Kerberos and Databases a Success…

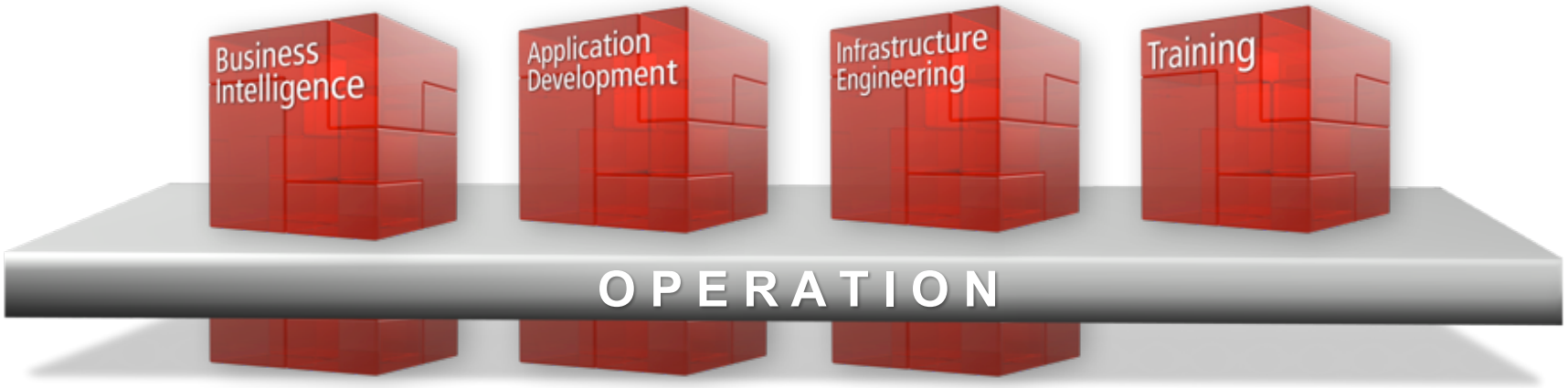
… or the History of a Varied Journey

Stefan Oehrli

@stefanoehrli www.oradba.ch

Our company.

Trivadis is a market leader in IT consulting, system integration, solution engineering and the provision of IT services focusing on ORACLE and Microsoft technologies
in Switzerland, Germany, Austria and Denmark. We offer our services in the following strategic business fields:



Trivadis Services takes over the interacting operation of your IT systems.

trivadis
makes IT easier.

With over 600 specialists and IT experts in your region.

- 14 Trivadis branches and more than 600 employees
- 200 Service Level Agreements
- Over 4,000 training participants
- Research and development budget: CHF 5.0 million
- Financially self-supporting and sustainably profitable
- Experience from more than 1,900 projects per year at over 800 customers

trivadis
makes IT easier.

Technology on its own won't help you.

You need to know how to use it properly.

trivadis
makes IT easier.

Stefan Oehrli

Solution Manager BDS SEC / Trivadis Partner

- Working since 1997 in IT
- Since 2008 with Trivadis AG
- Since 2010 Discipline Manager SEC INFR
- Since 2014 Solution Manager BDS Security

IT Experience

- Database Administration and Database security solutions
- Administration complex, heterogeneous Environments
- Team leader of a team of database administrators

Specialization

- Database Security und Operation
- Security Concepts and Implementations
- Security Reviews
- Oracle Backup & Recovery
- Enterprise User Security and Oracle Unified Directory

Skills

- Backup & Recovery
- Oracle Advanced Security
- Oracle AVDF and DB Vault
- Oracle Directory Services
- Team / Project Management
- Lector for Trivadis Database Security (O-SEC) and Backup & Recovery (O-BR/O-BR-Pract) Training

trivadis makes IT easier.

Agenda

1. Introduction
2. Kerberos: The Network Authentication Protocol
3. Setup and Configure
4. First Steps
5. Advanced Use Cases
6. Oracle Net Services and Kerberos Troubleshooting
7. Round Up

trivadis
makes IT easier.

Introduction

trivadis
makes IT easier.

Introduction

- Greek Κέρβερος
- Latinisiert Cerberus, German Zerberus
- A moon of Pluto
- "Dämon der Grube"
- In Greek mythology it is the hell hound and gatekeeper who guards the entrance to the underworld..

"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)

trivadis makes IT easier.

But why do we need a gatekeeper from hell?

- Avoid unsecure logins
- Start using strong authentication
- Increased security requirements
  - Compliance requirements
  - Legal requirements eg. GDPR
- Improve user experience
  - SSO Single Sign On / Logon
- It is Friday and the DBA has nothing to do... ☺

trivadis makes IT easier.

