ORACLE®

Oracle Database: Net Naming and Single Sign-on with Active Directory

Santanu Datta
Vice President of Development, Oracle

Alan Williams
Senior Principal Product Manager, Oracle

Christian Shay
Senior Principal Product Manager, Oracle

ORACLE OPEN WORLD

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. New – Centrally Managed Users (CMU) NEW IN 18c
4. Q&A

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Active Directory for Name Resolution

Centralize configuration and reduce administration

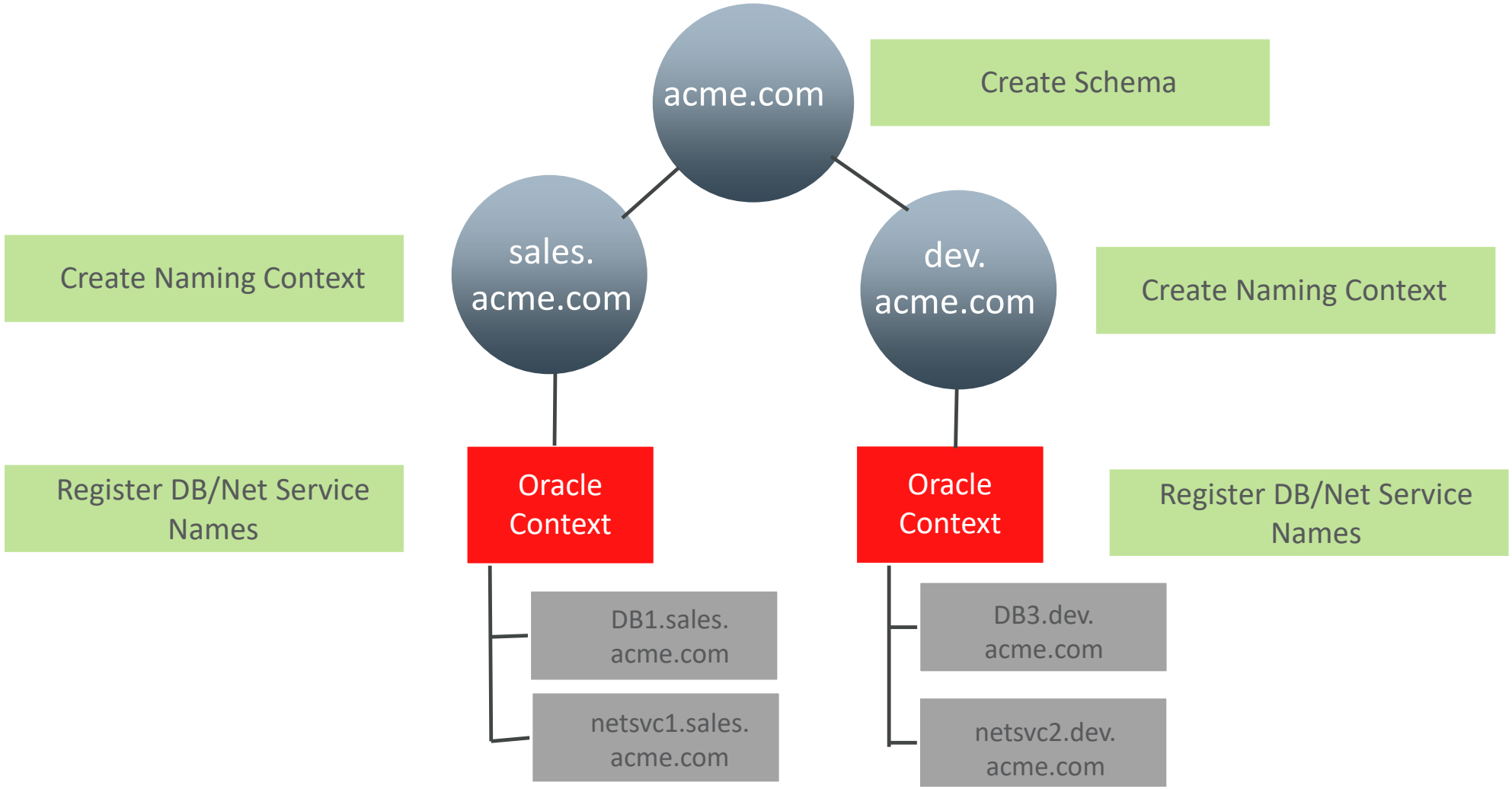
- Store and resolve Net names (used for database connections) through Active Directory
  - Active Directory is used as a central repository instead of local TNSNAMES.ORA
- Supports DB clients on Windows connecting to DB servers on any platform
- Supports authenticated connection to Active Directory (11g+ clients)

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Active Directory for Name Resolution

Directory Structure



Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Active Directory for Name Resolution

Tools

Oracle Net Configuration Assistant (NetCA)

- Configures Active Directory
- Configures local ldap.ora

Oracle Net Manager

- Registers Net Service Names in Active Directory

Additional Tools

Database Configuration Assistant (DBCA)

- Register Database names in Active Directory

AD User and Computers

- Browse Net names
- Connect to Oracle Database

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Active Directory for Name Resolution
Configuration/Administration

1 – Ensure that Administrator can modify Schema in Active Directory
(Check membership in Schema Admins group,
Enable Schema modifications on a Domain Controller)

2 – Register Schema using NetCA
(Verify with ADSIEDIT)

Windows System

Active Directory/KDC

3 - Create Naming Context using NetCA
(This creates directory object)

4 - Register database in AD using DBCA or Net Manager
(This creates directory object)

