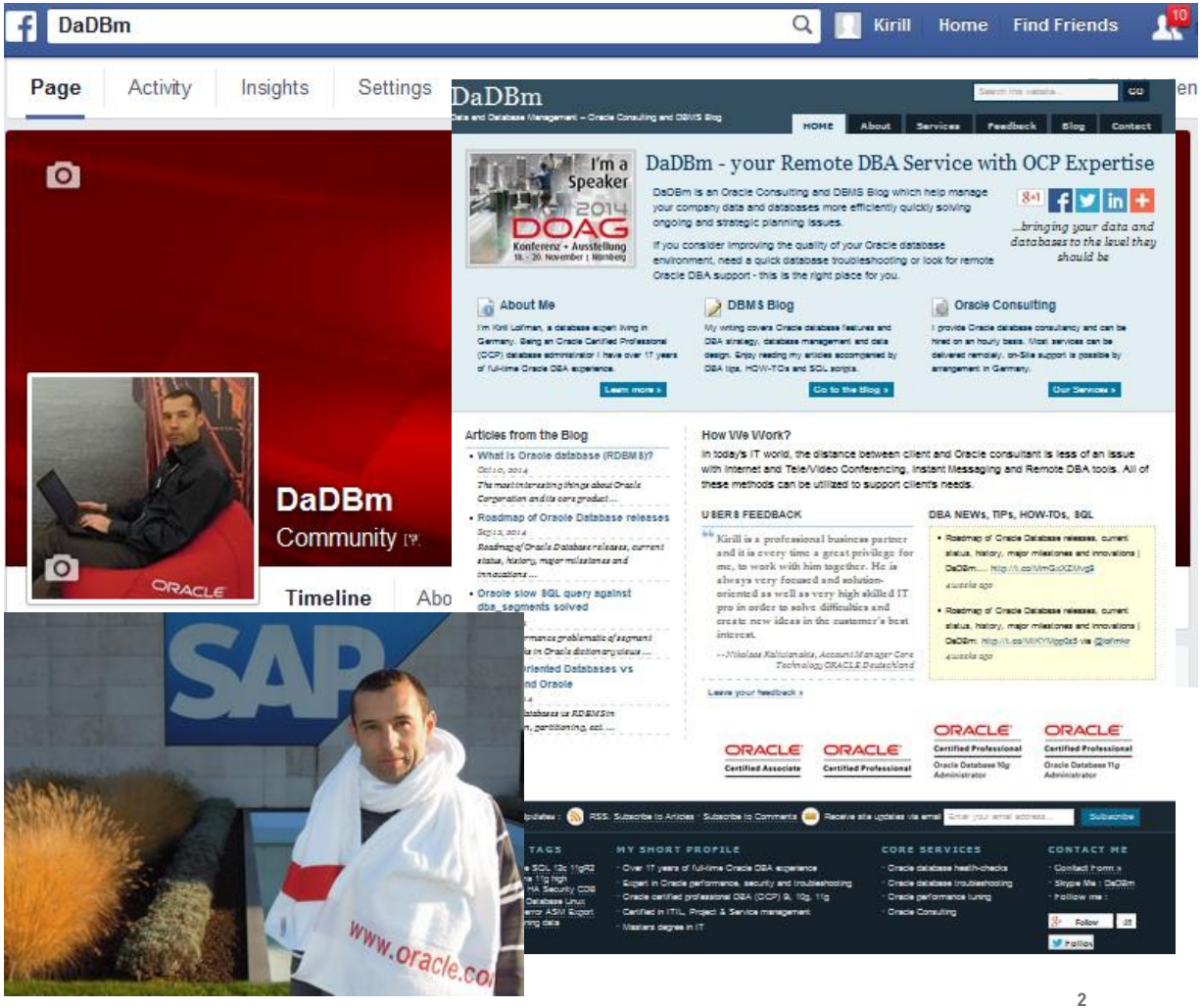
LIVE ADVENTURE - FROM MY PC TO ORACLE REMOTE DATABASE

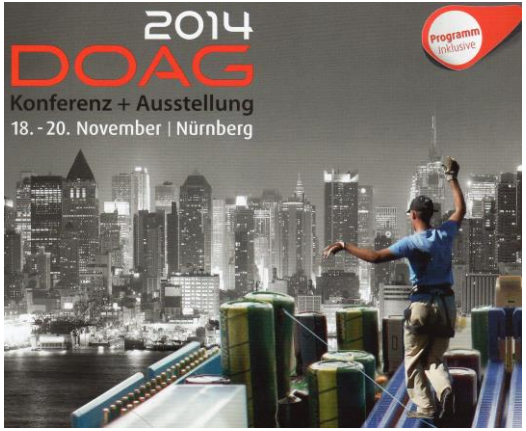
Kirill Loifman
dadbm.com
Germany

WHO IS KIRILL LOIFMAN

- Working with Oracle since 1996
- Full-time DBA expirience on Unix AIX, OpenVMS, Tru64, HP-UX, Linux
- Database architect at adidas
- OCP DBA 9i,10g,11g,..
- Blogger, speaker & a father
- Contacts
  www: dadbm.com
  Twitter: @loifmkir
  Google.com/+Dadbm
  Facebook, LinkedIn, Xing ...



DOAG ABOUT ME IN CONFERENCE BROCHURE



Die Datenbank hacken

Kirill Loifman, geboren im russischen Kaliningrad, lebt seit dreizehn Jahren in Deutschland. Er ist Oracle-Certified Database Consultant (OCP DBA) und besitzt mehr als siebzehn Jahre Erfahrung als Oracle-Datenbank-Administrator. Sein Blog (www.dadbm.com) sowie seine Kommentare auf Twitter (@loifmkir), Google plus und Facebook sind in der Community weithin bekannt. Der Vortrag „live adventure – from my PC to Oracle Remote Database" hat zum Ziel, sich live ohne Passwort in einen Datenbank-Server einzuhacken, um zu demonstrieren, wie man seine Daten vor unerlaubten Zugriffen schützen kann. Drei Fragen an Kirill Loifman:

Wie wichtig ist Ihnen die Sicherheit Ihrer Daten?