But it's gonna cost...

- A small update to the Oracle documentation…
  - …which is overlooked quickly ☺
- Oracle® Database Licensing Information, Oracle Advanced Security

*Network encryption (native network encryption and SSL/TLS) and strong authentication services (**Kerberos**, PKI, and RADIUS) are no longer part of Oracle Advanced Security and are available in all licensed editions of all supported releases of the Oracle database.*

- Introduced with Oracle 12c Release 1
- Adjusted with Oracle 11.2.0.4 for **any** licensed Oracle Database
  - Require a valid Oracle License for 11g, 12g etc.
  - Valid for Standard and Enterprise Editions

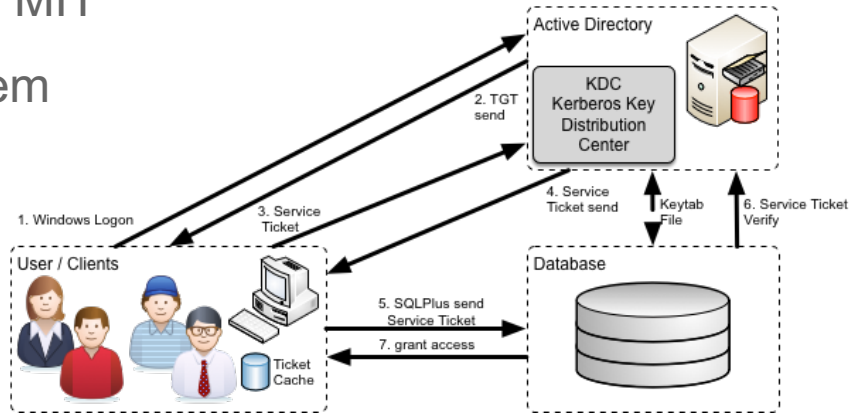
trivadis makes IT easier.

Kerberos: The Network Authentication Protocol

trivadis
makes IT easier.

