ORDIX AG

Eintritt nur mit Ticket – Kerberos für Oracle Datenbanken einrichten

Andreas Jordan

DOAG Konferenz + Ausstellung
22.11.2023, Nürnberg

Andreas Jordan

ORDIX AG

- Principal Consultant und Teamleiter

- Microsoft SQL Server
- Oracle Database
- PowerShell

- Sprecher auf den IT-Tagen 2015, 2022, 2023
- Sprecher auf der DOAG Konferenz & Ausstellung 2022, 2023

- https://blog.ordix.de/andreas-jordan

Wie komme ich zu diesem Thema?

ORDIX AG

- Die Anmeldung ohne Kennwort an einem Microsoft SQL Server ist ganz normal.
  Geht das nicht auch bei Oracle?

- AD-Integration ist bei Oracle durchaus ein großes Thema mit vielen Produkten und Technologien.
  Die Oracle Kollegen haben mich nach meinem AD-Knowhow gefragt.

- Ich habe sehr viel recherchiert und dabei viele Artikel und Videos gefunden.
  Alle haben einen unterschiedlichen Fokus, betrachten unterschiedliche Situationen und Ziele.

- Ich möchte mit diesem Vortrag einen weiteren Baustein beisteuern, um anderen zu helfen.

Agenda

ORDIX AG

- Authentifizierung
- Service Principal Name (SPN)
- Einrichtung von Kerberos …
  - … auf dem Domain Controller
  - … auf den Oracle Servern und Clients
  - … Datenbankbenutzern
- Einrichtung von CMU …
  - … auf dem Domain Controller (Achtung: Nur Teilkomponenten von CMU)
  - … auf den Oracle Servern
  - … Datenbankbenutzern

Authentifizierung

ORDIX AG

- Klassische Authentifizierung:
  - Client sendet Benutzername und Kennwort an den Oracle Server.
  - Oracle Server prüft Benutzername und Kennwort anhand eigener Daten.

- Authentifizierung mit Kerberos:
  - Bei der Anmeldung an Windows wird automatisch ein Ticket Granting Ticket erstellt.
  - Bei Linux wird dazu der Befehl kinit verwendet.
  - Vor dem Verbindungsaufbau mit dem Oracle Server wird damit ein Service Ticket erstellt.
  - Client sendet das Service Ticket an den Oracle Server.
  - Oracle Server prüft das Service Ticket indem es dieses entschlüsselt.

Ticket vom Active Directory statt Kennwort der Datenbank

Service Principal Name (SPN)

ORDIX AG

- Microsoft SQL Server
  - Der Service Principal Name hängt am Computer-Konto.
  - Der SQL Server kann den SPN selbst bei jedem Start registrieren.

- Oracle Database
  - Kein Computer-Konto vorhanden, da der Server nicht Mitglied einer Domäne ist.
  - Daher wird ein Benutzer-Konto angelegt und der Service Principal Name dort hinzugefügt.
  - Der Oracle Server kann den Schlüssel nicht selbst vom Active Directory beziehen.
  - Daher muss eine Schlüsseltabellen-Datei erzeugt und zum Oracle Server übertragen werden.

Einrichtung von Kerberos auf dem Domain Controller
Benutzer anlegen

ORDIX AG

- Vorschlag für den Benutzernamen: <servername>spn (db01spn)
  - Nicht nur den Namen des Servers verwenden, das gibt Probleme.

- Notwendiger Parameter: KerberosEncryptionType = 'AES256'

```
$serviceUserParams = @{
    Name                  = 'db01spn'
    DisplayName           = 'User for Service Principal Name for Kerberos'
    Path                  = 'CN=Managed Service Accounts,DC=ordix,DC=local'
    PasswordNeverExpires  = $true
    Enabled               = $true
    AccountPassword       = $password
    KerberosEncryptionType = 'AES256'
}
New-ADUser @serviceUserParams
```

Einrichtung von Kerberos auf dem Domain Controller
Schlüsseltabellen-Datei erzeugen

ORDIX AG

- Das dazu genutzte Programm ktpass.exe ist auf dem Domain Controller vorhanden.
  - https://learn.microsoft.com/de-de/windows-server/administration/windows-commands/ktpass

