Kerberos für die Datenbank

Dr. Günter Unbescheid
Database Consult GmbH
Jachenau

Schlüsselworte:

Datenbank, Authentifizierung, Kerberos, Single Sign-on, Enterprise User

Einleitung

Die gesetzlichen wie funktionalen Anforderungen an die Sicherheit von Oracle-Systemen sind in den letzten Jahren beständig verschärft worden. In diesem Zusammenhang werden auch Forderungen nach persönlichen Benutzer-Accounts für Administratoren und anderen "Power-Usern" laut. Die Arbeit unter SYS und SYSTEM wird immer mehr eingeschränkt.

Windows-Client-Netzwerke sind in den meisten Firmennetzen an der Tagesordnung. Benutzer authentifizieren sind in diesen Netzen über Active Directory Verzeichnisdienste mit persönlichen Accounts. Im AD-Kontext ist es darüber hinaus leicht möglich, Kerberos Ticket Server einzubinden und auf diese Weise der netzweiten Authentifizierung mit Kerberos Mitteln Tür und Tor zu öffnen.

Der vorliegende Beitrag zeigt Möglichkeiten, Kerberos Tickets in Oracle Datenbankumgebungen einzubinden und für die persönliche Authentifizierung zu nutzen. Dabei wird sowohl die direkte Authentifizierung bei der Datenbank, als auch die Authentifizierung über Enterprise User mit Hilfe von Kerberos diskutiert. Auf diese Weise lassen sich Single-Sign-On Funktionalitäten kostengünstig implementieren.

Kerberos – eine Einführung

Kerberos ist ein verteilter Authentifizierungsdienst für offene Computernetze, der Identitäten verifiziert und für die Nutzung von vorgegebenen Services qualifiziert. Das System wurde Ende der 70er Jahre des letzten Jahrtausends vom Massachusetts Institute of Technology entwickelt und nach dem Höllenhund der griechischen Mythologie benannt, der den Eingang zur Unterwelt bewacht.

Die erstaunliche Verbreitung des Dienstes geht nicht zuletzt auf Microsoft zurück. Der Konzern verwendet Kerberos als Standardprotokoll für die Authentifizierung unter Windows 2000/2003/2008 basierten Netzwerken sowie für den Windows 2000/XP-Client. Die für die Arbeit von Kerberos nötigen Schlüssel werden dabei im hauseigenen Verzeichnisdienst Active Directory gespeichert. Kerberos verwendet dann zur weiteren Authentifizierung sogenannte Tickets.

Bereits bei der Anmeldung an eine Windows-Domain wird dem Client ein Kerberos Ticket ausgestellt, mit dem er beim Kerberos Server Tickets für weitere Dienste – unter ihnen auch Oracle Datenbanken – anfordern kann. Wurde die Oracle Datenbanken entsprechend konfiguriert, sind sie in der Lage, die Rechtmäßigkeit der Tickets zu prüfen und den Haltern entsprechenden Zugang zu verschaffen, ohne dass diese erneut ihre Passwörter eingeben müssen. Für Clients im Unix-Umfeld stehen zusätzliche Werkzeuge bereit, um Kerberos-Tickets vom Active Directory Dienst zu erhalten und für die Oracle-Authentifizierung zu nutzen. Allerdings ist in diesen Fällen – einmalig – die zusätzliche Eingabe des Passwortes erforderlich. Zur Nutzung des Kerberos-Dienstes ist die Advanced Security Option zu lizenzieren.