Daten sind das Wertvollste, was Unternehmen besitzen. Deshalb sollte die Datensicherheit auch die größte Beachtung erhalten, noch vor deren Verfügbarkeit.

Was bedeutet Ihnen Ihre Arbeit?
Mich fasziniert die IT-Technologie im Allgemeinen sowie die Oracle-Technologie im Besonderen. Nichts bleibt bestehen, alles ändert sich schnell und dynamisch. Als Lernbegeisterter konnte ich mich deshalb über mehr als siebzehn Jahre weiterentwickeln und bin somit in der Lage, neue Datenbank-Lösungen zu entwickeln, Datenbank-Probleme zu beheben und die Performance von Anwendungen zu steigern.

Werden Sie es im Rahmen Ihres Vortrags schaffen, ohne Passwort die Verbindung zu einem Server herzustellen?
Ich gebe zu, die Beschreibung meines Vortrags ist etwas provozierend. Um sich mit einer Oracle-Datenbank zu verbinden, ist ein Authentifizerungsmechanismus erforderlich, und ich werde einige davon beschreiben. Es gibt jedoch undokumentierte Tricks, mit denen ein erfahrener Oracle-Anwender ein ineffizientes Sicherheitssystem umgehen kann. Ich werde auch einige Techniken vorstellen, die den alltäglichen Datenbank-Zugang für Administratoren und Entwickler vereinfachen – ohne die Sicherheit außer Acht zu lassen.