Repository of Database Names and Net Service Names

5 - Configure Directory Naming and Directory Usage (AD) using NetCA
(this sets up LDAP.ORA and SQLNET.ORA)

Database Client Systems on Windows

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Active Directory for Name Resolution

SQL*Net configuration files

- **LDAP.ORA**

  DEFAULT_ADMIN_CONTEXT = **"DC=rtdom,DC=netdev"**
  DIRECTORY_SERVER_TYPE = AD

- **SQLNET.ORA**

  NAMES.DIRECTORY_PATH= (LDAP, TNSNAMES, EZCONNECT)
  NAMES.LDAP_AUTHENTICATE_BIND = TRUE

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Active Directory for Name Resolution

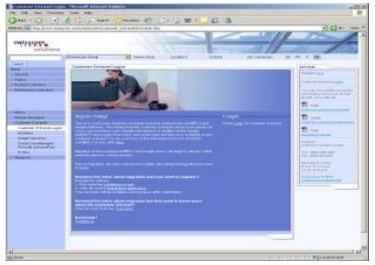
Run-time

Repository (Database Names and Net Service Names)

3 - Retrieves Connect Descriptor

Active Directory/KDC

1 – User signs on to Desktop



2 – User issues Connect Request

4 - Connect to Database using Connect Descriptor

Oracle Database (Any Platform)

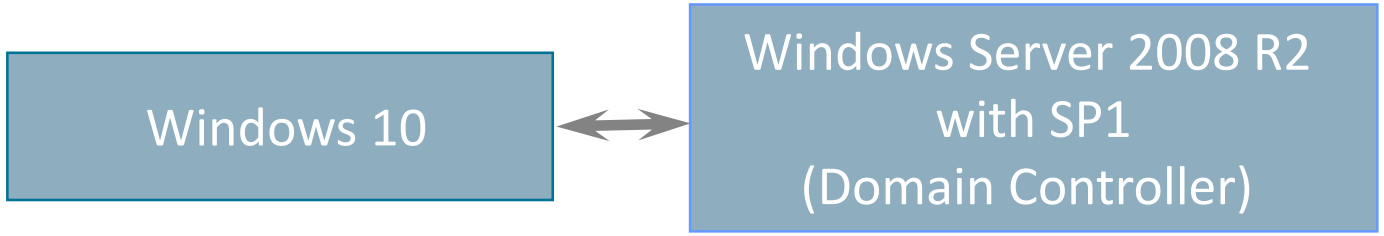
Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Active Directory for Name Resolution

Demo Environment

Machine Name:
W10Client.rtdom.netdev
Windows Users:
oracle, test
Database Server:
SID: orcl
PDB: orclpdb
OS installed: Windows 10

Machine Name:
W2K8Server.rtdom.netdev
Domain: rtdom.netdev
OS installed: Windows Server 2008 R2 with SP1



Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Net Naming with Active Directory

Demo

Copyright © 2017, Oracle and/or its affiliates. All rights reserved. |

Active Directory for Name Resolution
Configuration Steps: Summary

1. Ensure that Administrator can modify Schema in AD
2. Register Schema using NetCA (once for the entire AD forest)
3. Create Naming Context using NetCA (once per domain)
4. Register Database in AD using DBCA or Net Manager
5. Configure Directory Naming and Directory Usage (AD) using NetCA or copy proper LDAP.ORA and SQLNET.ORA files (on systems that want to use AD)

Please refer to the white paper ***Configuring Microsoft Active Directory for Net Naming*** for detailed information

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Comparison between OID and Active Directory support

OS Platform	Active Directory	Oracle Internet Directory
DB Client on Windows (DB Server on any platform)	✓ *	✓
DB Client on any other OS platform	Not supported	✓

* NetCA and Net Manager must be run on Windows platforms for schema/container creation and registration of Net service names

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

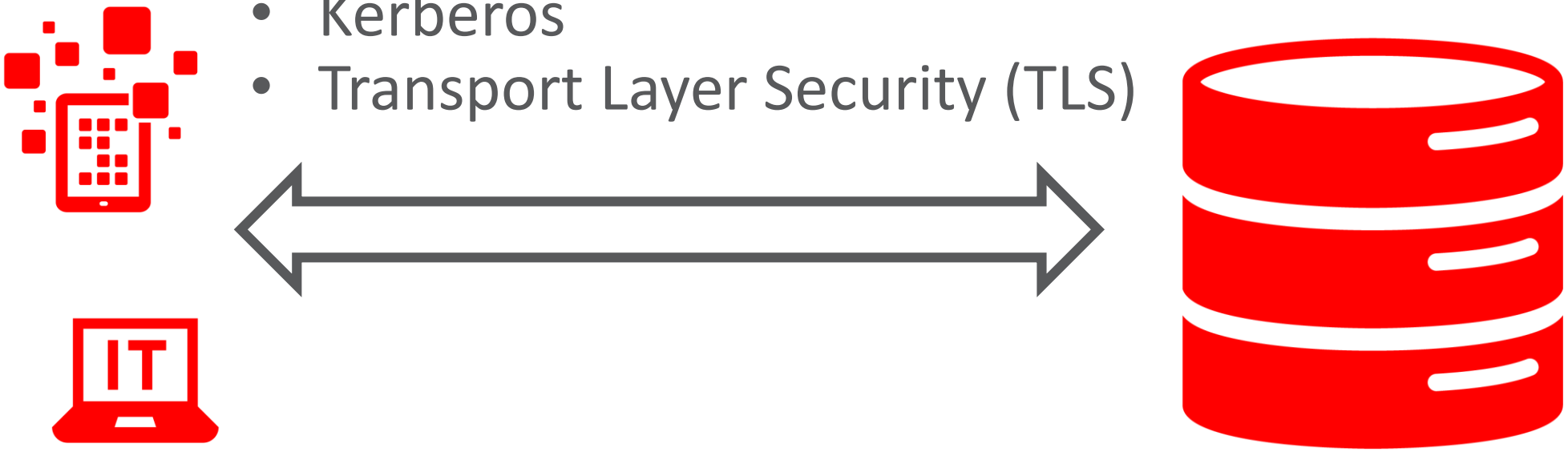
Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. New – Centrally Managed Users (CMU) NEW IN 18c
4. Q&A

