Active Directory and Windows Security Integration with Oracle Database

Santanu Datta  
Vice President of Development  
Database Technologies

Christian Shay  
Principal Product Manager  
Windows and .NET  
Database Technologies
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, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. Windows Native Authentication
4. Kerberos
5. SSL
6. Web Applications: Security Integration
7. Q&A
Active Directory for Name Resolution

Overview

• Store and resolve Net names through Active Directory
  – Active Directory is used instead of tnsnames.ora
  – Authenticated connection to Active Directory (11g and later)
  – Anonymous connection for older clients

• Enhanced tools support for Net naming
  – Oracle Net Configuration Assistant
    • Configures Active Directory
    • Configures local ldap.ora
  – Oracle DB Configuration Assistant and Net Manager
    • Registers Database names/Net Service names in Active Directory
  – AD Users and Computers

Centralize Configuration
Reduce Administration
(Eliminate TNSNAMES.ORA)
Active Directory for Name Resolution

Directory Structure

Create Schema

Create Naming Context

Register DB/Net Service Names

Oracle Context

sales.acme.com

DB1.sales.acme.com

netsvc1.sales.acme.com

Oracle Context

dev.acme.com

DB3.dev.acme.com

netsvc2.dev.acme.com
Active Directory for Name Resolution
Configuration/Administration

1 - Ensure that Administrator can modify Schema in Active Directory
2 - Register Schema using NetCA

3 - Create Naming Context using NetCA
4 - Register database in AD using DBCA or Net Manager

5 - Configure Directory Naming and Directory Usage (AD) using NetCA

Repository of Database Names and Connect Descriptors

Active Directory/KDC

Windows System

Database Client Systems on Windows
Active Directory for Name Resolution

Run-time

1 – User signs on to Desktop

2 – User issues Connect Request

3 – Retrieves Connect Descriptor

4 – Connect to Database using Connect Descriptor

Repository (Database Names and Connect Descriptors)

Active Directory/KDC

Oracle Database

(Any Platform)
Active Directory for Name Resolution
Demo Environment

Machine Name: W7Client.rtdom.netdev
User: Oracle
Database Server (12cR1):
SID: orcl
PDB: pdborcl
OS installed: Windows 7

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

Windows 7 ↔ Windows Server 2008 R2 with SP1 (Domain Controller)
Active Directory for Name Resolution
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 (on systems that want to use AD)
6. Set NAMES.LDAP_AUTHENTICATE_BIND=Yes in SQLNET.ORA (11g and later clients)

To support pre-11g Clients
1. Enable anonymous bind in AD
2. Change ACLs for Oracle Naming Context and Database/Net Services objects to allow anonymous access

Please refer to the white paper Configuring Microsoft Active Directory for Net Naming for detailed information
# Active Directory for Name Resolution

## OID and Active Directory

<table>
<thead>
<tr>
<th>Client OS</th>
<th>Server OS</th>
<th>AD</th>
<th>OID</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Windows</td>
<td>Yes</td>
<td>Yes</td>
<td>Tools for registering Net Service in AD must be run on Windows</td>
</tr>
<tr>
<td>Windows</td>
<td>Any</td>
<td>Yes</td>
<td>Yes</td>
<td>AD Integration solutions can be used</td>
</tr>
<tr>
<td>Linux/Unix</td>
<td>Any</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. Windows Native Authentication
4. Kerberos
5. SSL
6. Web Applications: Security Integration
7. Q&A
Single Sign On

- Windows Native Authentication or OS Authentication (NTS)
- Kerberos
- SSL

Independent of “Active Directory for Name Resolution” feature
Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. Windows Native Authentication
4. Kerberos
5. SSL
6. Web Applications: Security Integration
7. Q&A
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: this only works for Domain Users)
Windows Native Authentication
Database Administrative Users

- Add Windows users to specific groups on the server system
- Authorization granted through Windows group membership
- Do not need to create corresponding users in Database
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
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
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
Windows Native Authentication
Database Administrative Users

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)
Windows Native Authentication

Database Regular Users

- 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
    e.g. Corresponding Windows group for a database with SID orcl:
    ORA_orcl_sales_d if this should be a default role.
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)
Windows Native Authentication
Configuration for Database Regular Users

• Ensure that sqlnet.authentication_services is set to NTS on both client and server in sqlnet.ora (default set up)
• Set os_authent_prefix to "" in init.ora
• Set os_roles to true in init.ora if you want to use Windows Group Membership for role authorization
DEMONSTRATION

Windows Native Authentication
Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. Windows Native Authentication
4. Kerberos
5. SSL
6. Web Applications: Security Integration
7. Q&A
Oracle Advanced Security Licensing Changes

“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 the Oracle database”

Please consult Database Licensing Guide for latest information
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
• Can also be supported with Enterprise User Security
Kerberos Authentication

• Removal of 30 character limit of the Kerberos user name (new limit is 1024 characters)
• Constrained Delegation support
  – Apply Kerberos Protocol Transitioning and Constrained Delegation fix (Bug 17012644)
• Connected User dblink support over Kerberos
• Kerberos authentication to Oracle database in a MS cross-domain setup
Kerberos Enhancements (12c)

• Security enhancements that were introduced in the MIT Kerberos Release 1.8 distribution
• In sqlnet.ora, set
  SQLNET.KERBEROS5_CC_NAME = MSLSA: (instead of OSMSFT:)
Kerberos Authentication

