

Kerberos - Single Sign On ganz einfach

DOAG Konferenz 2011

Jürgen Kühn
Senior Consultant
Trivadis GmbH

16. November 2011
Nürnberg

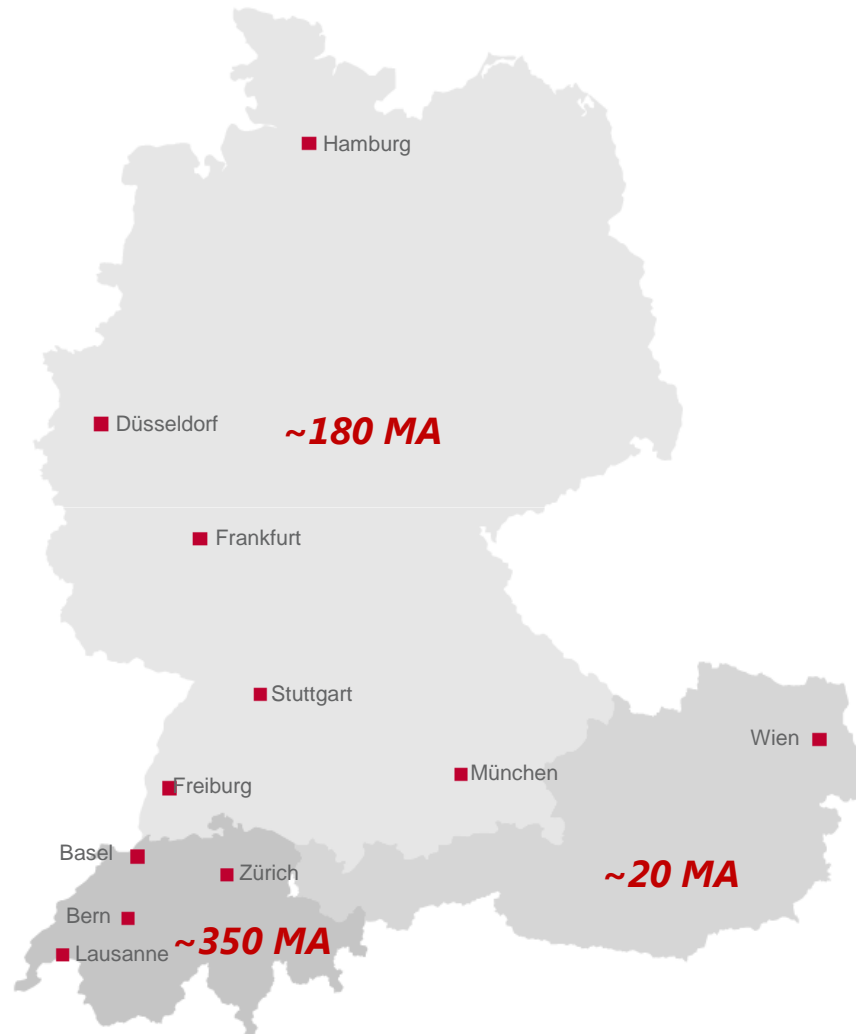
BASEL BERN LAUSANNE ZÜRICH DÜSSELDORF FRANKFURT A.M. FREIBURG I.BR. HAMBURG MÜNCHEN STUTTGART WIEN



2011 © Trivadis

trivadis
makes IT easier. ■ ■ ■

Trivadis Facts & Figures



11 Trivadis Niederlassungen mit über 550 Mitarbeitern

Finanziell unabhängig und nachhaltig profitabel

Kennzahlen 2010

- Umsatz CHF 101 / EUR 73 Mio.
- Dienstleistungen für über 700 Kunden in mehr als 1'800 Projekten
- Über 170 Service Level Agreements
- Mehr als 5'000 Trainingsteilnehmer
- Forschungs- und Entwicklungsbudget: CHF 5.0 / EUR 3.6 Mio.