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Single Sign-on

- Windows Native Authentication (NTS)
- Kerberos
- Transport Layer Security (TLS)



Oracle Database

Completely independent of "Active Directory for Name Resolution" feature

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Authentication Methods: Platform Support

Platforms	Windows Native Authentication (NTS)	Kerberos including MS KDC support	TLS
Windows only environment	✓	✓	✓
All OS Platforms		✓	✓ *

* MS certificate store is supported on Windows clients only

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Windows Native Authentication

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Windows Native Authentication

- Enabled by default and works across Windows systems
  - Ensure that *sqlnet.authentication_services* is set to NTS on both client and server systems in sqlnet.ora (default set up)
- Windows user logon credentials implicitly used for database authentication
- Optional Client-side sqlnet.ora parameter (new feature in 12.1)
  - "no_ntlm”, which can be set to "true“ to disable NTLM. (Note: only Domain Users can use Kerberos)

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Windows Native Authentication
Database Administrative Users

- Add Windows users to specific groups on the server system
- Authorization granted through Windows group membership

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Windows Native Authentication
SYSDBA and SYSOPER Privileges

- ORA_DBA
  - All members get SYSDBA privileges for all Oracle Databases on the system
- ORA_OPER
  - All members get SYSOPER privileges for all Oracle Databases on the system
- ORA_<HomeName>_DBA (12c)
  - All members get SYSDBA privileges for Oracle Databases on a specific Oracle Home
- ORA_<HomeName>_OPER (12c)
  - All members get SYSOPER privileges for Oracle Databases on a specific Oracle Home

All the groups are on the server system

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Windows Native Authentication
Separation of Privileges

- ORA_<HomeName>_ SYSBACKUP (12c)
  - All members get Backup privileges (SYSBACKUP) for databases on a specific Oracle Home
- ORA_<HomeName>_SYSDG (12c)
  - All members get Data Guard Privileges (SYSDG) for databases on a specific Oracle Home
- ORA_<HomeName>_ SYSKM (12c)
  - All members get Encryption Key Management privileges (SYSKM) for databases on a specific Oracle Home

All the groups are on the server system

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Windows Native Authentication
Administrative Privileges for ASM Instance

- ORA_ASMADMIN (12c)
  - All members get SYSASM administration privileges on the computer
- ORA_ASMDBA (12c)
  - All members get SYSDBA privileges for ASM Instance on the computer
- ORA_ASMOPER (12c)
  - All members get SYSOPER privileges for ASM Instance on the computer

Note: ORA_DBA and ORA_OPER group members get SYSDBA and SYSOPER privileges for ASM instance in 11g and older releases only

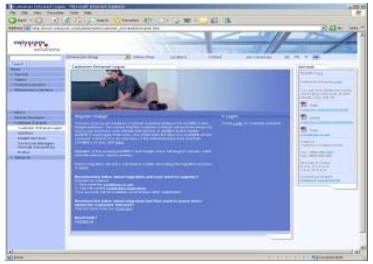
All the groups are on the server system

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Windows Native Authentication

Database Administrative Users



MS Active Directory/KDC

Oracle Database

1 - User signs on to desktop

2 - User attempts to sign on to Oracle

3 – Negotiate security protocol and exchange security tokens

4 – Find Windows identity of the user

5 – Find Windows Group memberships for the user in pre-defined group(s)

6 – Allow logon if the Windows user is a member of the required group(s)

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Windows Native Authentication

Database Regular Users

- Set *os_authent_prefix* to “” in init.ora for the Database
- For each Windows user, a corresponding external user needs to be created in Oracle DB

