakte Informationen
- Informationen als *entries*
  - Vorgabe durch Objektklassen mit Attributtypen
  - Hierarchisch sortiert in Directory Information Tree (DIT)

Kurzinfo Directory

- Distinguished names (DN)
  - DN: *cn=unbescheid, o=databaseconsult, c=de*
- Relative Distinguished Names (RDN)
  - *cn=unbescheid*
- Entries auf Basis von Objektklassen
- Eigene Objektklassen und Attributtypen möglich

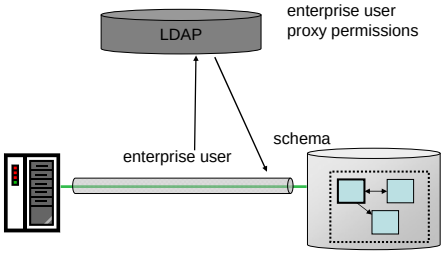
Proxy User

- Prinzip: Benutzer A schaltet sich auf Benutzer B
  - DB kennt A und B
  - DB gibt Regeln für die Aufschaltung per grant
  - A braucht kein Passwort von B
- Auditing und Logging kennen Proxy
  - `proxy_sessionid` in Tabelle `aud$`
- Unterschiedliche Möglichkeiten der Authentifizierung
- Untermenge von Privilegien ist möglich

Proxy-Authentifizierung

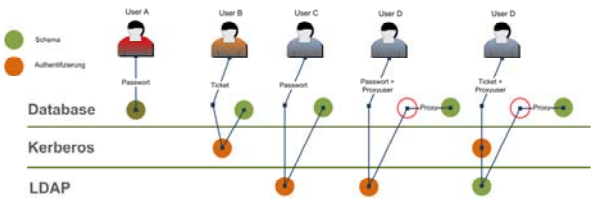
```
-- App-User anlegen
CREATE USER app IDENTIFIED BY appwd;
-- andere Authentifizierungen sind machbar

-- App-User minimal privilegieren
GRANT CREATE SESSION TO app;

-- Enduser anlegen und privilegieren
CREATE USER end1 IDENTIFIED BY endpwd;
GRANT r1, r2, r3 TO end1;

-- Proxy einrichten und privilegisieren
ALTER USER end1 GRANT CONNECT THROUGH app WITH ROLE r2;
-- alternativ
ALTER USER end1 GRANT CONNECT THROUGH ENTERPRISE USERS;

-- View
SELECT * FROM DBA_PROXIES;

-- Connect
connect app[end1]/appwd;
```


Enterprise User Proxy

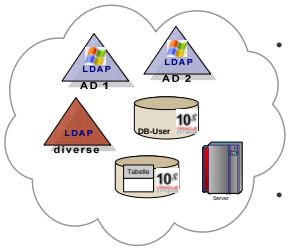



```
ALTER USER local_database_user_name
GRANT CONNECT THROUGH ENTERPRISE USERS;
```


Authentifizierungsvarianten



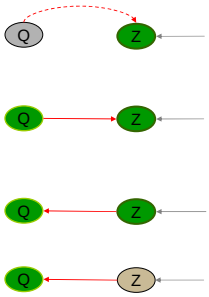
Benutzerdaten lokalisieren



- Typen
  - interne Mitarbeiter
  - externe Zugreifer
- Quellen
  - Windows User: Kerberos Schlüssel in AD
  - ggf. mehrere ADs
  - DB-Benutzer – diverse Verfahren
  - OS-Benutzer
  - diverse Quellen: DB-Tabellen etc.
- Herausforderung
  - Aktualität
  - Transparenz bei Passwort-Änderungen

Kerberos für die Datenank

Konsolidierungs-Techniken



- Datenmigration
  - einmalige Übernahme und Abkopplung
- Synchronisation
  - permanente Ankopplung, Redundanz, Verfügbarkeit
  - Directory oder Datenbank-Tabellen
- Server Chaining
  - Verlinkung mit jeweils einem AD und/oder SunONE
- Virtual Directory
  - beliebige Verlinkung mit diversen Sourcen

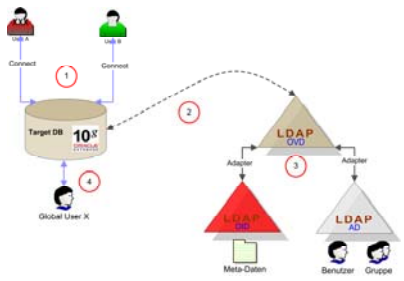
Kerberos für die Datenank

Architekturvarianten

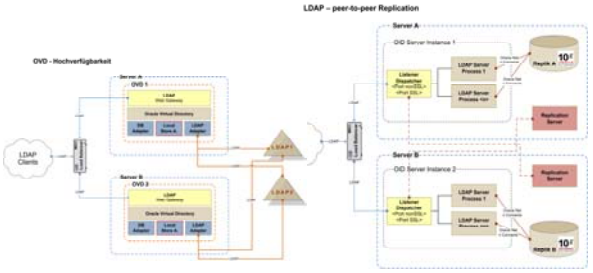
- Problematik User-Daten – Redundanz vermeiden
  - Userstamm in AD
  - ggf. weitere Sourcen: Verzeichnisse, Tabellen etc.
- Lösungsvarianten
  - OID – Directory Integration Plattform (kopieren)
  - OID – Server Chaining (verlinken)
  - OVD integriert/verlinkt diverse Verzeichnisse/DBs
    - Trennung von Metadaten und Userdaten
- Schemaerweiterung für EUS notwendig
- Password-Problematik – ggf. Passwordfilter (für AD)

Kerberos für die Datenank

OVD Nutzung



(Hoch)Verfügbarkeit



Danke für‘s Zuhören

www.database-consult.de