- Der Service Principal Name wird dem Benutzer automatisch hinzugefügt.

```
$server = 'db01'
$domain = 'ordix.local'
$realm  = 'ORDIX.LOCAL'

$spn  = 'oracle/{0}.{1}@{2}' -f $server, $domain, $realm
$user = '{0}spn@{1}'         -f $server, $domain
$file = 'oracle.{0}.keytab'  -f $server

$spn  = 'oracle/db01.ordix.local@ORDIX.LOCAL'
$user = 'db01spn@ordix.local'
$file = 'oracle.db01.keytab'

ktpass.exe -princ $spn -mapuser $user -out $file -crypto all -ptype KRB5_NT_PRINCIPAL +rndPass
```

Einrichtung von Kerberos auf den Oracle Servern und Clients
krb5.conf

ORDIX AG

- Die Datei krb5.conf ist in network-admin anzulegen.

- Auf allen Oracle Servern und Clients mit diesem Inhalt:

```
[libdefaults]
default_realm = <realm>
[realms]
<realm> = {
    kdc = <domain>:88
}
[domain_realm]
<domain> = <realm>
.<domain> = <realm>
```

Einrichtung von Kerberos auf den Oracle Servern und Clients
sqlnet.ora (I)

ORDIX AG

- Die Datei sqlnet.ora ist in network-admin anzulegen oder zu erweitern.

- Auf allen Oracle Servern und Clients mit diesem Inhalt:

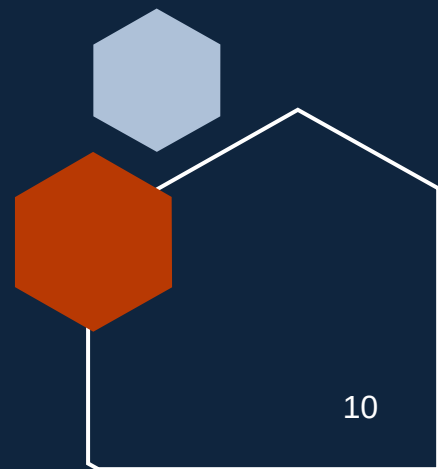
```
NAMES.DIRECTORY_PATH=(TNSNAMES, EZCONNECT)
SQLNET.FALLBACK_AUTHENTICATION=TRUE
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE=oracle
SQLNET.KERBEROS5_CONF_MIT=TRUE
SQLNET.KERBEROS5_CONF=<Pfad zur Datei krb5.conf>
```

- Auf den Oracle Servern zusätzlich:

```
SQLNET.KERBEROS5_KEYTAB=<Pfad zur keytab-Datei>
```

- Auf den Oracle Clients unter Windows zusätzlich:

```
SQLNET.KERBEROS5_CC_NAME=OSMSFT://
```



Einrichtung von Kerberos auf den Oracle Servern und Clients
sqlnet.ora (II)

ORDIX AG

- Die Datei sqlnet.ora muss zusätzlich enthalten:

- Auf den Oracle Servern unter Windows:

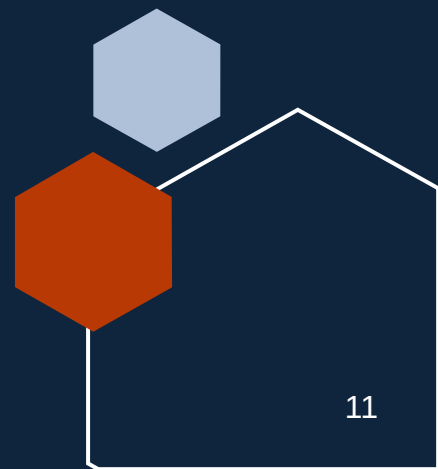
```
SQLNET.AUTHENTICATION_SERVICES=(NTS,KERBEROS5PRE,KERBEROS5)
```

- Auf den Oracle Servern unter Linux:

```
SQLNET.AUTHENTICATION_SERVICES=(ALL)
```

- Auf den Oracle Clients:

```
SQLNET.AUTHENTICATION_SERVICES=(KERBEROS5PRE,KERBEROS5)
```