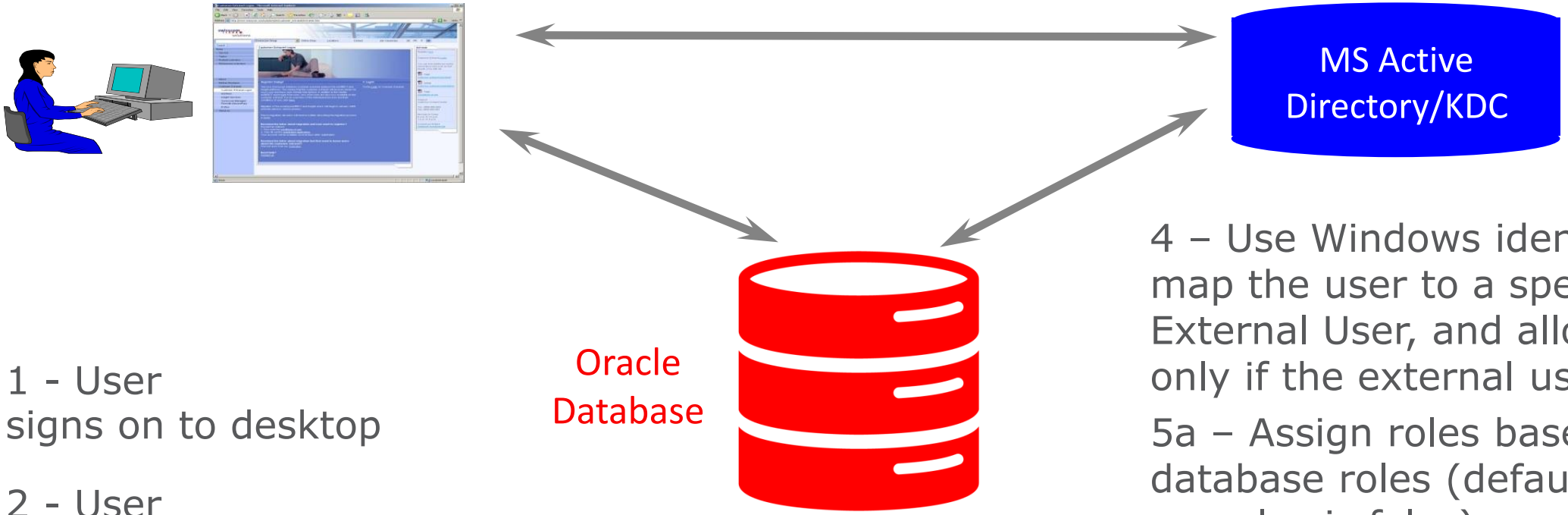
  e.g. create user “SALES\FRANK” identified externally;
- Role assignment based on Database Roles (default and most flexible)
- To enable role assignment based on Windows groups
  - Set os_*roles* to true
  - Create external role
    e.g. create role sales identified externally;
  - Create corresponding Windows group and add members to that group

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Windows Native Authentication

Database Regular Users



1 - User signs on to desktop

2 - User attempts to sign on to Oracle

3 – Negotiate security protocol and exchange security tokens

4 – Use Windows identity to map the user to a specific External User, and allow login only if the external user exists

5a – Assign roles based on database roles (default, i.e. os_roles is false)

5b – Find Windows Group memberships and assign roles based on group memberships (if os_roles is true)

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Windows Native Authentication

Summary

- Ensure that *sqlnet.authentication_services* is set to NTS on both client and server in sqlnet.ora (default set up)
- For database administrative users
  - Add Windows user to the appropriate group on database server system.
- For database regular users
  - Set *os_authent_prefix* to “” in init.ora
  - Create a corresponding external user for the Windows user
  - Assign database roles to the external user in the database.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Kerberos

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Kerberos Authentication

- Integrated with Microsoft Key Distribution Center (MSKDC)
- Supports heterogeneous systems
  - A Windows client can connect to a non-Windows server and vice versa
- Uses External User mechanisms in Database
- Supported with all Database Editions

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Kerberos Authentication

Server configuration

- Create an user in Active Directory for Database Server (e.g. dbservername.rtdom.netdev) with the following attributes:
  - "Kerberos DES" unchecked
  - "Kerberos AES 128 bit“, "Kerberos AES 256 bit", and "Kerberos preauthentication not required“ checked
- On the Domain Controller
  - Use ktpass utility (available from Microsoft) to create Kerberos "keytab" file ktpass -princ **oracle**/dbservername.rtdom.netdev@RTDOM.NETDEV -crypto all -pass Welcome1 -mapuser dbservername.rtdom.netdev@RTDOM.NETDEV -out v5srvtab
- Securely copy keytab file to DB server node and set proper file permissions
- Set *os_authent_prefix* to “” in init.ora

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Kerberos Authentication

Configuration on all systems

- Change the Kerberos entry in the Windows service file (C:\windows\system32\drivers\etc\services) from:
  kerberos 88/tcp krb5 kerberos-sec #Kerberos
  to:
  kerberos 88/tcp kerberos5 krb5 kerberos-sec #Kerberos
- Create Kerberos and sqlnet configuration files using Oracle Net Manager or copy appropriate configuration files to all the systems

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Kerberos Configuration Files

- **krb5.conf files (Client and Server):**

```
[libdefaults]
default_realm = RTDOM.NETDEV

[realms]
RTDOM.NETDEV = {
kdc = W2k8Server.rtdom.netdev
}

[domain_realm]
.rtdom.netdev = RTDOM.NETDEV
rtdom.netdev = RTDOM.NETDEV
```

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Kerberos Configuration Files

- **Sqlnet.ora (Server)**
  SQLNET.AUTHENTICATION_SERVICES= (KERBEROS5)
  SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = **oracle**
  SQLNET.KERBEROS5_CONFIG = C:\Temp\kerberos\krb5.conf
  SQLNET.KERBEROS5_CONF_MIT = TRUE
  SQLNET.KERBEROS5_KEYTAB = C:\Temp\kerberos\v5srvtab

- **Sqlnet.ora (Clients)**
  SQLNET.AUTHENTICATION_SERVICES= (KERBEROS5)
  SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = **oracle**
  SQLNET.KERBEROS5_CONFIG = C:\Temp\clientAdmin\kerberos\krb5.conf
  SQLNET.KERBEROS5_CONF_MIT = TRUE
  SQLNET.KERBEROS5_CC_NAME = MSLSA:

For Windows using 12.1+ DB Clients, use **MSLSA:**
For pre-12.1 Windows clients, use **OSMSFT:**
While configuring a client not using Microsoft Credential Cache (e.g. non-Windows systems), use okinit <username> to populate the credential cache and point to the file:
SQLNET.KERBEROS5_CC_NAME = c:\krb\krb.cc

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Kerberos Authentication
User Creation