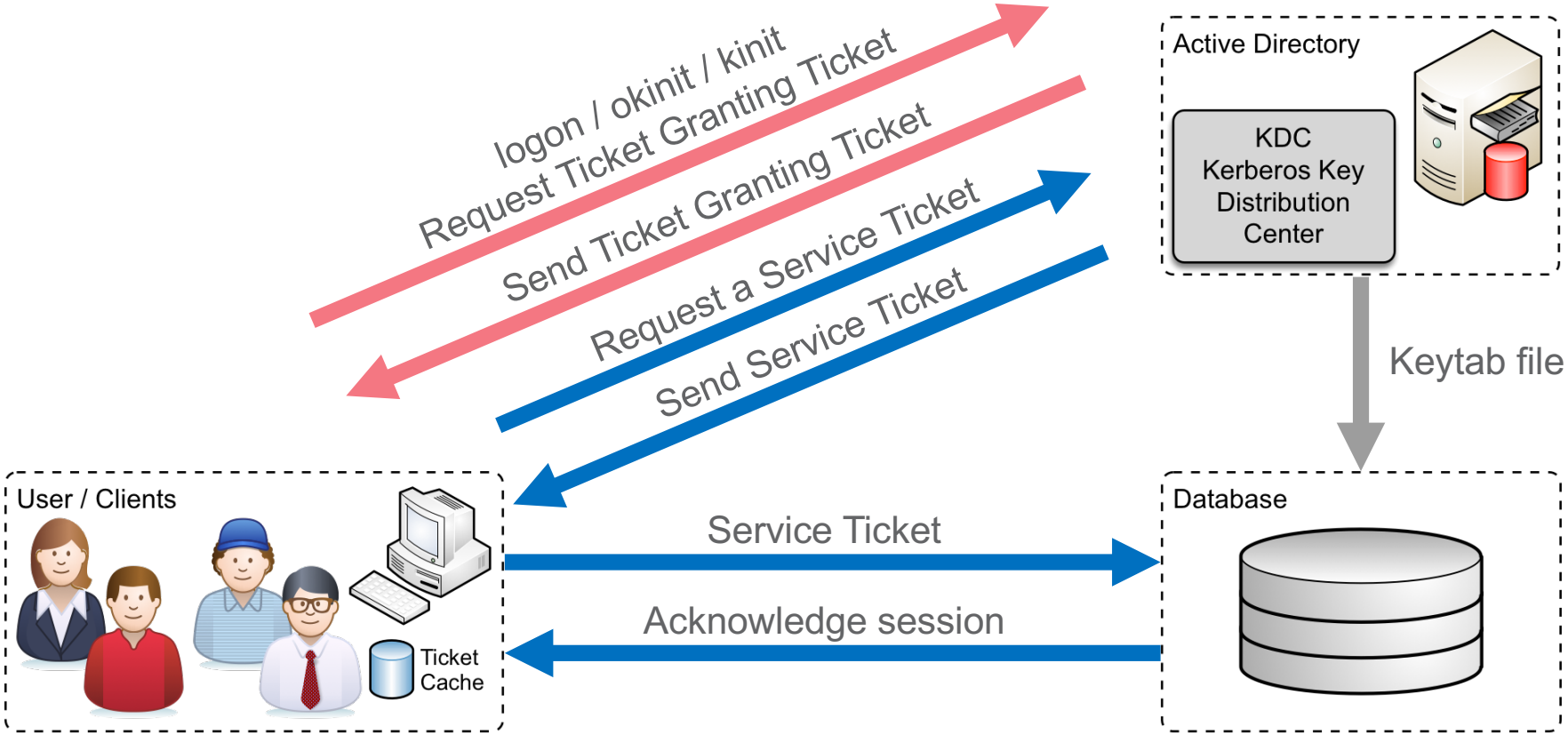
Kerberos in a Nutshell

- Network Authentication Protocol developed by MIT
- Uses a trusted third-party Authentication System KDC (not KGB…)
  - “strong” Authentication
- Basis for a couple of Services and Tools
- Windows Servers
- Requires three parties
  - KDC with Authentication Service and Ticket Granting Service
  - Service or Service Principle who provide a Service
  - Client who request access
- Has been around for some time now



trivadis
makes IT easier.

Kerberos Authentication Workflow



trivadis
makes IT easier.

Terms

- KDC Key Distribution Center
- AS Authentication Service
- TGS Ticket Granting Service
- TGT Ticket Granting Ticket
- Key Table keytab
  stores long-term keys for one or more principals
- Credential Cache / “ccache”
  holds the Kerberos credentials while they remain valid

trivadis
makes IT easier.

More Information on Kerberos

- Massachusetts Institute of Technology (MIT), *Kerberos: The Network Authentication Protocol* https://web.mit.edu/kerberos
- Master Note For Kerberos Authentication (Doc ID 1375853.1) https://support.oracle.com/epmos/faces/DocumentDisplay?id=1375853.1
- Configuring ASO Kerberos Authentication with a MS Windows 2008 R2 AD KDC https://support.oracle.com/epmos/faces/DocumentDisplay?id=1304004.1
- Explain like I'm 5: Kerberos http://www.roguelynn.com/words/explain-like-im-5-kerberos
- Microsoft Developer Network, *Kerberos Explained* https://msdn.microsoft.com/en-us/library/bb742516.aspx
- Kerberos explained in pictures http://danlebrero.com/2017/03/26/Kerberos-explained-in-pictures

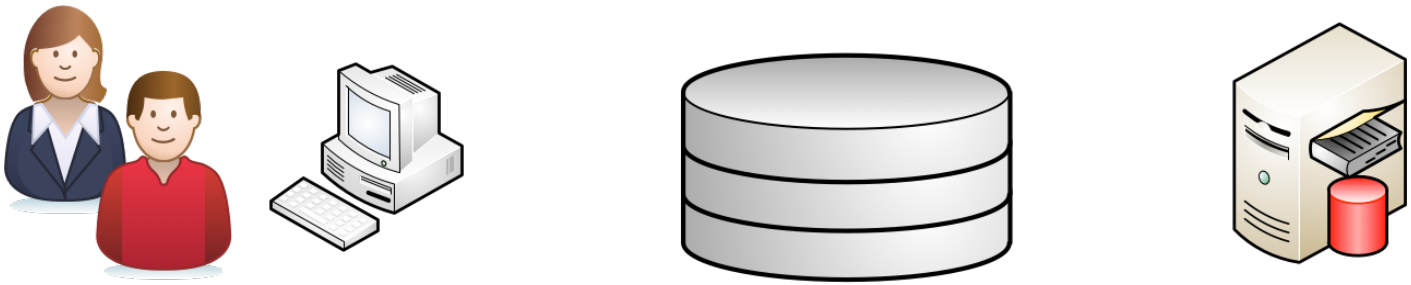
trivadis makes IT easier.

Setup and Configure

trivadis
makes IT easier.

