Microsoft Active Directory and Windows Security Integration with Oracle Database

Santanu Datta
VP, Development

Christian Shay
Principal PM

Etienne Remillon
Sr. Principal PM
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

• Active Directory for Name Resolution
• Single Sign On
• Web Applications: Security Integration
• Enterprise User Security
• 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

- acme.com
  - sales.acme.com
    - Oracle Context
      - DB1.sales.acme.com
      - netsvc1.sales.acme.com
  - dev.acme.com
    - Oracle Context
      - DB3.dev.acme.com
      - netsvc2.dev.acme.com

Create Schema
Create Naming Context
Register DB/Net Service Names
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: orcl
OS installed: Windows 7

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

Windows Server 2008 R2 with SP1 (Domain Controller)
DEMONSTRATION

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></td>
</tr>
<tr>
<td>Linux/Unix</td>
<td>Any</td>
<td>No</td>
<td>Yes</td>
<td>AD Integration solutions can help</td>
</tr>
</tbody>
</table>
Program Agenda

• Active Directory for Name Resolution
• Single Sign On
• Web Applications: Security Integration
• Enterprise User Security
• Q&A
Single Sign On

- Windows Native Authentication or OS Authentication (NTS)
- Kerberos
- SSL
  - Microsoft Certificate Store Support
    - set parameter `WALLET_LOCATION` in `sqlnet.ora` to:
    - `WALLET_LOCATION = (SOURCE = (METHOD=MCS))`

*Independent of “Active Directory for Name Resolution” feature*
Windows Native Authentication

- Enabled by default and works across Windows systems
- Windows user logon credentials used for database authentication
- For using Windows users as Database Administrative Users
  - Do not need to create corresponding users in Database
  - Windows tools can be used to manage Windows group membership
- For using Windows users as Database Regular Users
  - Need to create corresponding users in Database
  - Authorization can be granted through Windows group membership or Database roles
  - Use Windows & Database tools or Oracle Administration Assistant
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 SYSASAM 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 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
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.

  (If Oracle Administration Assistant is used, it makes appropriate changes in AD and Database)
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

MS Active Directory/KDC

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
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 Authentication
Windows Client Configuration

- Create Kerberos and sqlnet configuration files using Oracle Net Manager
  - Set sqlnet.kerberos5_cc_name to “OSMSFT:” in sqlnet.ora so that the credential is retrieved from Microsoft Credential Cache
Kerberos Authentication
Server configuration (non-Windows)

- Create Kerberos and sqlnet configuration files on the sever using Oracle Net Manager
- Create an user in Active Directory for Database Server
- On the Domain Controller
  - Create Database Service Principal in AD
  - Map the Principal to AD user
  - Use ktpass utility (available from Microsoft) to create Kerberos "keytab" file
- Copy keytab file to DB server node
- Set `os_authent_prefix` to "" in init.ora
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

Oracle Database

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

Example:
SQL> CREATE USER KRBUSER IDENTIFIED EXTERNALLY AS 'FRANK@SALES';
SQL> Grant connect, resource to KRBUSER;
# Windows Single Sign On Comparison

<table>
<thead>
<tr>
<th>Windows Native Authentication</th>
<th>Kerberos</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Windows only solution</td>
<td>• Supports heterogeneous platforms</td>
</tr>
<tr>
<td>• MS KDC is used implicitly</td>
<td>• MS KDC is supported</td>
</tr>
<tr>
<td>• Uses External Users mechanism in DB</td>
<td>• Can use External Users mechanism in DB (default)</td>
</tr>
<tr>
<td>• Enterprise User Security not supported</td>
<td>• Enterprise User Security supported</td>
</tr>
<tr>
<td>• Direct support of Windows group membership for role authorization</td>
<td>• EUS and AD integration solutions can be used to support role authorization through Windows group membership; provides more power and flexibility</td>
</tr>
<tr>
<td>• All DB Editions – included and configured</td>
<td>• All DB Editions</td>
</tr>
</tbody>
</table>
Program Agenda

• Active Directory for Name Resolution
• Single Sign On
• Web Applications: Security Integration
• Enterprise User Security
• 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

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

Web Applications On Windows (IIS)

Active Directory/KDC

Oracle Identity Management

Oracle Database

ASP.NET Providers

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:"
    - Database can be on any platform
Web Applications on Windows

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

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

- Active Directory for Name Resolution
- Single Sign On
- Web Applications: Security Integration
- Enterprise User Security
- Q&A
Enterprise User Security

- Problem Definition
- Enterprise Directory Overview and benefits
Each Database is an island. Users are managed separately in each database.
The Cost

- **User Productivity**
  - Multiple database login names and passwords to remember
  - No self-service capability for password reset

- **Database Administrator time**
  - DBAs manage the same user many times

- **Audit & Compliance**
  - Each database must be examined individually to find out who has which privileges

- **Security**
  - Hard to ensure user access to all databases is removed
  - Ensuring passwords meet policy requirements is difficult
Solution

Centralized User Management

- Define users in one place
- Assign users’ privileges in one place
- Delegate database user management to the help desk
- Control user’s passwords through a common identity store such as Corporate Directory
Centralized Database Users

Each person has one username/password for ALL databases. Directory identities are *mapped* to database schemas. Directory groups are *mapped* to database roles.
Benefits

Decrease Time Spent Managing Users
Devote more time to value-added activities

Improve Your End-User’s Experience
Give your user’s a single username/password, standardized access request procedures

Reduce the Cost of Compliance
Delete/disable user access in ALL databases with a single click
Managing Enterprise Authentication

- Authentication Stores
  - Oracle Unified Directory
  - Oracle Internet Directory
  - Oracle Directory Server Enterprise Edition
  - Active Directory
  - eDirectory

- Authentication Options
  - Username/Password, Kerberos, Radius, X.509
EUS Account management with Active Directory

1. Connect Steve.smith/Oracle1

2. Request Steve.smith

3. Request Steve.smith

4. Returned Steve.smith

5. Returned Steve.smith

6. Request Schema and Enterprise Roles

7. Returned Schema and Enterprise Roles
EUS Account management with Kerberos and AD

User first must login to AD to get a TGT

(1) Authenticate Steve.smith/Oracle1 Using TGT

Validates TGT, Maps users to schema and roles

(2) Request Steve.smith

Maps tree, Translates Data, Stores EUS configuration

(3) Request Steve.smith

EUS-enabled Oracle DB

(4) Request Steve.smith

Oracle Unified Directory

(5) Returned Steve.smith

(6) Request Schema and Enterprise Roles

Active Directory

(7) Returned Schema and Enterprise Roles
Next Steps

- Contact Your Oracle Account Representative For More Information About Enterprise User Security
Join the Oracle Community

Twitter
twitter.com/OracleIDM

Facebook
facebook.com/OracleIDM

Oracle Blogs
blogs.oracle.com/OracleIDM
blogs.oracle.com/directoryservices

Oracle.com/Identity
For More Information

- **Sessions**
  - Tue 12- 1 PM - What’s New for Oracle and .NET (Marriott Marquis - Salon 7)
  - Wed 11:45 AM - 12:45 PM - Best Practices for Oracle Database Performance On Windows (Moscone South 252)
  - Wed 5-6 PM – Oracle Database 12c on Windows (Moscone South 104)

- **Booth:** Moscone South, Left - SL-043 – Oracle Database 12c on Windows

- [Windows Server System Center](#)
- [Oracle .NET Developer Center](#)
- [Identity Management](#)
Questions & Answers