Server configuration

• Create an user in Active Directory for Database Server (e.g. w7client.rtdom.netdev) with the following attributes:
  – "Kerberos DES" unchecked
  – "Kerberos AES 128 bit" checked
  – "Kerberos AES 256 bit" checked
  – "Kerberos preauthentication not required" checked

• On the Domain Controller
  • Use ktpass utility (available from Microsoft) to create Kerberos "keytab" file
    ktpass -princ oracle/w7client.rtdom.netdev@RTDOM.NETDEV -crypto all -pass Welcome1 -mapuser w7client.rtdom.netdev@RTDOM.NETDEV -out v5srvtab
  • Copy keytab file to DB server node
Kerberos Authentication

Server configuration

• 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 on the sever using Oracle Net Manager

• Set os_authent_prefix to "" in init.ora
Kerberos Authentication

Client Configuration

- 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

- On Windows clients, you may set sqlnet.kerberos5_cc_name to “OSMSFT:” (Pre-12.1) or “MSLSA:” (12.1+) in sqlnet.ora so that the credential is retrieved from Microsoft Credential Cache

- If you are not using Microsoft Credential Cache (e.g. Linux/Unix clients), use okinit <username> to get the Kerberos credential cache file
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
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:

MSLSA: indicates that you are using Microsoft Credential Cache on a Windows system. While configuring a client not using Microsoft Credential Cache (e.g. non-Windows systems), change the last line to:
SQLNET.KERBEROS5_CC_NAME = c:\krb\krb.cc

C:\krb\krb.cc should point to the credential file obtained through okinit.
Kerberos Authentication

User Creation

• An external user needs to be created in Oracle DB
  —CREATE USER "RTDOM\KRUSER" 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

• Enterprise User Security can be used for role assignment based on group memberships (Optional)
Kerberos Authentication

1 - User signs on to desktop

2 - User attempts to sign on to Oracle

3 - Exchange security tokens to identify the Kerberos user

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\KRUSER" IDENTIFIED EXTERNALLY AS "krbuser@RTDOM.NETDEV";
SQL> Grant connect, resource to "RTDOM\KRUSER";
```
Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. Windows Native Authentication
4. Kerberos
5. SSL
6. Web Applications: Security Integration
7. Q&A
Microsoft Certificate Store support for SSL

Configuration:

- Load the pkcs12 formatted certificate in MS Certificate Store, Example:
  - `certutil -importPFX -f -p welcome -user ewallet.p12`
- Ensure that there is a common trust point between server and client certificate
- 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.
Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. Windows Native Authentication
4. Kerberos
5. SSL
6. Web Applications: Security Integration
7. Q&A
Web Applications on Windows

Recommend the use of Application Context/Client ID for end-to-end auditing and security
Web User Authentication Solutions

• ASP.NET Membership and Role Provider for Oracle
  – Validate and manage user and authorization information for your ASP.NET web applications in Oracle Database
  – Oracle Database can be on any platform

• Oracle Identity Management solutions
  – Integrated with Active Directory
  – Supports heterogeneous environments
  – Check http://www.oracle.com/identity

These are Oracle provided solutions which can be used in addition to the solutions provided by Microsoft
Web User Authentication on Windows

Active Directory/KDC

Web Applications On Windows (IIS)

Oracle Identity Management

Oracle Database

1. ASP.NET Providers
2. Oracle Identity Management and AD integration

Web User Authentication on Windows
Web Applications to Database Authentication

• User ID/Password
  – If you must use it, use Secure External Password Store (in Oracle Wallet) to store the password securely
  – Database can be on any platform

• Windows Native Authentication or Kerberos
  – Run Web Applications as Windows Services (specific Windows user) or use IIS mechanisms for mapping Web users to Windows users
  – Use OS authenticated connection pool for performance
  – Use Windows Native Authentication if Database server is on Windows
  – Use Kerberos authentication if Database server is on a non-Windows platform
    – Set up Kerberos to use MS Credentials cache, i.e. “MSLSA:” (or “OSMSFT:”)
Summary

- Oracle Database fully Integrated with Active Directory and Windows Security
  - Name Resolution
  - Single Sign On
  - Security Integration for Web Applications
For More Information

- Windows Server System Center
- Oracle .NET Developer Center
- Identity Management
Upcoming Windows/.NET Sessions

• Best Practices for Oracle Database Performance on Windows
  – Monday – 5:15 PM – 6:00 PM Moscone South – 305

• What’s New with Oracle Database on Windows: On-premises and in the Cloud
  – Wednesday – 1:45 PM – 2:30 PM Moscone South – 308

• Visit Windows experts at the Demogrounds:
  Oracle Database 12c on Windows
  – Today through Wednesday
  – Moscone South Exhibition Hall, Far Left Middle in Oracle Database Demogrounds
  – Booth SLD-003

• Getting Started with Oracle and .NET
  – Tuesday – 4:00 PM – 4:45 PM Moscone South – 305
Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. Windows Native Authentication
4. Kerberos
5. SSL
6. Web Applications: Security Integration
7. Q&A
Keep Learning with Oracle University

UNIVERSITY

Classroom Training
Learning Subscription
Live Virtual Class
Training On Demand

Cloud
Technology
Applications
Industries

education.oracle.com
Safe Harbor Statement

The preceding 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, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Integrated Cloud
Applications & Platform Services