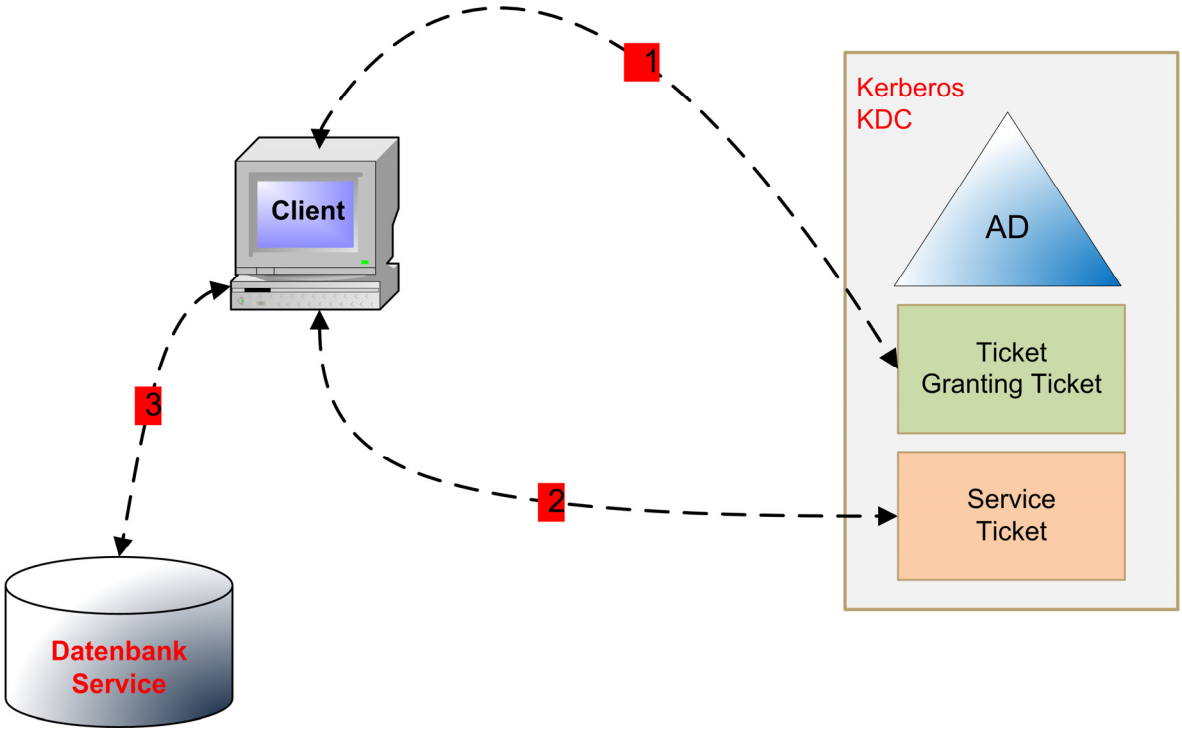

Abb. 1: Kerberos-Architektur und der Anmeldeprozess

Der Kerberos Authentifizierungsprozess läuft – vereinfacht – wie folgt ab:

- Um einen Dienst, den Kerberos unterstützt, nutzen zu können, muss sich der betreffende Client zunächst beim Kerberos-Authentifizierungs-Server des Key Distribution Center (KDC) anmelden (Schritt 1 der Abbildung 1). Auf Windows-Systemen ist diese Kerberos-Anmeldung implizit an die Windows-Anmeldung gekoppelt. Auf Unix-Systemen erfolgt sie explizit über ein Hilfsprogramm (`okinit`).
- Nach erfolgreicher Anmeldung erhält der Benutzer vom Kerberos-Server ein sogenanntes Ticket Granting Ticket (TGT), also eine Art von Generalvollmacht, die an seine Identität gebunden ist. Mit dieser Generalvollmacht kann der Client ohne erneute Eingabe seines Passworts weitere Tickets beim Ticket Granting Server des KDC für spezifische Dienste, z.B. Datenbanken, anfordern (Schritt 2).
- Der Server prüft schließlich dieses Dienst-Ticket und gewährt dem Client im Erfolgsfall Zugang zu dem betreffenden Dienst (Schritt 3). Handelt es sich bei dem Service um eine Datenbank, wird in diesem Modell der Client mit einem extern authentifizierten Datenbankbenutzer verbunden, dessen Name identisch mit seinem *Principal Name* ist: Beispielsweise wird der Benutzer `testuser` mit dem *Principal Name* `testuser@dbc.de` mit dem entsprechenden Datenbankbenutzer namens `testuser@dbc.de` verbunden.