OUR JOURNEY SCENARIO

End-User / Windows Client

Firewall

Oracle database 11gR2 on Linux

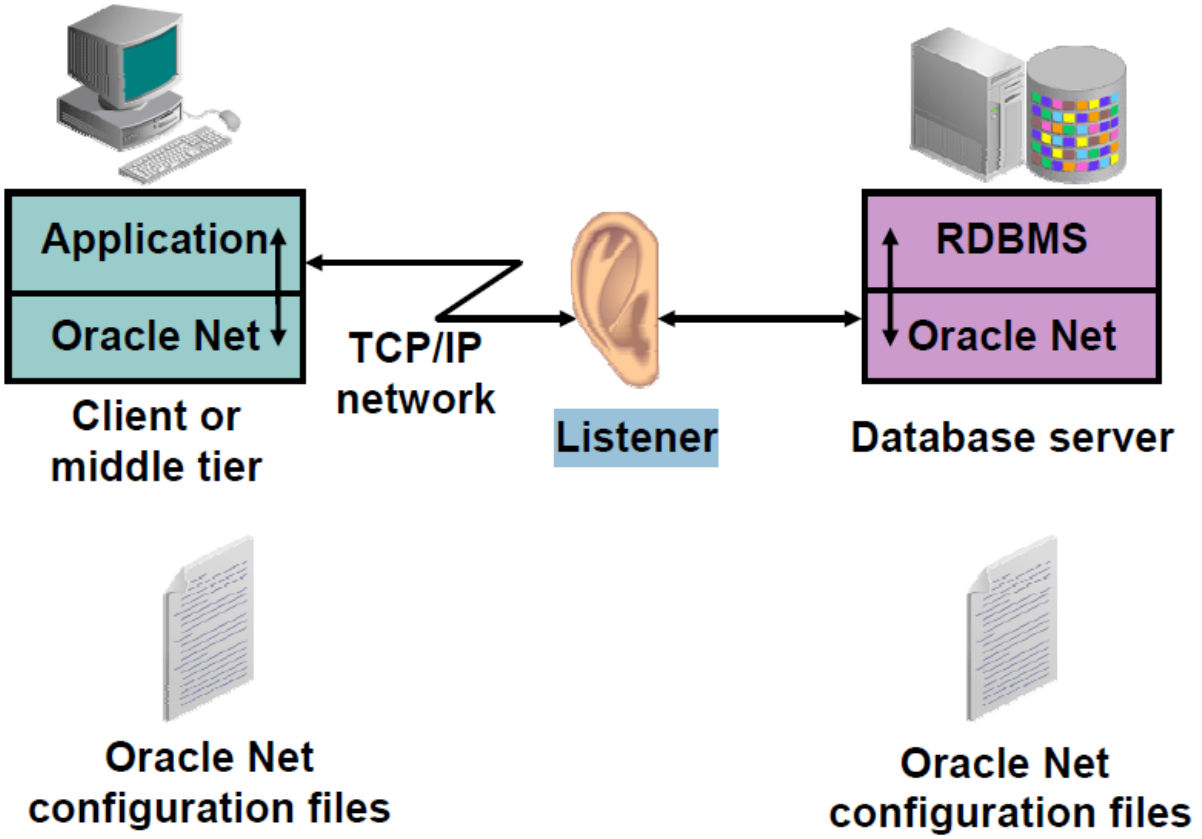
Host name: dadbm-host
Host name virtual: dadbm-vip
DB name: orcl
Port: 1521

Our GOALs:

- Establish remote connection from Client PC to Remote Oracle database via Firewall
- Connect to any database user without password
- Simplify further database connection attempts
- Explore a few security points along the way