Das Besondere

Kundenindividuelle Lösungskompetenz und Herstellerunabhängigkeit

- bietet fundierte Methodenkenntnisse und eigenentwickelte Vorgehensweisen
- garantiert wiederholbare Qualität und Realisierungssicherheit

Technologiekompetenz

- hat über 17 Jahre Expertise in Oracle und Microsoft
- verfügt über ein eigenes Technology Center und setzt auf technologische Exzellenz

Lösungs- und Integrations-Know-how

- hat eine breite, branchenübergreifende Kundenbasis und jährlich über 1800 Projekte
- verbindet technologisches Spezialistenwissen mit dem Verständnis für die Business-Spezifika des Kunden

Begleitung über den gesamten IT-Projekt- Lifecycle

- begleitet den gesamten IT-Projekt-Lifecycle mit einem modularen Dienstleistungsportfolio
- bietet für jeden „Reifegrad“ die passende Dienstleistungs- und Lösungskombination



Agenda

1. Kerberos
2. Active Directory Server
3. Datenbankserver
4. Client
5. Stolperfallen
6. Diskussion

Kerberos (1)

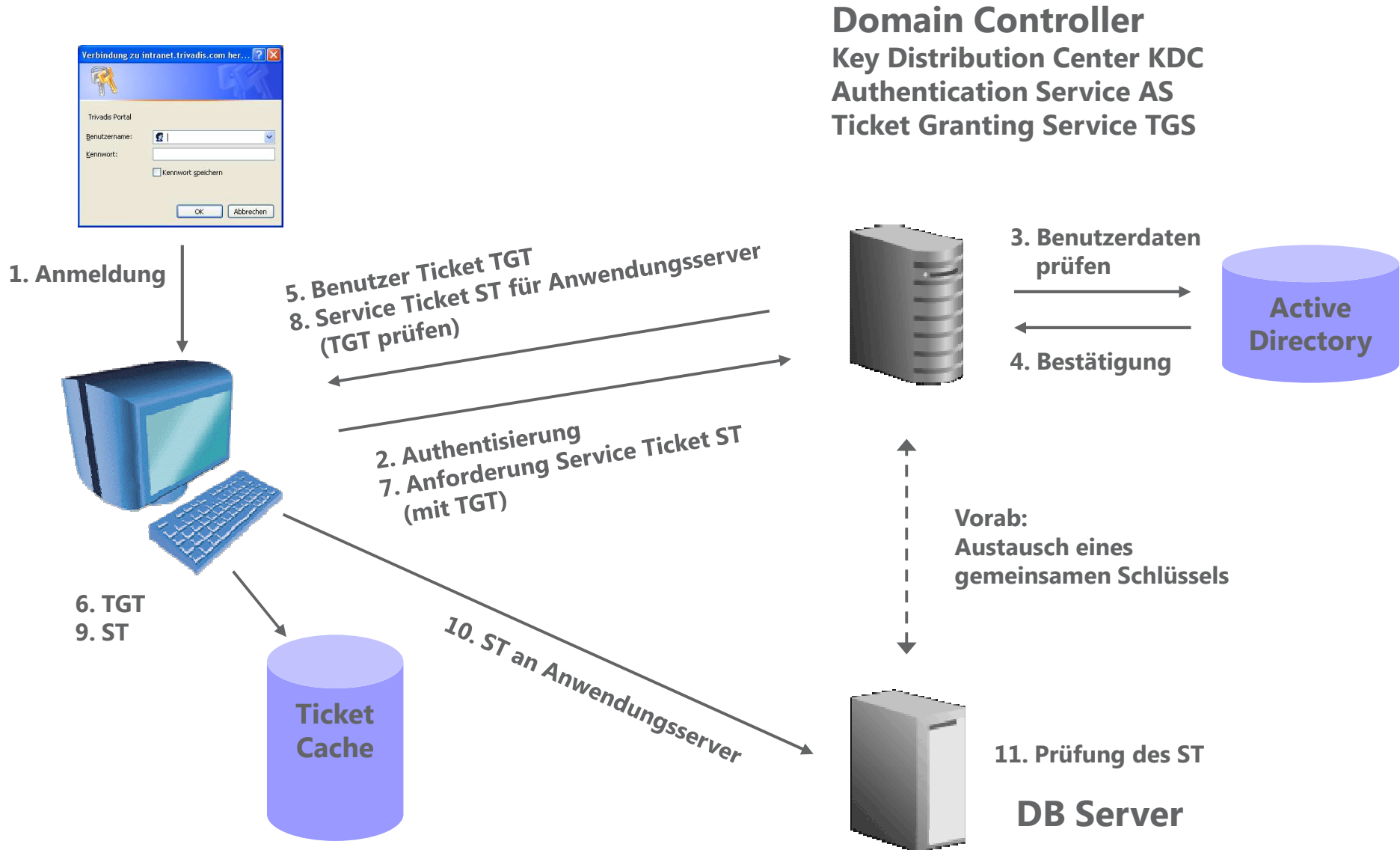
- Griechisch Κέρβερος
- Latinisiert Cerberus
- Im Deutschen auch Zerberus
- "Dämon der Grube"
- In der griechischen Mythologie der Höllenhund Eingang zur Unterwelt bewacht.