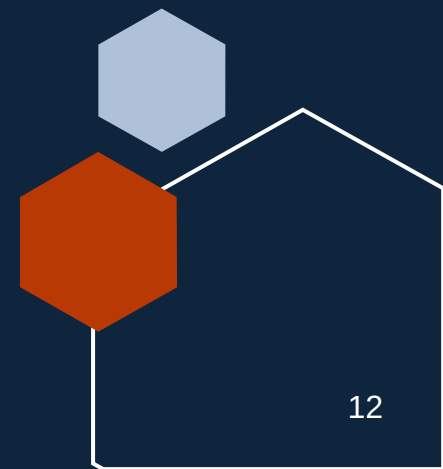


Einrichtung von Datenbankbenutzern für Kerberos

ORDIX AG

```
CREATE USER TestUser IDENTIFIED EXTERNALLY AS 'TestUser@<realm>';
GRANT CREATE SESSION TO TestUser;
```

Testen wir das doch mal in meinem Labor…

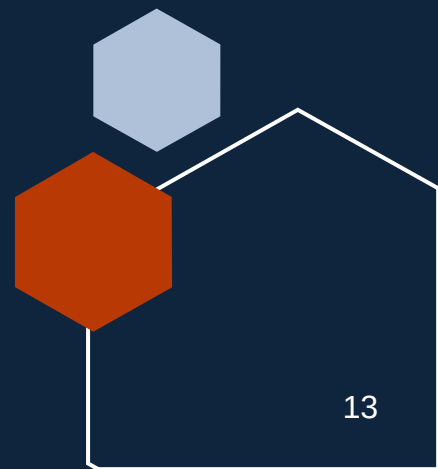


Falls das Labor nicht funktioniert…

ORDIX AG

```
$credential = Get-Credential -Message 'Test User'
$userParams = @{
    Name              = $credential.UserName
    AccountPassword = $credential.Password
    Path              = 'OU=OracleUser,DC=ordix,DC=local'
    Enabled           = $true
}
New-ADUser @userParams
```

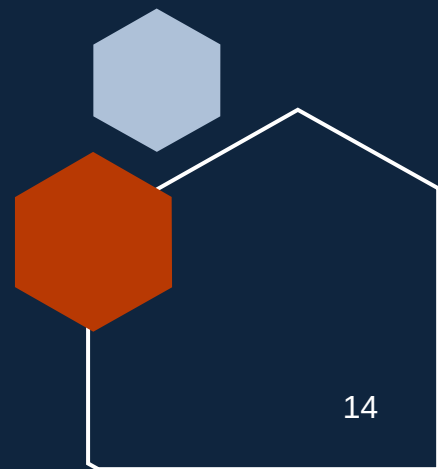
```
CREATE USER andreas IDENTIFIED EXTERNALLY AS 'Andreas@ORDIX.LOCAL';
GRANT CREATE SESSION TO andreas;
```



Falls das Labor nicht funktioniert…

ORDIX AG

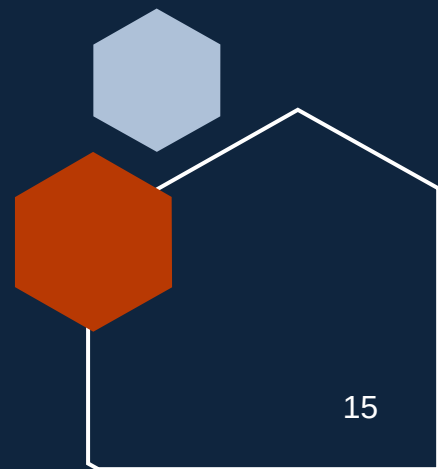
```
PS C:\> whoami
ordix\andreas
PS C:\> klist

Current LogonId is 0:0x6f3e55

Cached Tickets: (1)

#0>     Client: Andreas @ ORDIX.LOCAL
        Server: krbtgt/ORDIX.LOCAL @ ORDIX.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 11/8/2023 19:01:55 (local)
        End Time:   11/9/2023 5:01:55 (local)
        Renew Time: 11/15/2023 19:01:55 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: DC
```