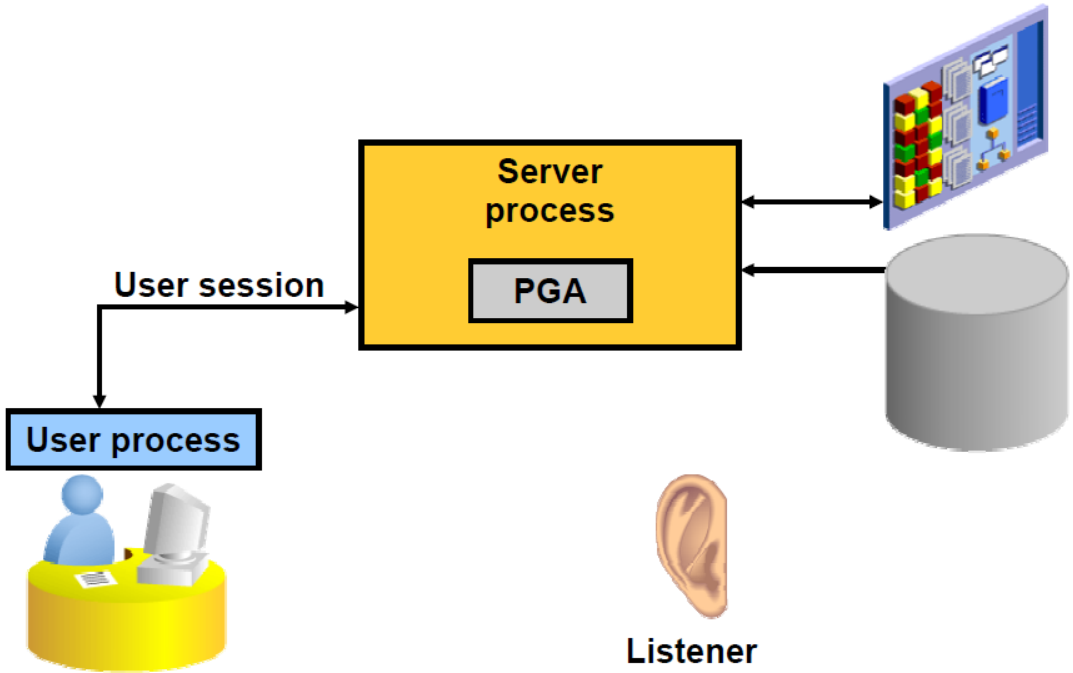
WHAT WE NEED TO ACHIEVE OUR GOAL

- Oracle database
- Network interface
- Firewall ports to be opened
- Oracle listener
- Oracle Client installable
- Oracle client utilitty
- Oracle database user
- Oracle user password
- tnsnames.ora
- ...



CONFIGURE DATABASE SIDE

- Install Oracle binaries
- Startup Oracle database
- Configure Oracle listener,
  or
  maybe NOT configure…
- Static vs Dynamic listener registration



- Tool Set (Linux): OUI (runInstaller), dbca, SQL*Plus (sqlplus), lsnrctl, netmgr, …

CONFIGURE CLIENT SIDE

- Which Oracle client to use
  - Oracle OCI Client / Instant Client vs JDBC thing client
- Client tool set (Windows)
  - ping tnsping telnet Putty OUI SQL*Plus, regedit
- Install Oracle Client properly (OUI)
  - http://www.dadbm.com/how-to-install-oracle-11gr2-64-bit-client-on-windows-7/
  - http://www.dadbm.com/oracle-11gr2-client-installation-on-windows-7-troubleshooting/
- Identify and configure your Oracle Client environment => ...

CONFIGURE CLIENT SIDE - CONTINUE

- Identify / configure your Oracle environment
  - ORACLE_HOME
    - OUI; SQL*Plus; “set” if set as OS environment variable
    - `C:\oracle\product\11.2.0\client_1`
  - TNS_ADMIN (optional)
    - “set” if set as OS environment variable
    - `C:\oracle\product\11.2.0\client_1\network\admin`
  - NLS_LANG
    - regedit (might not be accessable) -> SQL*Plus
- Create a connection string in %TNS_ADMIN%\tnsnames.ora
  - `orcl=(description=(address=(protocol=tcp)(host=dadbm-vip)(port=1521))(connect_data=(service_name=orcl))))`

DATABASE POTENTIAL CONNECTION WAYS

```
sqlplus user/pass@orcl                                  # tnsnames.ora

sqlplus user/pass@'(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=dadbm-
vip)(1521=1521))(CONNECT_DATA=(SERVICE_NAME=orcl)))'

sqlplus user@'(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=dadbm-
vip)(HOST=1521))(CONNECT_DATA=(SID=orcl)))'

sqlplus user/pass@//dadbm-vip:1521/orcl                 # EZCONNECT (sqlnet.ora)
sqlplus user@'//dadbm-vip:1521/orcl'                    # without password
sqlplus user@'//dadbm-vip/orcl'                         # default port

jdbc:oracle:thin:@dadbm-vip:1521/orcl                   # custom JDBC url
jdbc:oracle:thin:user@dadbm-vip:1521:orcl
jdbc:oracle:oci:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=dadbm-
vip)(1521=1521))(CONNECT_DATA=(SERVICE_NAME=orcl)))
```

FIREWALL ISSUE

- 1st Problem – tnsping does NOT respond
  - `ping <dadbm-host-ip>` -> ping works!
  - `tnsping orcl` -> timed out
  - `telnet <dadbm-vip> 1521` -> Connect failed

=> Potential issue with Firewall => Need a solution!