Zusätzlich zur Authentifizierung von Identitäten können über Kerberos auch Session Keys für die Verschlüsselung des Datenverkehrs sorgen.

Vorbereitung des Verzeichnisdienstes

Alle Parteien, die an der Kommunikation teilnehmen wollen, müssen zunächst beim Kerberos Dienst registriert werden und erhalten dann einen eindeutigen, geheimen Schlüssel, der nur ihnen und dem

KDC bekannt ist. Dies sind zum einen die – bereits in AD registrierten – Benutzer selbst, zum anderen aber auch ein stellvertretender Kerberos Principal User für die Oracle-Datenbankdienste, dem entsprechende Service Principal Names für die individuellen Zielinstanzen zugeordnet werden. Das Ganze ergibt dann den sogenannten *Kerberos Principal*, der in der Form

```
service/principalUser@realm
```

geschrieben und strukturiert wird. Die entsprechende Zieldatenbank spezifiziert dann in ihren NET-Konfigurationsdateien, welchen Kerberos-Servicenamen sie unterstützt, und kann dies mit dem Service-Ticket, das der Benutzer beim Verbindungsaufbau präsentiert, abgleichen und ihm bei Erfolg Zugang gewähren.

Während die `realm`-Komponente sich in der Regel nach dem Domänennamen des Netzwerks richtet, können die Namen für *Services* und *Principal User* im Prinzip frei gewählt werden, sofern sie mit den Einstellungen der NET-Dateien (siehe unten) übereinstimmen. Es empfiehlt sich jedoch, ein Regelwerk für die Vergabe der Namen zu vereinbaren. Das folgende Verfahren hat sich in vielen Fällen bewährt:

- Für jeden Server, dessen Datenbanken über die Kerberos-Authentifizierung erreicht werden sollen, wird ein eigener Principal User angelegt, der den Namen des Servers trägt.
- Da die Datenbanken – wie erwähnt – ihre Kerberos-Identität in den NET-Konfigurationsdateien festschreiben und diese für jedes Home-Verzeichnis konfiguriert werden und darüber hinaus jeder Oracle-Client ebensolche Dateien konfiguriert hat, mit denen er sein Service-Ticket anfordert, ist es empfehlenswert, pauschal einen Servicenamen für alle Systeme einzurichten, beispielsweise `oracle`.

Demnach könnte der Kerberos Principal für die Systeme auf dem Server `testserver01` der Domäne `dbc.de` folgendermaßen benannt werden: `oracle/testserver01@DBC.DE`

Im Einzelnen ist zur Konfiguration Folgendes auszuführen:

- Auf dem AD-Server: Anlegen der Kerberos Principal User alias Hostnamen mithilfe der GUI "Active Directory Users and Computers" (`dsa.msc`). Für unser Beispiel bedeutet dies:

```
[General tab]
First name: testserver01
Display name: testserver01
Password: <beliebiges Kennwort>
[Account tab:]
User logon name: testserver01@DBC.DE
User logon name (pre-Windows 2000): DBC\testserver01
```

Bei den Optionen muss "Use DES encryption types for this account" ausgewählt werden!

- Im nächsten Schritt lässt sich nun der *Service Principal Name* dem Benutzer zuordnen. Hierzu wird auf Windows-Systemen das Kommando `ktpass` benutzt, das gleichzeitig noch ein *keyfile* für den betreffenden Server/Principal User erstellt (`-out` Klausel). Dieses *keyfile* enthält den symmetrischen Schlüssel für den betreffenden Kerberos Principal und muss im Anschluss sicher auf den Zielserver kopiert werden. Auf Großschreibung der Domäne ist zu achten! Für unser Beispiel bedeutet dies:

```
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
```

Die Ausführung kann über den Befehl `setspn` oder direkt über die grafische Oberfläche von AD kontrolliert werden:

```
setspn -L testserver01

Registered ServicePrincipalNames for
CN=testserver01,CN=Users,DC=dbc,DC=de:
oracle/testserver01
```

