Microsoft Active Directory and Windows Security Integration with Oracle Database

Santanu Datta
Vice President
Server Technologies

Christian Shay
Principal Product Manager
Server 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. Web Applications: Security Integration
6. 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
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
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

Windows 7

Window Server 2008 R2 with SP1
(Domain Controller)

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

Domain: rtdom.netdev
OS installed: Windows Server 2008 R2 with SP1
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></td>
</tr>
<tr>
<td>Windows</td>
<td>Any</td>
<td>Yes</td>
<td>Yes</td>
<td>Tools for registering Net Service in AD must be run on Windows</td>
</tr>
<tr>
<td>Linux/Unix</td>
<td>Any</td>
<td>No</td>
<td>Yes</td>
<td>AD Integration solutions can be used</td>
</tr>
</tbody>
</table>
Program Agenda

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

- Enabled by default and works across Windows systems
- Windows user logon credentials 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)
- For using Windows users as Database Administrative Users (e.g. / as SYSDBA)
  - Do not need to create corresponding users in Database
  - Authorization granted through Windows group membership
- For using Windows users as Database Regular Users (e.g. / )
  - Corresponding users must be created in Database
  - Authorization mostly granted through Database Roles assigned to the Database User
  - Optionally, authorization can be granted through Windows group membership
    (os_roles=true)
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

Oracle Database

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)

MS Active Directory/KDC
Windows Native Authentication
Database Administrative Users

- Ensure that `sqlnet.authentication_services` is set to NTS on both client and server in `sqlnet.ora` (default set up)
Windows Native Authentication

Database Regular Users

• An 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 identify as a specific External User

5 - Find Windows Group memberships (if os_roles is true)

6 - Assign roles based on database roles or group memberships (based on os_roles)
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
Windows Native Authentication
Program Agenda

1. Active Directory for Name Resolution
2. Single Sign on
3. Windows Native Authentication
4. Kerberos
5. Web Applications: Security Integration
6. 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 Enhancements (11g)

- IPv6 Support
- Constrained Delegation support
  - Supports Windows Server constrained delegation feature
  - Middle tier applications can use Kerberos adapter and authenticate to Oracle DB on behalf of the Windows user (uses MS Credentials Cache)
- Connected User dblink support over Kerberos
Kerberos Enhancements (11g)

- Stronger encryption algorithms (AES)
  - Support default encryption type supported by MS KDC
  - Encryption type configuration no longer needed in Registry
- Use DNS Domain Name as Kerberos REALM name by default
  - Mapping between DNS Domain Name and Kerberos REALM name no longer needed in kerberos config file
- Kerberos authentication to Oracle database in a MS cross-domain setup
- Removal of 30 character limit of the Kerberos user name (new limit is 1024 characters)
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)

• 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

• Set os_authent_prefix to "" in init.ora

• Create Kerberos and sqlnet configuration files on the sever using Oracle Net Manager
Kerberos Authentication
Windows Client Configuration

• Create Kerberos and sqlnet configuration files using Oracle Net Manager
  – 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
  [On Linux/Unix Database Clients, use okinit <username> since Microsoft Credential Cache can not be used]
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_CONF = C:\Temp\kerberos\krb5.conf
  SQLNET.KERBEROS5_CONF_MIT = TRUE
  SQLNET.KERBEROS5_KEYTAB = C:\Temp\kerberos\v5srvtab

• **Sqlnet.ora (Client):**
  SQLNET.AUTHENTICATION_SERVICES= (KERBEROS5)
  SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
  SQLNET.KERBEROS5_CONF = C:\Temp\clientAdmin\kerberos\krb5.conf
  SQLNET.KERBEROS5_CONF_MIT = TRUE
  SQLNET.KERBEROS5_CC_NAME = MSLSA:
Kerberos Authentication
User Creation

• An external user needs to be created in Oracle DB
e.g. CREATE USER “RTDOM\KRUSER” IDENTIFIED EXTERNALLY AS “krbuser@RTDOM.NETDEV”;

• 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 - Identify as a specific External User and assign roles based on database roles

Example:

```sql
SQL> CREATE USER "RTDOM\KRUSER" IDENTIFIED EXTERNALLY AS "krbuser@RTDOM.NETDEV";
SQL> Grant connect, resource to "RTDOM\KRUSER";
```
Each person has one username/password (or identity) for ALL databases. Directory identities are *mapped* to database schemas. Directory groups are *mapped* to database roles.
Program Agenda

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

Active Directory/KDC

Web Applications On Windows (IIS)

Oracle Database

Web User Authentication

Web Application to DB Authentication

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

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

1. ASP.NET Providers
2. Oracle Identity Management and AD integration
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
  – Windows Native Authentication
    • Database must be on Windows
  – Kerberos authentication
    • Set up Kerberos to use MS Credentials cache, i.e. "OSMSFT:" (or MSLSA:)
    • Database can be on any platform
Web Applications on Windows

Web Applications On Windows (IIS)

1. User id and Password
2. Windows Native Authentication or Kerberos (no EUS)
3. Kerberos (with EUS)

Oracle Identity Management

Active Directory/KDC

Oracle Database

Web Application to DB Authentication
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
Questions and Answers