- Proper solution -> Ask Security to open a DB listener port in Firewall

Source IP	Source Zone	Destination IP	Destination Zone	Destination Port
<Client PC IP>	LAN/WAN	<dadbm-vip>	DMZ	1521

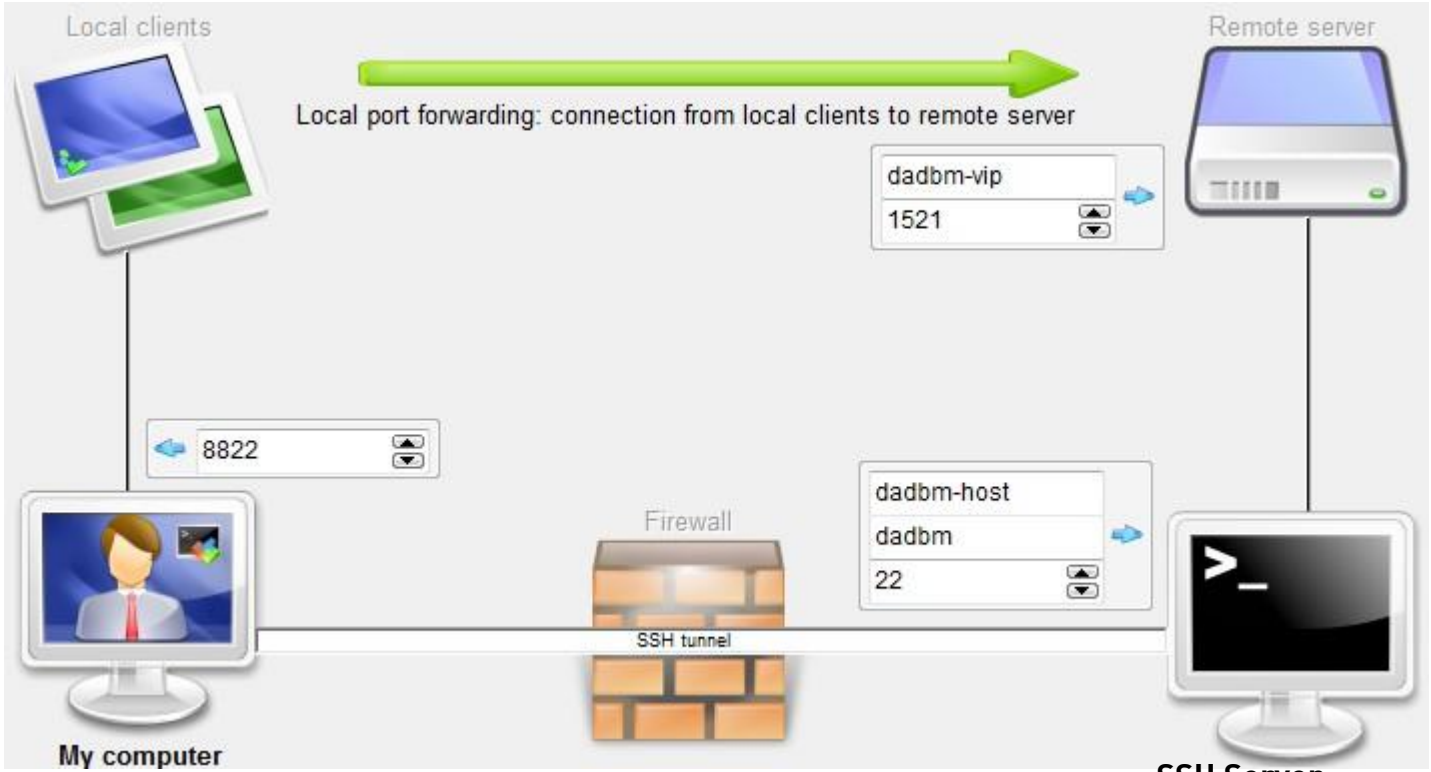
- *Adventure solution* -> Firewall Tunneling

FIREWALL TUNNELING

- *Adventure solution* steps
  - SSH port 22 is usually open in Firewalls by default
  - Request a Linux user on database host
  - Use Putty Firewall Tunneling feature
    - Menu *Connection -> SSH -> Tunnels*
    - Add a Tunnel with *Source port* „8822“ to *Destination* „dadbm-vip:1521“
  - Adjust DB connection string on the client as following:

```
orcl=(description=(address=(protocol=tcp)(host=127.0.0.1)
(port=8822))(connect_data=(service_name=orcl)))
```

FIREWALL TUNNELING – CONTINUE



Local clients can access the remote DB server by connecting to <mycomputer>:8822

DATABASE CONNECTION TEST – STEP1

1) Ping your host and database listener

```
ping dadbm-host

telnet 127.0.0.1 8822

tnsping
(description=(address=(protocol=tcp)(host=127.0.0.1)(port=8822))
(connect_data=(service_name=orcl)))

tnsping orcl

tnsping 127.0.0.1:8822/orcl
```