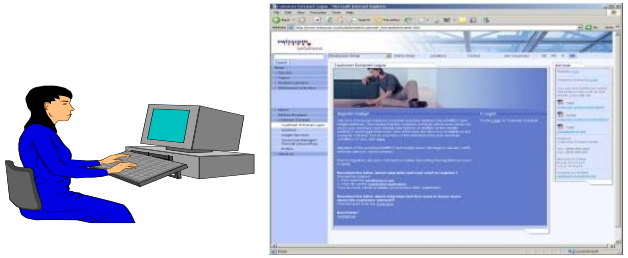
- An external user needs to be created in Oracle DB
  - CREATE USER "RTDOM\KRBUSER" IDENTIFIED EXTERNALLY AS "krbuser@RTDOM.NETDEV";

  (Please ensure that you use all capital letters while providing the DB user name)
- Role assignment based on Database Roles

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Kerberos Authentication



3 – Exchange security tokens to identify the Kerberos user

MS Active Directory/KDC

Oracle Database

1 - User signs on to desktop

2 - User attempts to sign on to Oracle

4 – Find Kerberos principal name of the user and map to the external user if the mapping exists

5 - Assign roles based on database roles for the user

Example:

```
SQL> CREATE USER "RTDOM\KRBUSER" IDENTIFIED EXTERNALLY AS
"krbuser@RTDOM.NETDEV";
SQL> Grant connect, resource to "RTDOM\KRBUSER";
```

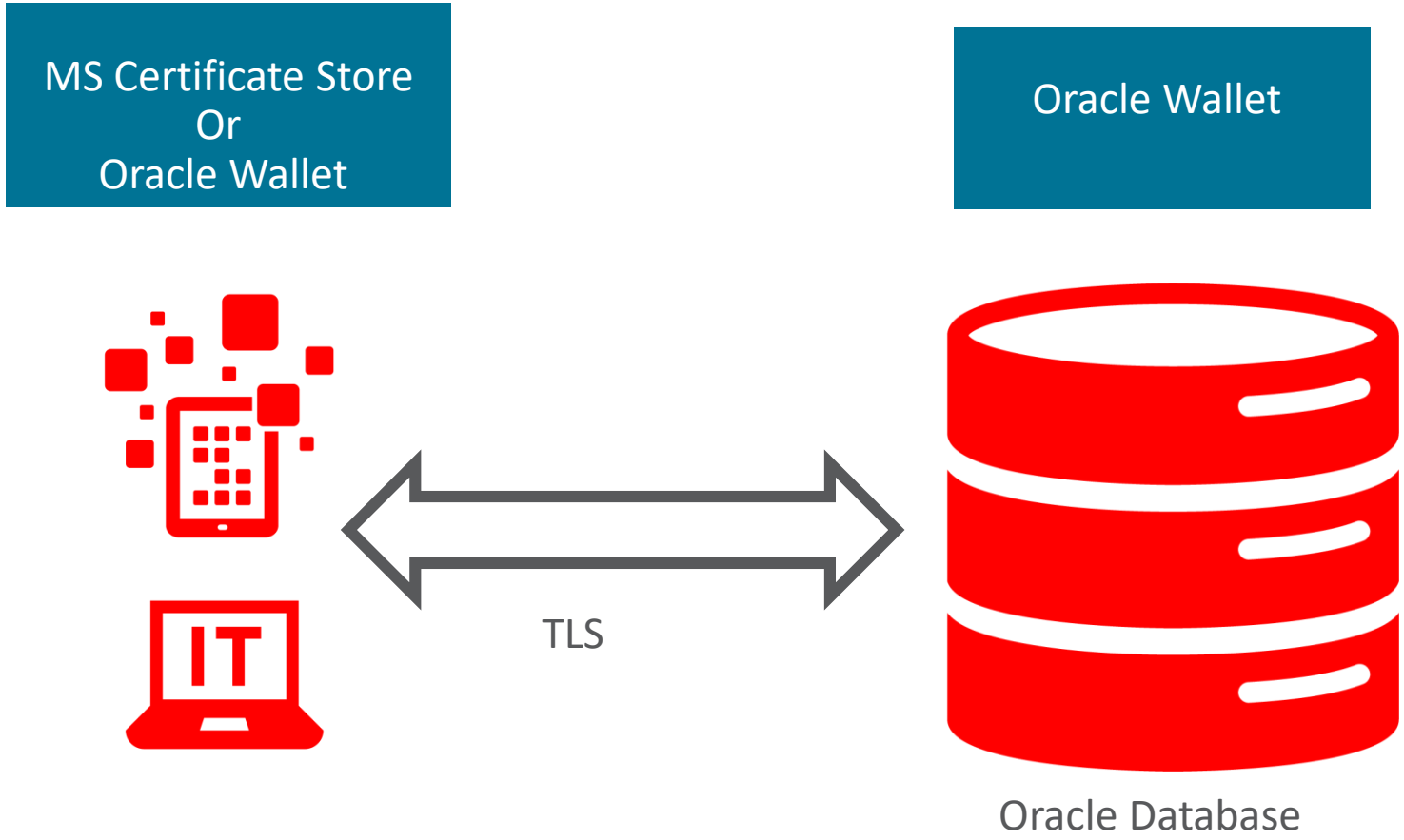
ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Transport Layer Security (TLS)

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

TLS



Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Microsoft Certificate Store support for TLS

- Load the pkcs12 formatted certificate in MS Certificate Store
  - Command line execution
    certutil -importPFX -f -p <password> -user ewallet.p12
  - GUI execution
    - Launch “Certificates” snap-in in mmc
    - Select "My user account", click "Finish" button
    - Import Client certificate into "Personal" from the desired location (e.g. "C:\tmp\walletloc\Client\ewallet.p12“)
- Set the following parameter in SQLNET.ORA
  - WALLET_LOCATION = (SOURCE = (METHOD = MCS))
  - Oracle Database Client retrieves the user certificate from MY or Personal certificate store.