*"Auch den Kerberos sah ich, mit bissigen Zähnen bewaffnet
Böse rollt er die Augen, den Schlund des Hades bewachend.
Wagt es einer der Toten an ihm vorbei sich zu schleichen,
So schlägt er die Zähne tief und schmerzhaft ins Fleisch der Entfliehenden
Und schleppt sie zurück unter Qualen,
Der böse, der bissige Wächter."*

(Quelle: Odyssee von Homer)

Kerberos (2)



Agenda

1. Kerberos
2. Active Directory Server
3. Datenbankserver
4. Client
5. Stolperfallen
6. Diskussion

Active Directory Server (1)

- Anlegen eines Active Directory Kontos für den Datenbankserver
 - Alternativ ein Konto für jeden Datenbankservice

The screenshot shows the 'New Object - User' dialog box with the following fields and values:

- Create in:** tciamfirma.tvd/OidUsers
- First name:** dbserver1
- Initials:** (empty)
- Last name:** (empty)
- Full name:** dbserver1
- User logon name:** dbserver1
- Domain:** @tciamfirma.tvd
- User logon name (pre-Windows 2000):** TCIAMFIRMA\ dbserver1

Buttons at the bottom: < Back, Next >, Cancel.

The screenshot shows the 'New Object - User' dialog box with the following fields and options:

- Password:** (masked with dots)
- Confirm password:** (masked with dots)
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

Buttons at the bottom: < Back, Next >, Cancel.

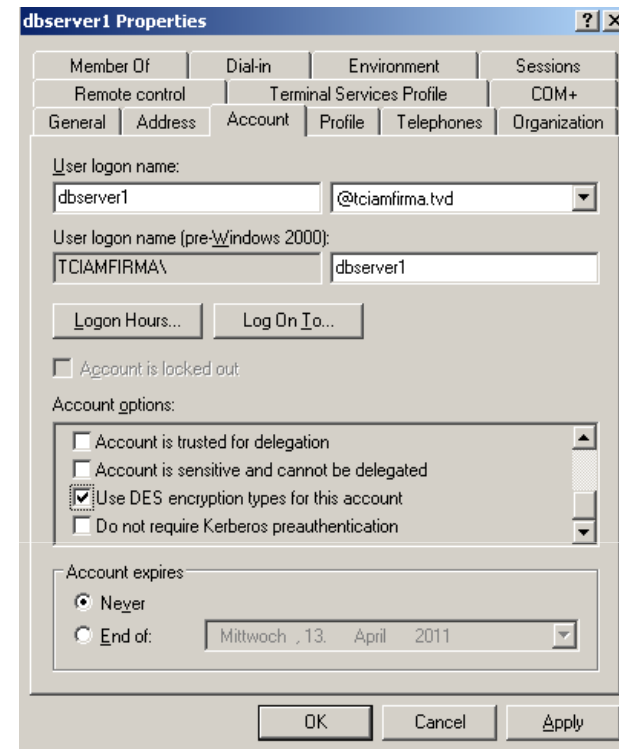
Active Directory Server (2)

- Service Principal Name SPN anlegen
- keytab File erzeugen
- ktpass
 - setzt das Passwort für den AD User "dbserver1" auf den unter "-pass" angegebenen Wert.
 - wählt mit "+desonly" DES als einzigen erlaubten kryptografischen Algorithmus aus (wird für Kerberos Kompatibilität mit Linux benötigt).
 - setzt den Service Principal Name auf "oracle/dbserver1.tvd"
 - erstellt das keytab File "dbserver1.keytab" für dbserver1

```
C:\Program Files\Support Tools>ktpass.exe -princ
oracle/dbserver1.tvd@TCIAMFIRMA.TVD -mapuser dbserver1 -pass
oracle +desonly -crypto des-cbc-md5 -out c:\dbserver1.keytab
Targeting domain controller: pdc.tciamfirma.tvd
Successfully mapped oracle/dbserver1.tvd to dbserver1.
```