Falls das Labor nicht funktioniert…

ORDIX AG

```
PS C:\> sqlplus /@PDB02

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Nov 8 19:03:01 2023
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.

Last Successful login time: Wed Nov 08 2023 18:54:49 +01:00

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> select user from dual;

USER
------------------------------------------------------------------------------
ANDREAS

SQL>
```



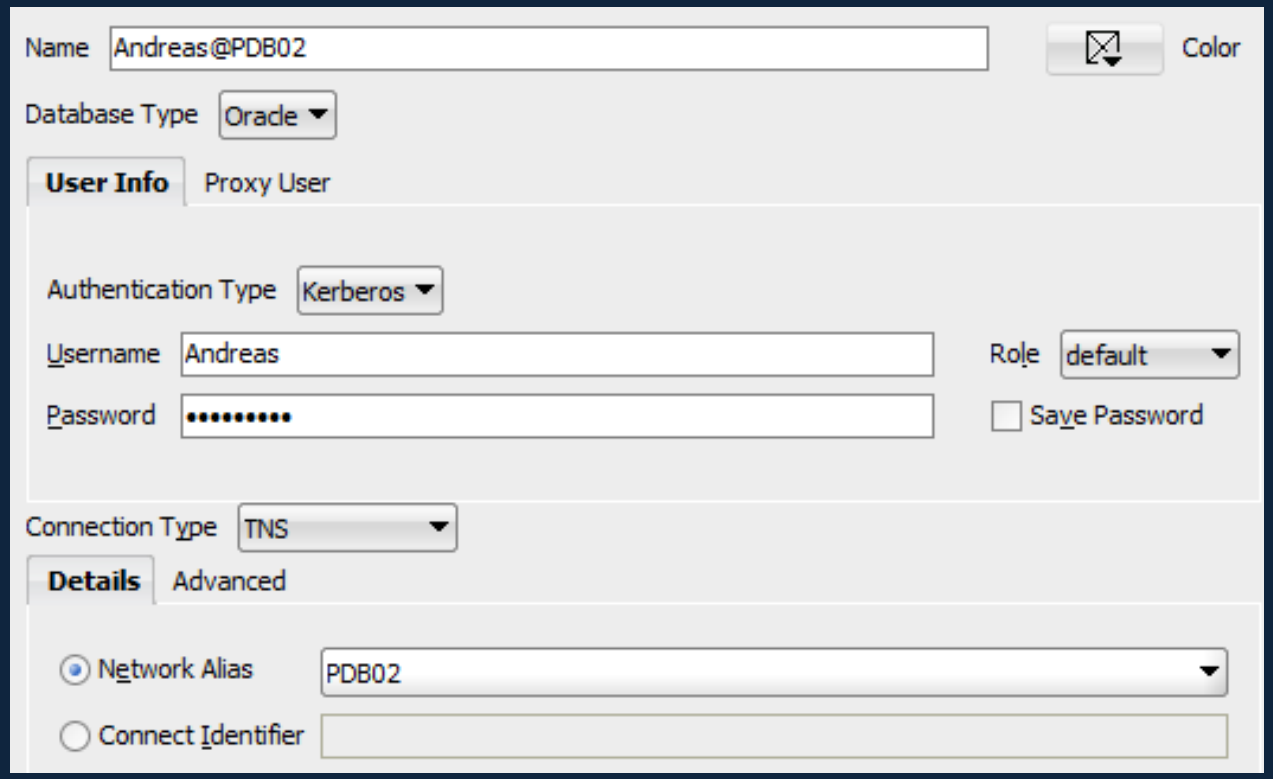
Falls das Labor nicht funktioniert…

ORDIX AG

```
PS C:\> klist

Current LogonId is 0:0x6f3e55

Cached Tickets: (2)

#0>     Client: Andreas @ ORDIX.LOCAL
        Server: krbtgt/ORDIX.LOCAL @ ORDIX.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 11/8/2023 19:01:55 (local)
        End Time:   11/9/2023 5:01:55 (local)
        Renew Time: 11/15/2023 19:01:55 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: DC

#1>     Client: Andreas @ ORDIX.LOCAL
        Server: oracle/db02.ordix.local @ ORDIX.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 11/8/2023 19:03:01 (local)
        End Time:   11/9/2023 5:01:55 (local)
        Renew Time: 11/15/2023 19:01:55 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called: DC.ordix.local
```