ORACLE

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. |

Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. New – Centrally Managed Users (CMU) NEW IN 18c
4. Q&A

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Oracle Database Authentication and Authorization

Method	Authentication	Authorization
Password	Password verifier	Database Built-In (privileges and roles)
Kerberos	Kerberos ticket	Database Built-In
PKI Certificate	PKI certificate	Database Built-In
Operating System	Operating System	OS Groups, Database Built-In
RADIUS	RADIUS	RADIUS, Database Built-In
Enterprise User Security – directory services	Password, Kerberos, and Certificate	Directory sub-tree, enterprise roles, Database Built-In

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Oracle Database Authentication and Authorization

Method	Authentication	Authorization
Password	Password verifier	Database Built-In (privileges and roles)
Kerberos	Kerberos ticket	Database Built-In
PKI Certificate	PKI certificate	Database Built-In
Operating System	Operating System	OS Groups, Database Built-In
RADIUS	RADIUS	RADIUS, Database Built-In
Enterprise User Security – directory services	Password, Kerberos, and Certificate	Directory sub-tree, enterprise roles, Database Built-In

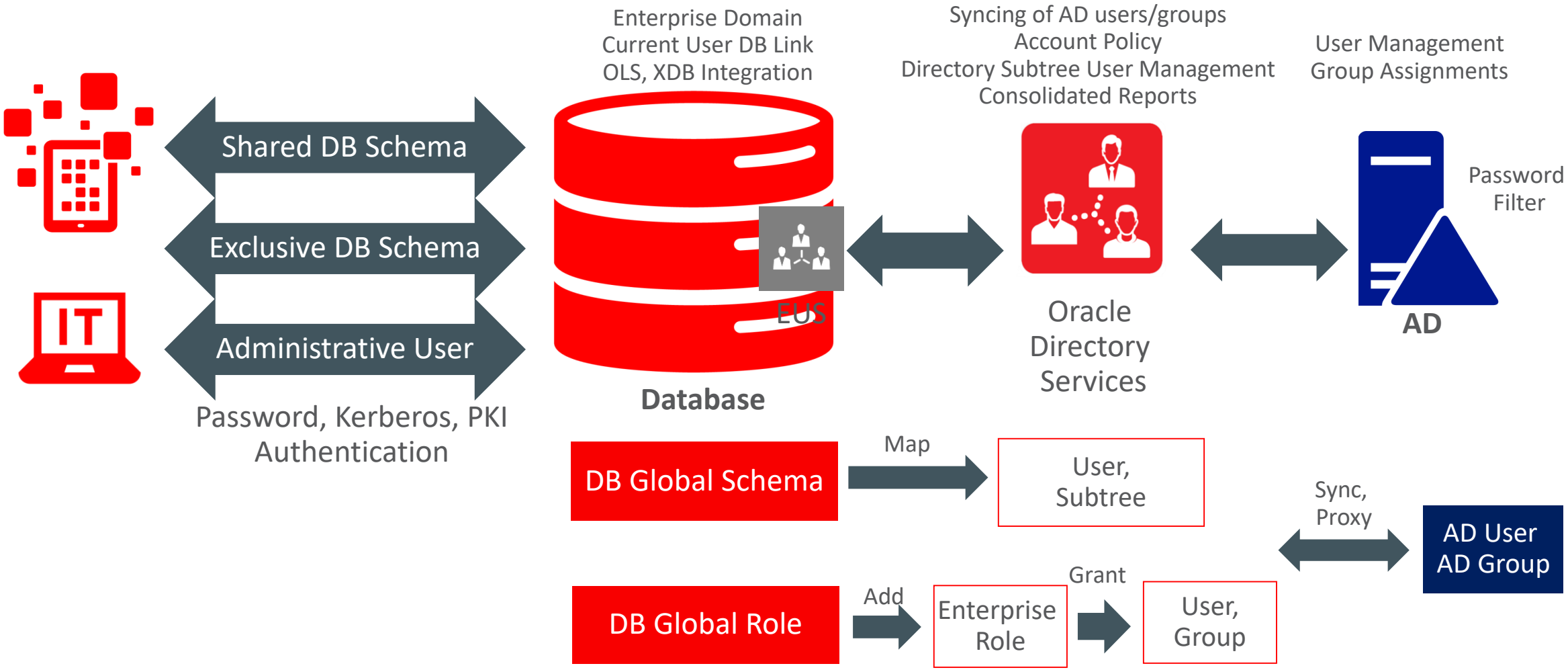
Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Oracle Database Authentication and Authorization

Method	Authentication	Authorization
Password	Password verifier	Database Built-In (privileges and roles)
Kerberos	Kerberos ticket	Database Built-In
PKI Certificate	PKI certificate	Database Built-In
Operating System	Operating System	OS Groups, Database Built-In
RADIUS	RADIUS	RADIUS, Database Built-In
Enterprise User Security – directory services	Password, Kerberos, and Certificate	Directory sub-tree, enterprise roles, Database Built-In
Centrally Managed Users with Active Directory (New with 18c)	Password, Kerberos, and Certificate	Active Directory Groups, Database Built-In