Architecture

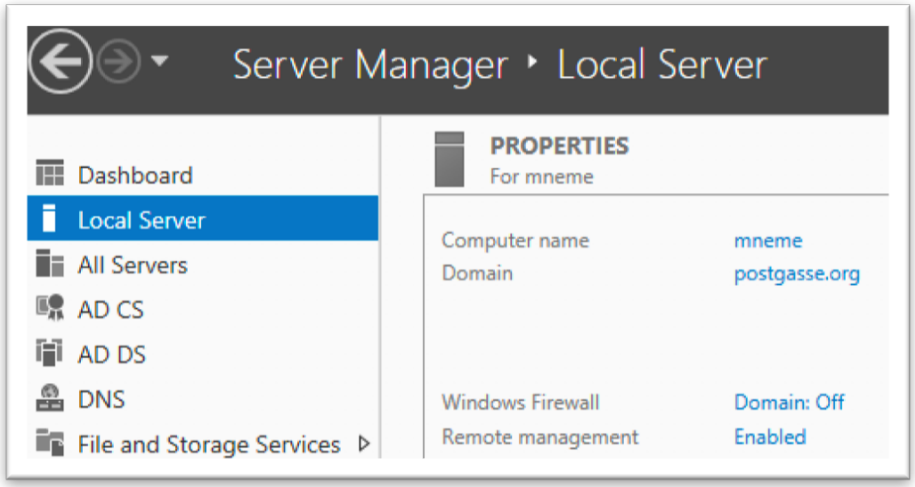
- MS Active Directory 2012 R2 Server
- Database Server with Oracle 11g, 12c
  - Enterprise and Standard Edition
- Client with Oracle Client (Full or Instant Client)
  - Mac OS or VM Host
  - MS Active Directory VM as “Client”

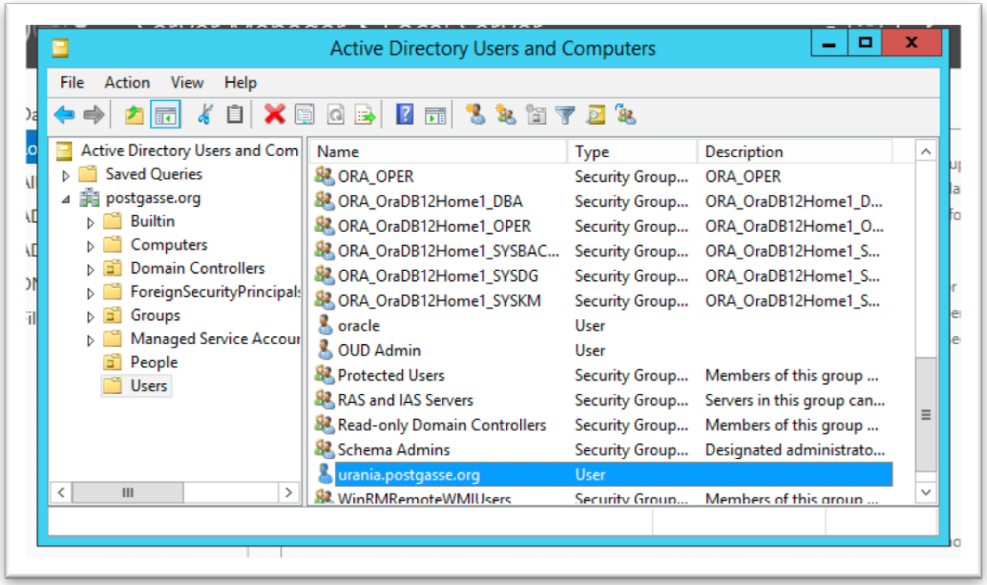


trivadis makes IT easier.

KDC / MS Active Directory

- Setup of a simple Windows 2012 R2 Server with Active Directory Role
  - Including AD, DNS, CS Services
- Create Containers for User, Groups etc
- Create a bunch of Test Users