DEMO 2…

DATABASE USER REQUIRED

- Solutions against missing database user ☺

  - Proper solution -> Ask DBAs to create a user

  - *Adventure solutions* -> See Demo

DATABASE CONNECTION TEST – STEP2

2) Establish a database connection

```
sqlplus dadbm@orcl as sysdba
sqlplus dadbm@orcl

sqlplus
dadbm@'(description=(address=(protocol=tcp)(host
=8822))(connect_data=(service_name=orcl)))'

sqlplus dadbm@'//127.0.0.1:8822/orcl'

jdbc:oracle:thin:@127.0.0.1:8822/orcl
jdbc:oracle:oci:@127.0.0.1:8822/orcl
```

DEMO 3...

DATABASE CONNECTION TROUBLESHOOTING

- Following connection errors may arise

```
ORA-12154: TNS:could not resolve the connect identifier specified
ORA-12198: TNS:could not find path to destination
ORA-12203: TNS:unable to connect to destination
ORA-12533: TNS:illegal ADDRESS parameters
TNS-12541: TNS:no listener
```

…

- Use a following post on dadbm.com to troubleshoot

  http://www.dadbm.com/how-to-troubleshoot-oracle-remote-database-connection/

AVOID DB PASSWORD USING SECURE PASSWORD STORE

1) Configure Oracle Client environment for Oracle Wallet

- **tnsnames.ora file**

```
orcl =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.1)(PORT = 8822))
    (CONNECT_DATA = (SERVICE_NAME = orcl))
  )
```

- **sqlnet.ora file**

```
WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA = (DIRECTORY = C:\oracle\product\11.2.0\client_1\network\admin))
)
SQLNET.WALLET_OVERRIDE = TRUE
```

SECURE PASSWORD STORE - CONTINUE

2) Create a wallet on the client

```
mkstore -wrl <wallet_location> -create

mkstore -wrl %TNS_ADMIN% -create
Enter password:  <= Choose wallet password and remember it
Enter password again:

Directory of C:\oracle\product\11.2.0\client_1\network\admin

12-Jun-14  12:39      3,589 cwallet.sso      # Auto login wallet file
12-Jun-14  12:39      3,512 ewallet.p12      # PKCS#12 wallet file
12-Jun-14  12:26        644 sqlnet.ora
04-Jun-14  22:49     15,237 tnsnames.ora
```

SECURE PASSWORD STORE - CONTINUE

3) Create database connection credentials in the wallet

```
mkstore -wrl %TNS_ADMIN% -createCredential <alias> <user> <passwd>
mkstore -wrl %TNS_ADMIN% -createCredential orcl    dadbm  ora4u
Enter password:  <= Wallet password
```

4) Managing External Password Store Credentials

```
mkstore -wrl %TNS_ADMIN% -listCredential
mkstore -wrl %TNS_ADMIN% -createCredential orcl1 dadbm9 pass
mkstore -wrl %TNS_ADMIN% -modifyCredential orcl1 dadbm9 newpassword
mkstore -wrl %TNS_ADMIN% -deleteCredential orcl1
```

SECURE PASSWORD STORE - CONTINUE

5) Connect to a database without a password

```
sqlplus /@orcl
```

6) Notes

- DB does not know about your secure password store and vice versa
- <DB alias> is unique in Wallet -> for different user create another alias
- Wallet can be generated somewhere else and copied to you client
- Extended Wallet management with orapki utility
- More details in MOS DOC ID 340559.1

DEMO 4...