Active Directory Server (3)

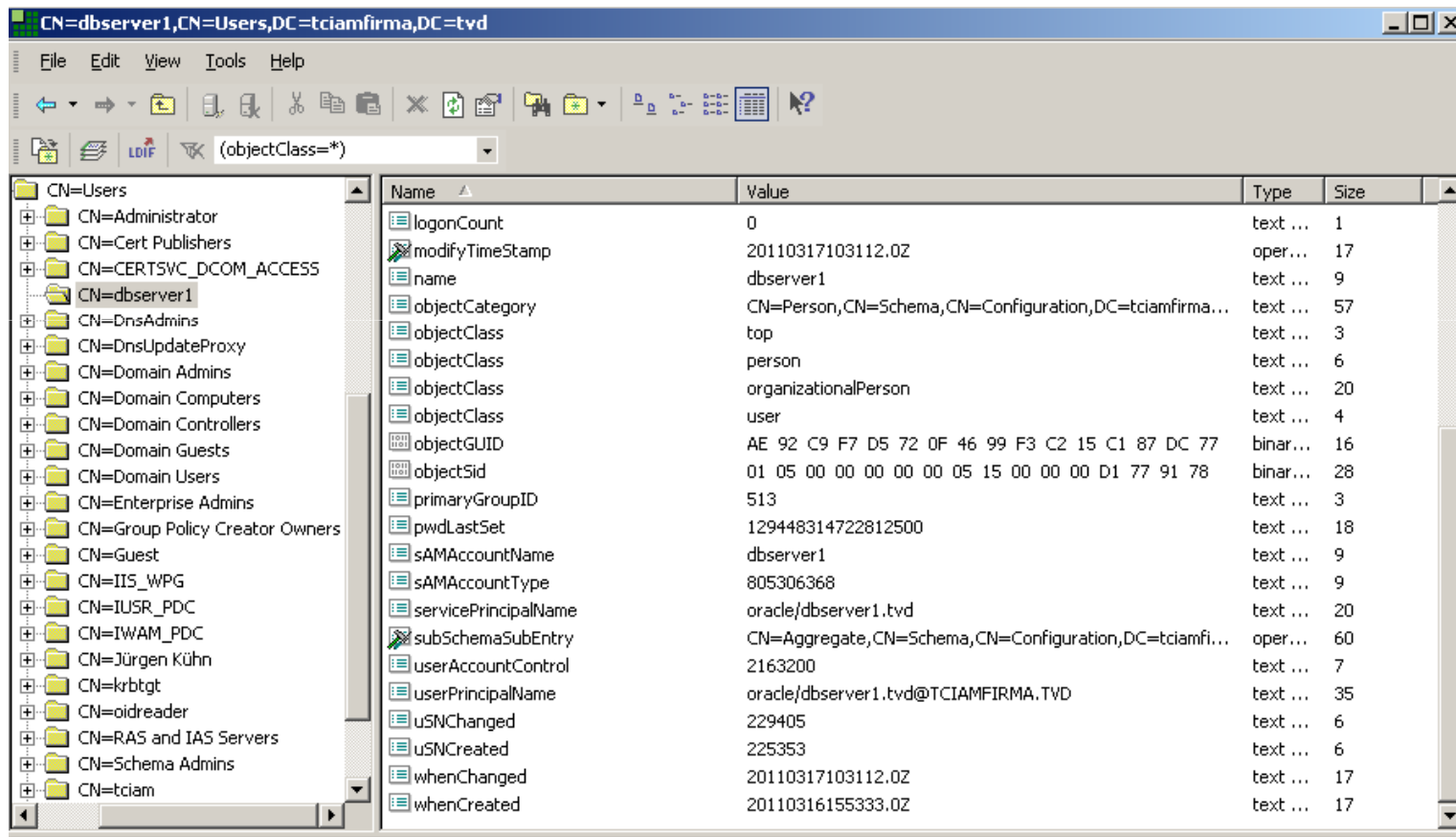
- Eigenschaften des Benutzerkontos
- SPN mit setspn kontrollieren



```
C:\Program Files\Support Tools>setspn -L dbserver1
Registered ServicePrincipalNames for
CN=dbserver1,DC=tciamfirma,DC=tvd:
    oracle/dbserver1.tvd
```