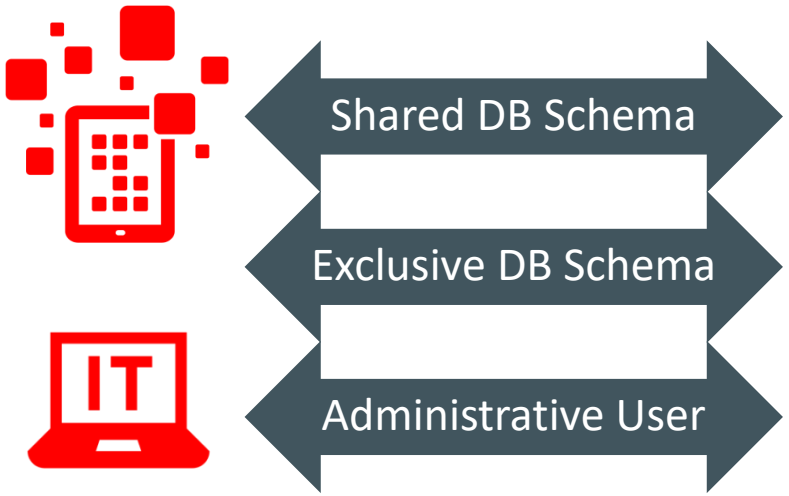
Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Legacy Active Directory Integration with EUS



Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

New Active Directory Integration with Oracle Database 18c



Password, Kerberos, PKI Authentication

Database

User Management
Group Assignments
Account Policy

Password Filter

Microsoft Active Directory

DB Global Schema → Map → AD User, AD Group

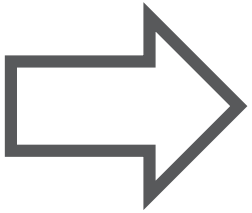
DB Global Role → Map → AD Group

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Authorization using Active Directory Groups and DB Roles

Database

Global user:
HR_RUNTIME



Directory

Domain (dc=examplecorp, dc=com)
cn = Users

Users:
Susan, Diana, Jennifer

Groups:
– hr–rep {*Susan, Diana, Jennifer*}

Map:
Global user HR_RUNTIME to AD Group hr-rep

CREATE USER HR_RUNTIME IDENTIFIED GLOBALLY AS
'cn=hr-rep,ou=hr,dc=examplecorp,dc=com';

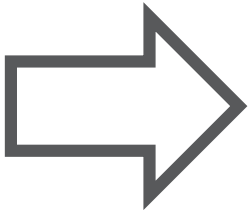
Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Authorization using Active Directory Groups and DB Roles

Database

Global user:
HR_RUNTIME

Global Role:
HR_MGR



Directory

Domain (dc=examplecorp, dc=com)
cn = Users

Users:
Susan, Diana, Jennifer

Groups:
- hr-rep {*Susan, Diana, Jennifer*}
- hr-mgr {*Susan*}

Map:
Global user HR_RUNTIME to AD Group hr-rep
Global role HR_MGR to AD Group hr-mgr

CREATE ROLE HR_MGR IDENTIFIED GLOBALLY AS
'cn=hr-mgr,ou=hr,dc=examplecorp,dc=com';

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Example of Susan's Login

```
SQL> CONNECT "examplead\susan"
Enter password:
Connected.
SQL> SHOW USER
USER is "HR_RUNTIME"
SQL> SELECT SYS_CONTEXT('USERENV','AUTHENTICATED_IDENTITY') FROM DUAL;

SYS_CONTEXT('USERNV','AUTHENTICATED_IDENTITY')
----------------------------------------------------------------------------
examplead\susan

SQL> SELECT SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY') FROM DUAL;

SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY')
----------------------------------------------------------------------------
cn=Susan Mavris,ou=hr,dc=examplecorp,dc=com

SQL> SELECT * FROM SESSION_ROLES:

ROLE
----------------------------------------------------------------------------
HR_MGR
```

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Example of Susan's Login

```
SQL> CONNECT "examplead\susan"
Enter password:
Connected.
SQL> SHOW USER
USER is "HR_RUNTIME"
SQL> SELECT SYS_CONTEXT('USERENV','AUTHENTICATED_IDENTITY') FROM DUAL;

SYS_CONTEXT('USERNV','AUTHENTICATED_IDENTITY')
----------------------------------------------------------------------------
examplead\susan

SQL> SELECT SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY') FROM DUAL;

SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY')
----------------------------------------------------------------------------
cn=Susan Mavris,ou=hr,dc=examplecorp,dc=com

SQL> SELECT * FROM SESSION_ROLES:

ROLE
----------------------------------------------------------------------------
HR_MGR
```

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Example of Susan's Login

```
SQL> CONNECT "examplead\susan"
Enter password:
Connected.
SQL> SHOW USER
USER is "HR_RUNTIME"
SQL> SELECT SYS_CONTEXT('USERENV','AUTHENTICATED_IDENTITY') FROM DUAL;

SYS_CONTEXT('USERNV','AUTHENTICATED_IDENTITY')
----------------------------------------------------------------------------
examplead\susan

SQL> SELECT SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY') FROM DUAL;

SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY')
----------------------------------------------------------------------------
cn=Susan Mavris,ou=hr,dc=examplecorp,dc=com

SQL> SELECT * FROM SESSION_ROLES:

ROLE
----------------------------------------------------------------------------
HR_MGR
```

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Example of Susan's Login

```
SQL> CONNECT "examplead\susan"
Enter password:
Connected.
SQL> SHOW USER
USER is "HR_RUNTIME"
SQL> SELECT SYS_CONTEXT('USERENV','AUTHENTICATED_IDENTITY') FROM DUAL;

SYS_CONTEXT('USERNV','AUTHENTICATED_IDENTITY')
----------------------------------------------------------------------------
examplead\susan

SQL> SELECT SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY') FROM DUAL;

SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY')
----------------------------------------------------------------------------
cn=Susan Mavris,ou=hr,dc=examplecorp,dc=com

SQL> SELECT * FROM SESSION_ROLES:

ROLE
----------------------------------------------------------------------------
HR_MGR
```