CONNECT TO ANOTHER USER WITHOUT A PASSWORD

- *Adventure solution* => Enable Proxy Authentication

1) Use `dadbm` as proxy user and create more proxy clients:

```
grant connect,resource to dadbm1 identified by adJIk3909sdfj;
grant connect,resource to dadbm2 identified by g7fk3kZfdhl05;
alter user dadbm1 grant connect through dadbm;
```

2) Connect to a database with proxy user and secure password store

```
sqlplus proxy_user[proxy_client]@orcl
sqlplus [dadbm1]@orcl                    sqlplus /@orcl
                              or         SQL>conn [dadbm1]@orcl

alter session set current_schema=dadbm2;
```

ENABLE PROXY AUTHENTICATION - CONTINUE

3) Check who you are

```
select sys_context('USERENV','PROXY_USER') PROXY_USER,
sys_context('USERENV','SESSION_USER') SESSION_USER,
sys_context('USERENV','CURRENT_SCHEMA') CURRENT_SCHEMA
from dual;
```

```
PROXY_USER           SESSION_USER         CURRENT_SCHEMA
-------------------- -------------------- --------------------
DADBM                DADBM1               DADBM2
```

4) More information

```
select * from dba_proxies;
select * from proxy_roles;
```

SIMPLIFY CONNECTION TO DATABASE

- Create 2 files sql.bat and proxy.sql on the client

```
# sql.bat
SET LOCAL=%1
sqlplus /@%LOCAL% %2
```

```
# proxy.sql
set verify off
alter user &&1 grant connect through dadbm;
connect [&&1]@&_CONNECT_IDENTIFIER
show user
```

- Ask for extra grant to my user dadbm: `grant alter user to dadbm;`

- Connect to any TNS alias using sql.bat and to any DB user with proxy.sql

```
sql orcl
DADBM@orcl+>@proxy dadbm1
USER is "DADBM1"
DADBM1@orcl+>
```

DEMO 5...

SIMPLIFY CONNECTION TO LINUX BOX

- Do we need a user password to connect to a Linux box?

- Setup Public-key (SSH RSA) authentication
- Use Putty tool set
  - puttygen.exe -> Generate SSH2-RSA keys
  - pscp.exe -> transfer Public key to Linux server
  - putty.exe -> Authenticate with Private key file
  - putty_auth_agent.bat -> enter keypass just once

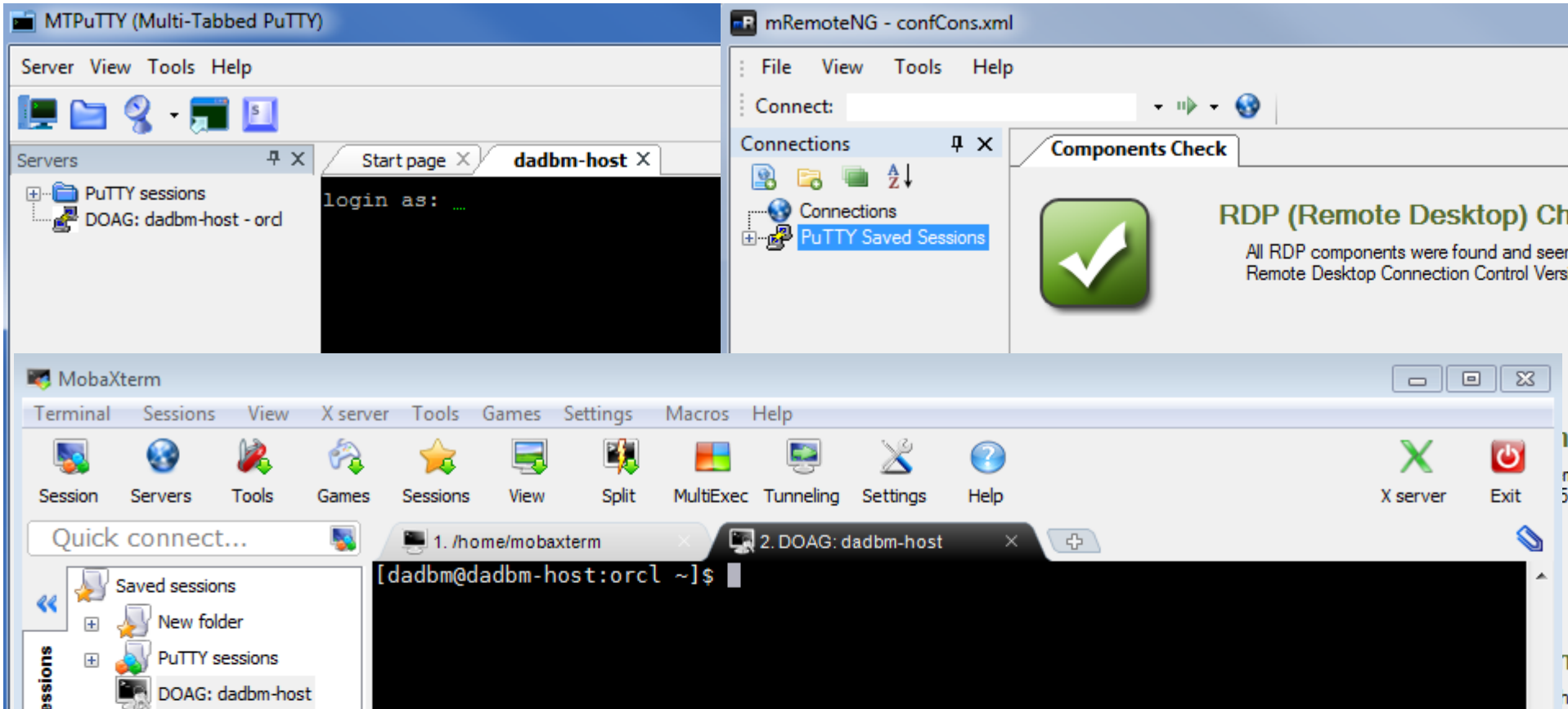
  -> Establish Linux connection withOUT password