Falls das Labor nicht funktioniert…

ORDIX AG



Einrichtung von CMU auf dem Domain Controller
Achtung: Nur Teilkomponenten von CMU

ORDIX AG

- Es wird ein zentraler Benutzer für den Zugriff aller Oracle Server benötigt.

```
$serviceUserParams = @{
    Name                  = 'OracleCMU'
    DisplayName           = 'User for Oracle CMU'
    Path                  = 'CN=Managed Service Accounts,DC=ordix,DC=local'
    PasswordNeverExpires  = $true
    Enabled               = $true
    AccountPassword       = $password
}
New-ADUser @serviceUserParams
```

- Es wird das Zertifikat benötigt.

```
certutil.exe '-ca.cert' rootcert.txt
```

- Die folgenden Anpassungen sind nicht notwendig:
  - Erweiterung des Active Directory Schemas.
  - Einrichtung einer Passwort-Filter-Bibliothek.

Einrichtung von CMU auf den Oracle Servern
Wallet

ORDIX AG

- Für das Wallet

```
$walletPath = '/opt/oracle/admin/CDB02/wallet'
$certPath   = '/tmp/rootcert.txt'
$userName   = 'OracleCMU'
$userDn     = 'CN=Managed Service Accounts,DC=ordix,DC=local'

orapki wallet create -wallet $walletPath -auto_login
mkstore -wrl $walletPath -createEntry ORACLE.SECURITY.USERNAME $userName
mkstore -wrl $walletPath -createEntry ORACLE.SECURITY.DN $userDn
mkstore -wrl $walletPath -createEntry ORACLE.SECURITY.PASSWORD
orapki wallet add -wallet $walletPath -trusted_cert -cert $certPath
```

Einrichtung von CMU auf den Oracle Servern
dsi.ora, sqlnet.ora und Oracle Parameter

ORDIX AG

- Die Datei dsi.ora ist in ldap-admin anzulegen.

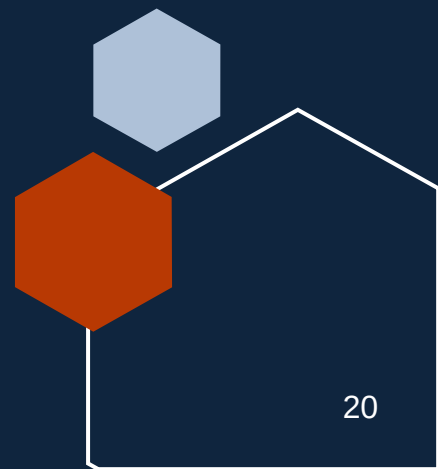
```
DSI_DIRECTORY_SERVERS = (<DC>.<domain>:389:636)
DSI_DEFAULT_ADMIN_CONTEXT = "<Distinguished Name der Domain>"
DSI_DIRECTORY_SERVER_TYPE = AD

DSI_DIRECTORY_SERVERS = (dc.ordix.local:389:636)
DSI_DEFAULT_ADMIN_CONTEXT = "DC=ordix,DC=local"
DSI_DIRECTORY_SERVER_TYPE = AD
```

- Die Datei sqlnet.ora ist zu ergänzen.

```
WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=<walletPath>)))
```

- Die folgenden Oracle Parameter sind zu setzen und die Instanz ist neu zu starten.

```
ALTER SYSTEM SET ldap_directory_access = PASSWORD
ALTER SYSTEM SET ldap_directory_sysauth = YES
```



Einrichtung von Datenbankbenutzern für CMU

ORDIX AG

```
CREATE USER OracleUsers IDENTIFIED GLOBALLY AS 'CN=OracleUsers,<UserOuDn>'
CREATE ROLE ReportsRole IDENTIFIED GLOBALLY AS 'CN=OracleReports,<UserOuDn>'
```