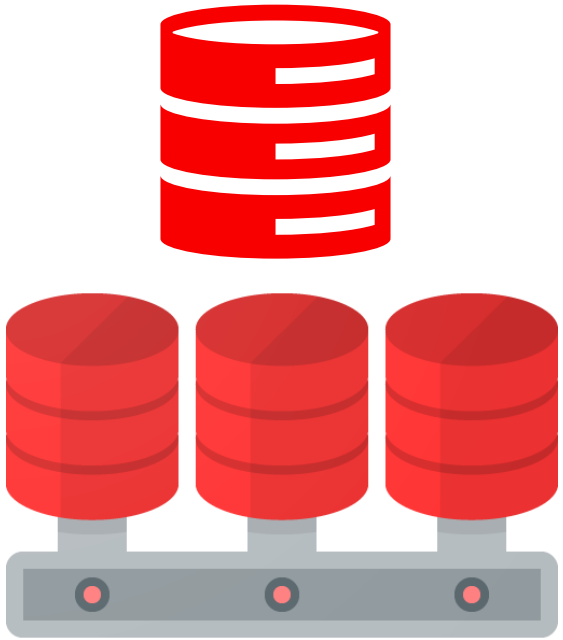
Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Example of Susan's Login

```
SQL> CONNECT "examplead\susan"
Enter password:
Connected.
SQL> SHOW USER
USER is "HR_RUNTIME"
SQL> SELECT SYS_CONTEXT('USERENV','AUTHENTICATED_IDENTITY') FROM DUAL;

SYS_CONTEXT('USERNV','AUTHENTICATED_IDENTITY')
----------------------------------------------------------------------------
examplead\susan

SQL> SELECT SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY') FROM DUAL;

SYS_CONTEXT('USERENV','ENTERPRISE_IDENTITY')
----------------------------------------------------------------------------
cn=Susan Mavris,ou=hr,dc=examplecorp,dc=com

SQL> SELECT * FROM SESSION_ROLES:

ROLE
----------------------------------------------------------------------------
HR_MGR
```

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Connecting Oracle Database to Active Directory



Net Naming Services

Oracle Directory Services

Centrally Managed Users

Active Directory Forest

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Steps to Connect to AD

- Create Oracle service directory user account in MSAD
- If using password authentication, install password filter and extend MSAD schema
- Create dsi.ora (can use ldap.ora)
- Get AD certificate
- Create wallet
- Verify wallet
- Configure AD connection

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Resources

- 18c Database Security Guide – Chapter 5
  - Most of this presentation is covered in the documentation

ORACLE Help Center

Home / Database / Oracle / Oracle Database / Release 18

Security Guide

Changes in This Release for Oracle Database Security Guide
1 Introduction to Oracle Database Security
Part I Managing User Authentication and Authorization
2 Managing Security for Oracle Database Users
3 Configuring Authentication
4 Configuring Privilege and Role Authorization
5 Configuring Centrally Managed Users with Microsoft Active Directory
Introduction to Centrally Managed Users with Microsoft Active Directory
Configuring the Oracle Database-Microsoft Active Directory Integration
Configuring

5 Configuring Centrally Managed Users with Microsoft Active Directory

Oracle Database can authenticate and authorize Microsoft Active Directory users with the database directly without intermediate directories or Oracle Enterprise User Security.

Introduction to Centrally Managed Users with Microsoft Active Directory
Centrally managed users (CMU) provides a simpler integration with Microsoft Active Directory to allow centralized authentication and authorization of users.

Configuring the Oracle Database-Microsoft Active Directory Integration
Before you can use Microsoft Active Directory to authenticate and authorize users, you must configure the connection from the Oracle database to Active Directory.

Configuring Authentication for Centrally Managed Users
You can configure password authentication, Kerberos authentication, or public key infrastructure (PKI) authentication.

Configuring Authorization for Centrally Managed Users
With centrally managed users, you can manage the authorization for Active Directory users to access Oracle databases.

Integration of Oracle Database with Microsoft Active Directory Account Policies
As part of the Oracle Database-Microsoft Active Directory integration, Oracle Database enforces the Active Directory account policies when Active Directory users log into the Oracle database.

Parent topic: Managing User Authentication and Authorization

Introduction to Centrally Managed Users with Microsoft Active Directory

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Choosing between EUS and CMU		EUS	CMU
Simplified Implementation			✓
Simplified Operations (movers, joiners, leavers)			✓
Authentication	Password, Kerberos, PKI certificates	✓	✓
	Enforce directory account policies	✓	✓
Authorization	Role authorization	✓	✓
	Administrative users	✓	✓
	Shared DB schema mapping	✓	✓
	Exclusive user mapping	✓	✓
Enterprise Domains	Current User trusted DB link	✓	
	Integrated with Oracle Label Security, XDB	✓	
	Consolidated reporting and management of data access	✓	

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Centrally Managed Users - Summary

- Simplified centralized directory services integration with less cost and complexity
  - Authentication in Active Directory for password, Kerberos and PKI
  - Map Active Directory Groups to shared database accounts and roles
  - Map database user to exclusive Active Directory user
  - Support Active Directory account policies
- No client update required
- Support all Oracle Database clients 11g and onwards (including WEBDAV)
- EUS and Oracle Directory Services authentication and authorization works as before

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. |

Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. New – Centrally Managed Users (CMU) NEW IN 18c
4. Q&A

Copyright © 2017, Oracle and/or its affiliates. All rights reserved. |

ORACLE®