Der Inhalt des *keyfile* kann nach dem Kopieren auf dem Datenbankserver mithilfe des Kommandos `oklist` kontrolliert und angezeigt werden:

```
oklist -k –t /<pfad>/<keyfile>
```

erzeugt – beispielsweise auf einem Solaris-Server – folgende Ausgabe:

```
Kerberos Utilities for Solaris: Version 10.2.0.1.0 - Production on 30-APR-
2010 11:42:37

Copyright (c) 1996, 2004 Oracle. All rights reserved.

Service Key Table:
/u01/app/oracle/product/1020/network/krb5/keytab.testserver01


Ver     Timestamp                Principal
 1   01-Jan-1970 01:00:00 oracle/testserver01@DBC.DE
```

Konfiguration der Oracle-Clients und Server

Nachdem alle Einträge in AD durchgeführt wurden, müssen nun sowohl die Oracle Client- als auch die Server-Umgebungen so konfiguriert werden, dass sie die neuen Kerberos Principals für ihre Authentifizierung nutzen können.

Arbeiten auf den Clients

Damit Oracle-Clients die Authentifizierung über Kerberos nutzen können, muss im Rahmen des Clients die "Advanced Security Option" installiert worden sein. Dies kann wie folgt überprüft werden:

```
$ORACLE_HOME/OPatch/opatch lsinventory -detail | grep "Advanced Security"
```

Bei allen Zielsystemen muss die Enterprise Edition, ebenfalls mit der "Advanced Security" Option installiert und lizenziert worden sein.

Die Kerberos-Konfiguration auf allen Oracle-Client-Maschinen betrifft drei Bereiche:

- Anpassung/Erweiterung der Host-Datei, sodass das Kerberos Key Distribution Center (KDC) und der AD-Verzeichnisdienst erreicht werden können.
- Aufbau der Kerberos-Konfigurationsdatei, z.B. `krb5.conf`, mit Verbindungsinformationen zum KDC. In unserem Beispiel unter `$ORACLE_HOME/network/krb`
- Erweiterung der Dateien `sqlnet.ora`

Der Hostname, der für den AD-Server in der Kerberos-Konfigurationsdatei angegeben wird, ist in der hosts-Datei entsprechend mit und ohne Domäne einzutragen, beispielsweise:

```
192.168.45.33 adnet.dbc.de adnet
```

Kerberos-Konfigurationsdatei: Es hat sich bewährt, diese Datei in einem eigenen Verzeichnis – `krb5` – unter `$ORACLE_HOME/network` anzulegen. Die Datei enthält Verbindungs- und Domänen-Informationen. Der Adresse des kdc-Rechners muss über die hosts-Datei auflösbar sein. Mit Hilfe der

realm-Klausel kann erreicht werden, dass der Client- und der Verzeichnisdienst nicht in der gleichen Domäne liegen müssen.

```
[libdefaults]
  default_realm = DBC.DE
  clockskew = 10000
[realms]
  DBC.DE = {
   kdc = adnet.dbc.de
 }
[domain_realm]
  .dbc.de = DBC.DE
  dbc.de = DBC.DE
```

Über die Datei sqlnet.ora hat der Client schließlich Zugang zu den Kerberos-Diensten, über die entsprechende Service-Tickets angefordert werden.

```
# sqlnet.ora Network Configuration File:
# /opt/oracle/client/network/admin/sqlnet.ora
# Generated by Oracle configuration tools.
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
```

Die Parameter werden in der folgenden Tabelle kurz erläutert.