Active Directory Server (4)

- Service Principal Name SPN in einem LDAP Browser



Agenda

1. Kerberos
2. Active Directory Server
3. Datenbankserver
4. Client
5. Stolperfallen
6. Diskussion



Datenbankserver (1)

- Advanced Security Option muss installiert sein
- keytab File in ein beliebiges Verzeichnis auf dem Server kopieren
 - TNS_ADMIN ist auch erlaubt 😊
- Kerberos Konfigurationsdatei "krb5.conf" anpassen
- Oracle Konfigurationsdatei "sqlnet.ora" anpassen

Datenbankserver (2)

keytab File

- Kann mehrere Einträge enthalten

Jeder Eintrag enthält die Daten aus dem SPN im AD

- die Kerberos Realm
- den Service Name
- Name des physikalischen Servers
- Den aus dem AD exportierten geheimen Schlüssel

```
00000000h: 05 02 00 00 00 3E 00 02 00 0E 54 43 49 41 4D 46 ; .....>....TCIAMF
00000010h: 49 52 4D 41 2E 54 56 44 00 06 6F 72 61 63 6C 65 ; IRMA.TVD..oracle
00000020h: 00 0D 64 62 73 65 72 76 65 72 31 2E 74 76 64 00 ; ..dbserver1.tvd.
00000030h: 00 00 00 00 00 00 00 04 00 01 00 08 76 52 52 1F ; .....vRR.
00000040h: A2 BC 38 83 ; 8f
```

Datenbankserver (3)

krb5.conf anpassen

- Zuordnung Kerberos Realm zu Windows Domäne
- Key Distribution Center KDC eintragen

```
#####krb5.conf DB Server
[libdefaults]
default_realm = TCIAMFIRMA.TVD
clockskew=300

[realms]
TCIAMFIRMA.TVD = {
    kdc = pdc.tvd
}

[domain_realm]
.tvd = TCIAMFIRMA.TVD
tvd = TCIAMFIRMA.TVD           # nicht sinnvoll
specialhost.tvd = OTHER.REALM
```

Datenbankserver (4)

sqlnet.ora anpassen

- Kerberos als Authentisierungsmethode eintragen
- Kerberos Service Name eintragen
- Pfad zur krb5.conf Datei und zum keytab File eintragen
- Pfad zum Ticket Cache
 - Muss das sein?

```
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE=oracle
SQLNET.KERBEROS5_CONF=/u01/app/oracle/product/10.2.0/db_1/network/admin/kr
b5.conf
SQLNET.KERBEROS5_CONF_MIT=TRUE
SQLNET.AUTHENTICATION_SERVICES=(BEQ,KERBEROS5)
SQLNET.KERBEROS5_KEYTAB=/u01/app/oracle/product/10.2.0/db_1/network/admin/
dbserver1.keytab
#Wenn ein Ticket auf dem Unix Host benötigt wird
SQLNET.KERBEROS5_CC_NAME=/u01/app/oracle/product/10.2.0/db_1/network/admin
/krb.tg
```


Datenbankserver (5)

Datenbankbenutzer anlegen

- Externally authenticated
- Mit Windows Benutzernamen

```
SQL> create user "JUK@TCIAMFIRMA.TVD" identified externally;  
User created.
```

```
SQL> grant connect, resource to "JUK@TCIAMFIRMA.TVD";  
Grant succeeded.
```

Agenda

1. Kerberos
2. Active Directory Server
3. Datenbankserver
4. Client
5. Stolperfallen
6. Diskussion

Client (1)