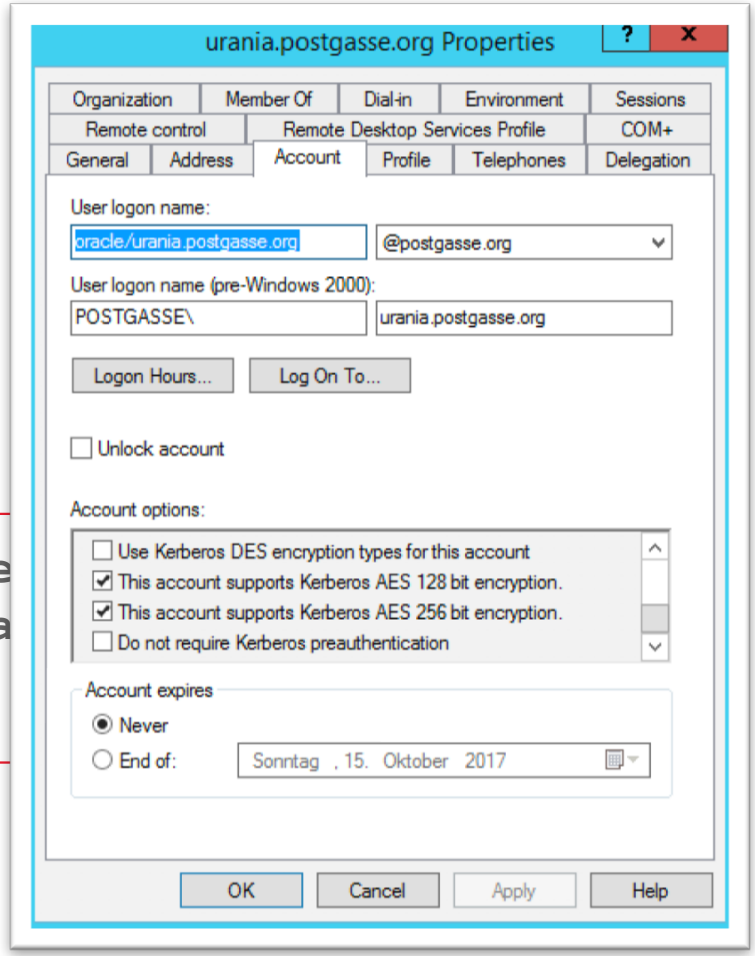


trivadis
makes IT easier.

KDC / MS Active Directory

- Create a Service Principle for the Database Service
  - One keytab file per DB Server
  - Usable Key Types / Crypto's highly depended AD and Oracle Version

```
C:\>ktpass.exe -princ oracle/urania.postgasse
-mapuser urania.postgasse.org -crypto all -pa
c:\urania.keytab
```



trivadis makes IT easier.

Database Server Configuration

- Kerberos adaptors are part of any Oracle Enterprise Edition installation
- Configured with *sqlnet.ora* and *krb5.conf*
- Keytab file has to be copied to Database Server
- DNS lookup and revers lookup has to work
- Servers have to have the same time (NTP, time synchronization)

trivadis
makes IT easier.

Database Server Configuration (1)

- Configured with *sqlnet.ora*

```
SQLNET.AUTHENTICATION_SERVICES = (BEQ, KERBEROS5) # KERBEROS5PRE
SQLNET.KERBEROS5_KEYTAB        = /u00/app/oracle/network/admin/urania.keytab
SQLNET.KERBEROS5_CC_NAME       = /u00/app/oracle/network/admin/krbcache
SQLNET.KERBEROS5_CONF          = /u00/app/oracle/network/admin/krb5.conf
SQLNET.KERBEROS5_CONF_MIT      = TRUE
SQLNET.FALLBACK_AUTHENTICATION = TRUE
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
```


trivadis makes IT easier.

Database Server Configuration (2)

- And a *krb5.conf* File

```
####krb5.conf DB Server
[realms]
 POSTGASSE.ORG = {
   kdc = mneme.postgasse.org
   admin_server = mneme.postgasse.org
}

[domain_realm]
.postgasse.org = POSTGASSE.ORG
postgasse.org = POSTGASSE.ORG
```


trivadis makes IT easier.

Database Server Configuration (3)

- More *krb5.conf* options but in general not used in Oracle Kerberos

```
####krb5.conf DB Server
[logging]
default      = FILE:/u00/app/oracle/network/log/krb5lib.log
Kdc.         = FILE:/u00/app/oracle/network/log/krb5kdc.log
admin_server = FILE:/u00/app/oracle/network/log/kadmind.log

[libdefaults]
 default_tgs_enctypes = aes128-cts-hmac-sha1-96 arcfour-hmac arcfour-hmac-md5
 default_tkt_enctypes = aes128-cts-hmac-sha1-96 arcfour-hmac arcfour-hmac-md5
 permitted_enctypes   = aes128-cts-hmac-sha1-96 arcfour-hmac arcfour-hmac-md5
 default_realm = POSTGASSE.ORG
 clockskew=300
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
```


trivadis makes IT easier.

What about Standard Edition?

- By default Oracle Standard Edition does not support Kerberos Authentication
  - No dependence on ASO anymore
- How To Enable Radius and Kerberos Adapters in Oracle Database 11g Standard Edition https://support.oracle.com/epmos/faces/DocumentDisplay?id=2145731.1
- Current status can be checked with **`adapters`**

```
adapters
Installed Oracle Net transport protocols are:
    IPC
    BEQ
...
    AES 256-bit encryption
    MD5 crypto-checksumming
    SHA-1 crypto-checksumming
```


trivadis makes IT easier.