Testen wir das doch mal in meinem Labor…

Falls das Labor nicht funktioniert…

ORDIX AG

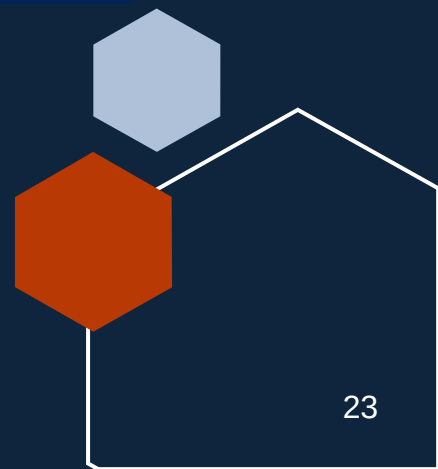
```
$credential = Get-Credential -Message 'Test User'
$userParams = @{
    Name              = $credential.UserName
    AccountPassword = $credential.Password
    Path              = 'OU=OracleUser,DC=ordix,DC=local'
    Enabled           = $true
}
New-ADUser @userParams

$groupParams = @{
    Name           = 'DOAG_Teilnehmer'
    Path           = 'OU=OracleUser,DC=ordix,DC=local'
    GroupScope     = 'Global'
    GroupCategory = 'Security'
}
New-ADGroup @groupParams
Add-ADGroupMember -Identity DOAG_Teilnehmer -Members $credential.UserName
```

```
CREATE USER doag_teilnehmer IDENTIFIED GLOBALLY AS 'CN=DOAG_Teilnehmer,OU=OracleUser,DC=ordix,DC=local';
GRANT CREATE SESSION TO doag_teilnehmer;
```

Falls das Labor nicht funktioniert…

ORDIX AG

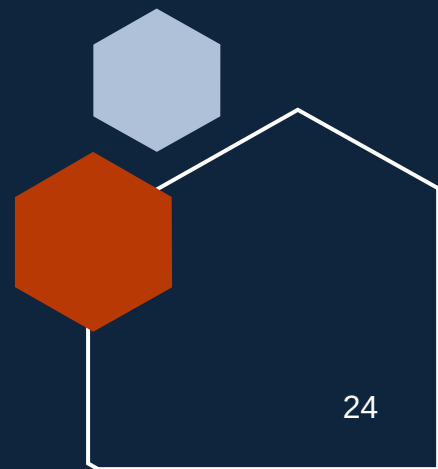
```
PS C:\> whoami
ordix\jordan
PS C:\> klist

Current LogonId is 0:0xadad53

Cached Tickets: (1)

#0>     Client: Jordan @ ORDIX.LOCAL
        Server: krbtgt/ORDIX.LOCAL @ ORDIX.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 11/8/2023 20:21:41 (local)
        End Time:   11/9/2023 6:21:41 (local)
        Renew Time: 11/15/2023 20:21:41 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: DC
```



Falls das Labor nicht funktioniert…

ORDIX AG

```
PS C:\> sqlplus /@PDB02

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Nov 8 20:22:07 2023
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> select user from dual;

USER
------------------------------------------------------------------------------
DOAG_TEILNEHMER

SQL>
```



Falls das Labor nicht funktioniert…

ORDIX AG

```
$groupParams = @{
    Name           = 'DOAG_Referenten'
    Path           = 'OU=OracleUser,DC=ordix,DC=local'
    GroupScope     = 'Global'
    GroupCategory = 'Security'
}
New-ADGroup @groupParams
Add-ADGroupMember -Identity DOAG_Referenten -Members $credential.UserName
```

```
CREATE ROLE doag_referenten IDENTIFIED GLOBALLY AS 'CN=DOAG_Referenten,OU=OracleUser,DC=ordix,DC=local';
```

```
SQL> select role from session_roles;

ROLE
--------------------------------------------------------------------------------
DOAG_REFERENTEN
```

Vielen Dank für Ihre Aufmerksamkeit

ORDIX AG

Aktiengesellschaft für Softwareentwicklung, Schulung, Beratung und Systemintegration

Zentrale Paderborn
Karl-Schurz-Straße 19a
33100 Paderborn
Tel.: 05251 1063-0
Fax: 0180 1 67349 0

Seminarzentrum Wiesbaden
Kreuzberger Ring 13
65205 Wiesbaden
Tel.: 0611 77840-00

info@ordix.de
https://www.ordix.de/