- Advanced Security Option muss installiert sein
- sqlnet.ora anpassen
 - Kerberos als Authentisierungsmethode eintragen
 - Kerberos Service Name nicht erforderlich
 - Der Service Name wird vom Datenbankserver übermittelt
- okinit nicht erforderlich
- Angabe des Ticket Caches

```
####sqlnet.ora
SQLNET.KERBEROS5_CONF=C:\u01\app\oracle\product\10.2.0\client\net
work\admin\krb5.conf
SQLNET.KERBEROS5_CONF_MIT=TRUE
SQLNET.AUTHENTICATION_SERVICES=(BEQ, KERBEROS5)
#SQLNET.AUTHENTICATION_KERBEROS5_SERVICE=oracle
SQLNET.KERBEROS5_CC_NAME = OSMSFT://
```

Client (2)

- Anmeldung an der Datenbank

```
C:\Program Files\Support Tools>sqlplus /@db10a
```

```
SQL*Plus: Release 10.2.0.1.0 - Production on Mi Okt 19 21:38:22  
2011
```

```
Copyright (c) 1982, 2005, Oracle. All rights reserved.
```

```
Verbunden mit:
```

```
Oracle Database 10g Enterprise Edition Release 10.2.0.4.0 -  
Production
```

```
With the Partitioning, OLAP, Data Mining and Real Application  
Testing options
```

```
SQL> show user
```

```
USER ist "JUK@TCIAMFIRMA.TVD"
```

```
SQL>
```

Client (3)

- Tickets anzeigen mit Microsoft Tool "klist"

```
C:\Program Files\Support Tools>klist tickets
```

```
Cached Tickets: (2)
```

```
Server: krbtgt/TCIAMFIRMA.TVD@TCIAMFIRMA.TVD
```

```
  KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
```

```
  End Time: 10/20/2011 7:38:02
```

```
  Renew Time: 10/26/2011 21:38:02
```

```
Server: oracle/dbserver1.tvd@TCIAMFIRMA.TVD
```

```
  KerbTicket Encryption Type: Kerberos DES-CBC-MD5
```

```
  End Time: 10/20/2011 7:38:02
```

```
  Renew Time: 10/26/2011 21:38:02
```

Client (4)

- Tickets anzeigen mit Oracle Tool "oklist"

```
C:\Program Files\Support Tools>oklist

Kerberos Utilities for 32-bit Windows: Version 10.2.0.1.0 - Production on
19-OKT
-2011 21:41:37

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

Ticket cache: win2kcc
Default principal: juk@TCIAMFIRMA.TVD

Valid Starting          Expires                Principal
19-Okt-2011 21:38:02   20-Okt-2011 07:38:02
krbtgt/TCIAMFIRMA.TVD@TCIAMFIRMA.TVD
renew until 26-Okt-2011 21:38:02
19-Okt-2011 21:38:22   20-Okt-2011 07:38:02
oracle/dbserver1.tvd@TCIAMFIRMA.TVD
renew until 26-Okt-2011 21:38:02
```

Agenda

1. Kerberos
2. Active Directory Server
3. Datenbankserver
4. Client
5. Stolperfallen
6. Diskussion



Stolperfallen

- Service Principal Name im Active Directory
 - Darf auf gar keinen Fall doppelt vorkommen
 - Gegebenenfalls Prüfung mittels Skript
- Ticketgröße
 - Standardgröße 16 KB
 - Basisinformationen 1200 Bytes
 - Jede Gruppenzugehörigkeit 40 Byte
 - Vergrößerung über Eintrag in Registry
 - Sharepoint hat ein Problem mit Token-Größen über 64 KB
- Client Ticket auf dem Datenbankserver
 - Bug 5054469: DATABASE AUTHENTICATED USERS REQUIRE KERBEROS CREDENTIAL CACHE TO CONNECT
 - Development is planning to solve this completely in Oracle 12
 - Workarounds: Unterschiedliche sqlnet.ora oder Dummy AD Konto

DEN TRIVADIS-
STAND FINDEN
SIE AUF

**EBENE 3,
STAND NR. 304**

Trivadis GmbH

Jürgen Kühn

Werdener Straße 4-6
40227 Düsseldorf

Tel. +49 211 586664 70

Fax +49 211 586664 71

info@trivadis.com

www.trivadis.com

BASEL

BERN

LAUSANNE

ZÜRICH

DÜSSELDORF

FRANKFURT A.M.

FREIBURG I.BR.

HAMBURG

MÜNCHEN

STUTTGART

WIEN



2011 © Trivadis

trivadis
makes IT easier. ■ ■ ■