What about Standard Edition?

- Solution requires relink of binaries

```
cd $cdh/lib
cp nautab.o nautab_se.o.dbl
cp nautab_ee.o.dbl nautab.o
relink all
```

- New adapters for Radius and Kerberos

```
adapters
Installed Oracle Net transport protocols are:
    IPC
    BEQ
...
    SHA-1 crypto-checksumming
    Kerberos v5 authentication
    RADIUS authentication
```


trivadis makes IT easier.

Database Users

- Create Kerberos enabled database users

```
CREATE USER "soe@POSTGASSE.ORG" IDENTIFIED EXTERNALLY;
CREATE USER joe IDENTIFIED EXTERNALLY AS 'joe@POSTGASSE.ORG';
```

- Alter existing users

```
ALTER USER scott IDENTIFIED EXTERNALLY
AS 'scott@POSTGASSE.ORG';
ALTER USER "soe@POSTGASSE.ORG" IDENTIFIED EXTERNALLY;
```


trivadis makes IT easier.

Client Configuration (1)

- Install at least an Oracle Instant Client
  - Full client offers more comfort for engineering ☺
- Wisely choose the right version and patch level
  - Mixed Clients and Oracle Version 11.2.0.3, 11.2.0.4, 12.1.0.1, 12.2.0.1,…
- Adjust *sqlnet.ora* and *krb5.conf*

```
SQLNET.AUTHENTICATION_SERVICES=(BEQ, KERBEROS5PRE, KERBEROS5)
SQLNET.KERBEROS5_CONF=C:\u00\app\oracle\network\admin\krb5.conf
SQLNET.KERBEROS5_CONF_MIT=TRUE
SQLNET.KERBEROS5_CC_NAME = OSMSFT://
#SQLNET.KERBEROS5_CC_NAME = MSLSA:
```


trivadis makes IT easier.

Client Configuration (2)

- Create a *krb5.conf* File

```
####krb5.conf Client
[libdefaults]
 default_realm = POSTGASSE.ORG
 clockskew=300

[realms]
 POSTGASSE.ORG = {
   kdc = mneme.postgasse.org
   admin_server = mneme.postgasse.org
}

[domain_realm]
.postgasse.org = POSTGASSE.ORG
postgasse.org = POSTGASSE.ORG
```


trivadis makes IT easier.

Authentication – Kerberos

- Oracle 12.2.0.1 introduced automatic krb5.conf discovery from DNS

```
oracle@urania:/u00/app/oracle/network/admin/ [TDB122A] sqlplus /@TDB122A

SQL*Plus: Release 12.2.0.1.0 Production on Thu Sep 14 06:23:10 2017

Copyright (c) 1982, 2016, Oracle. All rights reserved.

Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production
SQL> select sys_context('userenv','authentication_method') from dual;
SYS_CONTEXT('USERENV','AUTHENTICATION_METHOD')
--------------------------------------------------------------------------------
KERBEROS
SQL> exit
Disconnected from Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit ProductionORA-24550:
signal received: [si_signo=7] [si_errno=0] [si_code=128] [si_int=-98422784] [si_ptr=0x7f9ffa223000]
[si_addr=(nil)]kpedbg_dmp_stack()+400<-kpeDbgCrash()+210<-kpeDbgSignalHandler()+121<-skgesig_sigaction
Handler()+272<-__sighandler()<-_int_free()+734<-nauztk5adisconnect()+3744<-snau_dis()+1436<-nadisc()+324<-
nsnadisc()+339<-nsclose()+727<-nioqds()+417<-upidhs()+210<-kpudtch()+513<-aficntdta()+107<-aficexf()+43<-
aficex()+366<-afiexi()+1086<-aficmd()+2914<-aficfd()+3053<-aficdr()+151<-afidrv()+5950<-main()+105<-
__libc_start_main()+245
Bus error (core dumped)
```


trivadis makes IT easier.

First Steps

trivadis
makes IT easier.

Kerberos Client Tools

- Oracle does provide a bunch of client tools
  - Mainly the “Oracle” version of the regular MIT Kerberos Tools
- Client tools are only part of the Database Binaries or Full Clients
- **`okinit`** / **`kinit`** obtains and caches Kerberos tickets
- **`oklist`** / **`klist`** display the list of tickets held
- **`okdstry / kdestroy`** remove credentials from the credentials cache file
- **`okcreate`** automates the creation of keytabs from the KDC or a service endpoint
  - Introduced with Oracle 12.2 but intend to be used on a real KDC

trivadis makes IT easier.