DEMO 6...

LIVE ADVENTURE EXERCISE SUMMARY

- Setting up the database and server connections this way will simplify the day-to-day tasks of DBAs and developers.
- But think about security! That was just a playground!
- Firewall tunneling and Secure Password Store are supported by other tools
- Get your servers listed using other fancy GUIs
  - MTPutty
  - MRemoteNG
  - MobaXTerm
  - …

EXTEND YOUR TOOL SET

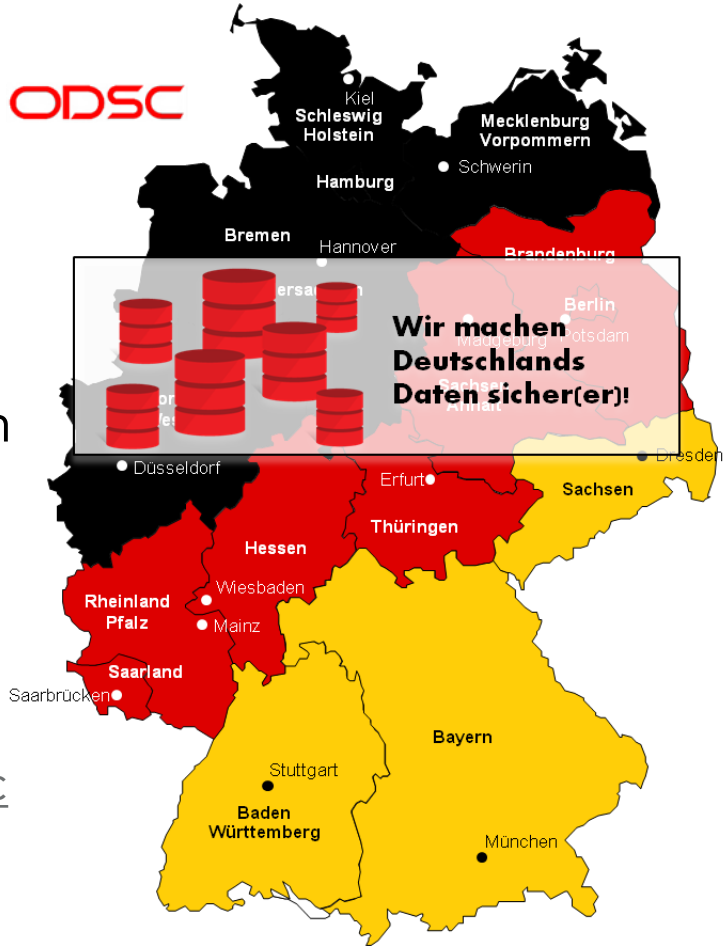


ORACLE

Database Security Community

Wir machen Deutschlands Daten sicher(er)!

Eine Community für DBAs, die aktiv die Daten Ihrer Datenbanksysteme schützen wollen oder müssen.
Wir erarbeiten sinnvolle Konzepte und tauschen unser Wissen aus.



https://blogs.oracle.com/SecurityDE/entry/db_security_community_wurde_gegr%C3%BCndet

Email to join: carsten.muetzlitz@oracle.com

???

THANK YOU!

Kirill Loifman

www.dadbm.com