SQLNET.AUTHENTICATION_SERVICES	Listet die gewünschten Authentifizierungsmethode(n) des Netzwerks auf
SQLNET.KERBEROS5_CONF	Pfad und Name der Kerberos-Konfigurationsdatei
SQLNET.KERBEROS5_CONF_MIT	Nutzt das neue MIT Konfigurationsformat (true)
SQLNET.KERBEROS5_CC_NAME	Pfad und Name der Cache-Datei. Enthält die Credentials
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE	Gibt den Servicenamen vor für den ein Serviceticket angefordert wird

Server-Konfiguration für Kerberos

Die Kerberos Konfiguration auf allen Oracle-Datenbankmaschinen ist ähnlich wie bei den Clients organisiert, mit einigen zusätzlichen Parametern bei der Datei sqlnet.ora

Auch hier haben wir drei Bereiche:

- Anpassung/Erweiterung der Host-Datei, sodass KDC und AD erreicht werden können – analog zum Client.
- Aufbau der Kerberos-Konfigurationsdatei, z.B. krb5.conf, mit Verbindungsinformationen zum Kerberos Key Center (KDC), analog zum Client.

- Erweiterung der Daten `sqlnet.ora` wie im folgenden Abschnitt beschrieben.

Die Datei enthält –im Gegensatz zum Client – zusätzlich die vom Key Center generierte Schlüsseldatei, die über den Parameter SQLNET.KERBEROS5_KEYTAB konfiguriert wird:

```
NAMES.DIRECTORY_PATH= (TNSNAMES)

SQLNET.AUTHENTICATION_SERVICES = (beq, kerberos5)

SQLNET.KERBEROS5_KEYTAB =
/u01/app/oracle/product/1020/network/krb5/keytab.testserver01

SQLNET.KERBEROS5_CONF = /u01/app/oracle/product/1020/network/krb5/krb5.conf

SQLNET.KERBEROS5_CC_NAME =
/u01/app/oracle/product/1020/network/krb5/krbcache

SQLNET.KERBEROS5_CONF_MIT = true

SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
```

Optional kann die Datei `sqlnet.ora` – sowohl auf dem Client als auch auf dem Server – mit Logging- und Trace-Parametern versehen werden, um im Fehlerfall ausführliche Meldungen zu generieren:

```
# Server: Tracing Logging nur im Bedarfsfall
TRACE_LEVEL_SERVER = SUPPORT
TRACE_FILE_SERVER = NETserver.ora
TRACE_DIRECTORY_SERVER = /u01/app/oracle/product/1020/network/network/trace
TRACE_TIMESTAMP_SERVER = TRUE

# Client: Tracing Logging nur im Bedarfsfall
TRACE_LEVEL_CLIENT=16
TRACE_DIRECTORY_CLIENT=/u01/oracle/1020client/network/network/trace
TRACE_UNIQUE_CLIENT=on
TRACE_FILE_CLIENT=kerb_client
# Okinit: Tracing
TRACE_LEVEL_OKINIT=16
TRACE_DIRECTORY_OKINIT=/u01/oracle/1020client/network/network/trace
TRACE_FILE_OKINIT=kerb_okinit
```

Zum Testen der neuen Kerberos-Anbindung kann nun beispielsweise folgender Benutzer im Active Directory angelegt werden:

```
Username/DN CN=testuser,CN=Users,DC=dbc,DC=de
Logon Name testuser@dbc.de
msDS-PrincipalName DBC\testuser
userPrincipalName testuser@dbc.de
```

Damit sich nun `testuser` an der Datenbank anmelden kann ist, ist dort folgender Benutzer anzulegen:

```
CREATE USER "TESTUSER@DBC.DE" IDENTIFIED EXTERNALLY;

GRANT connect, resource TO "TESTUSER@DBC.DE";
```

Wegen des Sonderzeichens "@" ist die Namensangabe auf jeden Fall in doppelte Hochkommas einzuschließen.

Nun kann ein erster Connect-Test durchgeführt werden. Von einem Unix-System aus, auf dem der Oracle-Client wie beschrieben installiert wurde, wird wie folgt vorgegangen (bei Windows-Systemen sollte das TGT bereits durch die Anmeldung vorliegen):

- Kerberos-Anmeldung und Erhalt des "`Ticket Granting Ticket"' (TGT)

```
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:
```

- Explizite Prüfung des TGT über `oklist` daselbst:

```
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
```

- Mit diesem TGT kann nun die Verbindung zum Zielsystem wie folgt angefordert werden:

```
sqlplus /@zieldb
```

Nach dem erfolgreichen `connect` kann der Benutzer im Sql*Plus nun wie gewohnt über `show user` geprüft werden.