Windows Client

- Steps to use Kerberos authentication
  - Just login then you have a TGT
  - Start SQLPlus

```
soe@MNEME:C:\u00\app\oracle\network\admin\ [rdbms11204] sqlplus /@TDB122A
SQL*Plus: Release 11.2.0.4.0 Production on Fr Sep 15 10:53:44 2017
Copyright (c) 1982, 2013, Oracle.  All rights reserved.
Verbunden mit:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production
SQL> SELECT sys_context('userenv','authentication_method') FROM dual;
SYS_CONTEXT('USERENV','AUTHENTICATION_METHOD')
--------------------------------------------------------------------------------
KERBEROS
```


trivadis makes IT easier.

Unix Clients

- Manually get a Ticket Granting Ticket

```
oracle Urania:~/ [TDB122A] okinit soe
Kerberos Utilities for Linux: Version 12.2.0.1.0 - Production on 15-SEP-2017 10:57:34
Copyright (c) 1996, 2016 Oracle.  All rights reserved.
Configuration file : /u00/app/oracle/network/admin/krb5.conf.
Password for soe@POSTGASSE.ORG:
```

- Use SQLPlus

```
oracle@urania:~/ [TDB122A] sqlplus /@TDB112A
...
SQL> SELECT sys_context('userenv','authentication_method') FROM dual;
SYS_CONTEXT('USERENV','AUTHENTICATION_METHOD')
--------------------------------------------------------------------------------
KERBEROS
```


trivadis makes IT easier.

Mac OS

- Does work even on MacOS

```
kinit -c /tmp/soe soe@POSTGASSE.ORG
Password for soe@POSTGASSE.ORG:
soe@gaia:~/local/dev/tvdsecdb/local/bin/ [ic12102] sqlplus /@TDB122A
...
SQL> SELECT sys_context('userenv','authentication_method') FROM dual;
SYS_CONTEXT('USERENV','AUTHENTICATION_METHOD')
--------------------------------------------------------------------------------
KERBEROS
```


trivadis makes IT easier.

Advanced Use Cases

trivadis
makes IT easier.

Advanced Use Cases

- Client Typ jdbc thin, jdbc thick, OCI?
  - All of them do work just depends on key type, OS, ccache etc
- Enterprise User Security
  - Well does work independently of Kerberos
- DB Links
  - Do not work or just limited possibilities
  - Require forward able ccache e.g. `okinit -f`
  - User CURRENT_USER database Links

trivadis makes IT easier.

Oracle Net Services and Kerberos Troubleshooting

trivadis
makes IT easier.

Kerberos Troubleshooting (1)

- Kerberos Troubleshooting ~~can be~~ **is** quite cumbersome
  - Only via SQLNet Trace
- Dedicated trace file for `okinit` possible

```
TRACE_LEVEL_OKINIT     = SUPPORT
TRACE_UNIQUE_OKINIT    = on
TRACE_DIRECTORY_OKINIT = /u00/app/oracle/network/log
```

- SQLNet Trace on Client
- SQLNet Trace on Server
- Use Network Tracing like WireShark

trivadis makes IT easier.

Kerberos Troubleshooting (2)

- Java Trace on Command line

```
java -Dsun.security.krb5.debug=true -Dsun.security.spnego.debug=true
-Djavax.net.debug=all LoginTestKerberos
>>>DEBUG <CCacheInputStream>  client principal is soe@POSTGASSE.ORG
>>>DEBUG <CCacheInputStream> server principal is krbtgt/POSTGASSE.ORG@POSTGASSE.ORG
>>>DEBUG <CCacheInputStream> key type: 17
>>>DEBUG <CCacheInputStream> auth time: Fri Sep 15 11:01:27 CEST 2017
>>>DEBUG <CCacheInputStream> start time: Fri Sep 15 11:01:27 CEST 2017
>>>DEBUG <CCacheInputStream> end time: Fri Sep 15 21:01:27 CEST 2017
>>>DEBUG <CCacheInputStream> renew_till time: Sat Sep 16 11:01:27 CEST 2017
>>> CCacheInputStream: readFlags()  RENEWABLE; INITIAL;
>>>DEBUG <CCacheInputStream>  client principal is soe@POSTGASSE.ORG
Java config name: /etc/krb5.conf
Loaded from Java config
...
```


trivadis makes IT easier.