Die Konfigurationsdateien müssen nun auf allen beteiligten Client- und Server-Rechnern verteilt werden.

Enterprise User – eine Einführung

Überall dort, wo die Kerberos Authentifizierung zwar genutzt werden soll, die Namen der in der Datenbank angelegten User jedoch nicht den oben dargestellten Namenskonventionen der Principal User genügen können, bietet sich eine interessante Alternative an: Mit Hilfe von Enterprise Benutzern, die in einem Verzeichnisdienst – beispielsweise Oracle Internet Directory – angelegt und mit globalen Benutzern der Datenbank verknüpft werden, kann ein per Kerberos authentifizierter Benutzer mit einem *shared schema* der Datenbank verbunden werden. Die Zuteilung der notwendigen Privilegien erfolgt über Enterprise Rollen und diesen zugeordneten globalen Rollen auf dem Zielsystem.

Die Darstellung aller konfiguratorischen Details dieses Szenarios würde den Rahmen dieser Darstellung sprengen und soll aus diesem Grunde hier nur stichwortartig zusammengefasst werden. Die Darstellung konzentriert sich auf eine Variante der Realisierung, andere sind technisch machbar. Beispielsweise kann Active Directory statt Internet Directory für die Konfiguration der Enterprise Benutzer eingesetzt werden. Es versteht sich, dass hierfür der Konfigurationsprozess unterschiedlich ausfällt.

- Konfiguration der Kerberos-Authentifizierung wie oben dargestellt. Verbindugstests mit einem entsprechenden Testbenutzer. Da der Verzeichnisdienst nicht die Kerberos-Authentifizierung initiiert, sondern lediglich für die Zuordnung des Kerberos Benutzers zu einem Enterprise Benutzer zuständig ist, muss die Authentifizierung zunächst unabhängig von diesem konfiguriert und gestestet werden.
- Installation und Konfiguration von Weblogic Server, einer Repository Datenbank und Oracle Fusion Middleware mit der Komponente „Identity Management“. Oracle Internet Directory ist Bestandteil dieser Komponente.

- Anbindung der Verzeichnisdienstes and die Datenbankserver (Datei ldap.ora) und Registrierung der Zieldatenbanken im Internet Directory mit Hilfe des „Database Configuration Assistant“.
- Anlegen von *shared schemas* und globalen Rollen in den Zielsystemen.
- Anlegen von Enterprise Benutzern im Verzeichnisdienst und Verknüpfen dieser Benutzer mit den globalen Benutzern der registrierten Zieldatenbanken. Statt die Benutzer aktiv anzulegen, existieren vielfältige Möglichkeiten der Verknüpfung mit oder Übernahme von Benutzerdaten aus Drittsystemen.
- Anlegen von Enterprise Rollen im Verzeichnisdienst und Zuordnung dieser Rollen zu Enterprise Benutzern und globalen Rollen der Zielsysteme.
- Eintrag des Kerberos Principal Name jedes Enterprise Benutzers im Verzeichnisdienst. Über diesen wird letzten Endes die Zuordnung zu den *shared schema* geregelt.

Die Anmeldung an der Datenbank erfolgt letzten Endes mit gleicher Syntax, wie bereits dargestellt wurde. Der Benutzer wird aber hier mit dem entsprechenden *shared schema* verbunden.

Kontaktadresse:

Dr. Günter Unbescheid
Database Consult GmbH
Laich 9 1/10
D-83676 Jachenau

Telefon: +49 (0) 8043-1010
Fax: +49 (0) 8043-1011
E-Mail g.unbescheid@database-consult.de
Internet: www.database-consult.de