Kerberos Trace Files

- Oracle 12c R2 has a reworked Kerberos stack (again… 🤔)
  - Supports the environment variable KRB5_TRACE
    ➡ finally some kind of a Kerberos Trace file

```
[654] 1505467906.511077: Getting credentials hmu@POSTGASSE.ORG ->
oracle/urania.postgasse.org@POSTGASSE.ORG using ccache FILE:/u00/app/oracle/network/admin/krbcache
[654] 1505467906.511223: Retrieving hmu@POSTGASSE.ORG -> oracle/urania.postgasse.org@POSTGASSE.ORG
from FILE:/u00/app/oracle/network/admin/krbcache with result: 0/Success
[654] 1505467906.511553: Creating authenticator for hmu@POSTGASSE.ORG ->
oracle/urania.postgasse.org@POSTGASSE.ORG, seqnum 0, subkey (null), session key aes256-cts/B93C
[654] 1505467906.514169: Getting credentials hmu@POSTGASSE.ORG ->
oracle/urania.postgasse.org@POSTGASSE.ORG using ccache FILE:/u00/app/oracle/network/admin/krbcache
...
[654] 1505467906.517510: Response was not from master KDC
[654] 1505467906.517546: Decoding FAST response
[654] 1505467906.517688: FAST reply key: aes256-cts/21CF
[654] 1505467906.517725: TGS reply is for hmu@POSTGASSE.ORG -> krbtgt/POSTGASSE.ORG@POSTGASSE.ORG with
session key aes256-cts/2E01
[654] 1505467906.517740: Got cred; 0/Success
```


trivadis makes IT easier.

Kerberos Troubleshooting Steps

- Check DNS lookup and revers lookup.
- Check System time. Do all system have the same time? Or within **clockskew**
- Is the account locked?
- Is an okinit possible?
- Is Kerberos Authentication used at all?
- Start to Trace if possible with Oracle 12c sqlplus and KRB5_TRACE
- Start SQLNet Tracing
- Use alternative SQLNet or Listener configuration
  - static listener with ENV defining alternative TNSADMIN directory
  - if possible have different configuration for different use ase

trivadis makes IT easier.

Usual issues

- Time shift
- DNS does not work
- Configuration file Issues (tabs, wrong parameter, case of username, ticket size etc)
- Wrong service name
- Wrong **kvno**, version of the keytab
- Wrong or not Supported Krypto Type
  - Old Krypto's like DES are blocked, new like AES 256 require JCE
- Kerberos Bugs Oracle or Microsoft
- bad hair day…

trivadis makes IT easier.

MOS Notes and other links

- Master Note For Kerberos Authentication
  https://support.oracle.com/epmos/faces/DocumentDisplay?id=1375853.1
- How To Configure Kerberos Authentication In A 12c Database
  https://support.oracle.com/epmos/faces/DocumentDisplay?id=1996329.1
- Configuring ASO Kerberos Authentication with a MS Windows 2008 R2 AD KDC
  https://support.oracle.com/epmos/faces/DocumentDisplay?id=1304004.1
- ORA-12518 / TNS-12518 Troubleshooting
  https://support.oracle.com/epmos/faces/DocumentDisplay?id=556428.1
- How To Enable Radius and Kerberos Adapters In Oracle Database 11g Standard Edition https://support.oracle.com/epmos/faces/DocumentDisplay?id=2145731.1
- Java Kerberos Troubleshooting
  http://docs.oracle.com/javase/7/docs/technotes/guides/security/jgss/tutorials/Troubleshooting.html

trivadis makes IT easier.

Round Up

trivadis
makes IT easier.

Round Up

- Oracle has done the homework and fixed a couple of bugs
  - but there is still some room for improvements
- The fault is not only with Oracle
  - although Kerberos is standardized it does not mean that every implementation is similar and without bugs, Kerberos MIT, Microsoft, OS etc does the rest
- Simple architectures can be implemented quickly, but …
  - … complex KDC or Active Directory
  - … version diversity
  - ... application and client types
  - … are challenging

Quote: Kerberos is hell, but as soon as it works, it's nice and comfortable...

…and now a bit cosier

trivadis makes IT easier.

Round Up

We are happy to support you:

- With Security Reviews and Risk Assessments
- In the creation of security concepts and their implementation
- Provide comprehensive advice in data security

trivadis
makes IT easier.

Session Feedback – now

- Please use the Trivadis Events mobile app to give feedback on each session
- Use "My schedule" if you have registered for a session
- Otherwise use "Agenda" and the search function

- If the mobile app does not work (or if you have a Windows smartphone), use your smartphone browser
  - URL: http://trivadis.quickmobileplatform.eu/
  - User name: <your_loginname> (such as “svv”)
  - Password: sent by e-mail...

trivadis
makes IT easier.

Stefan Oehrli
Solution Manager / Trivadis Partner

Tel.: +41 58 459 55 55
stefan.oehrli@trivadis.com

http://www.trivadis.com/security
http://www.oradba.ch
@stefanoehrli

trivadis
makes IT easier.