
ORACLE®

Rdb Authentication and LDAP

Ian Smith
& Martin Ramshaw

Oracle Rdb Engineering
October, 2014

ORACLE

Remote Speaker Photo

Ian Smith

Rdb Product Architect, Oracle

Program Agenda

1. Rdb Authentication
2. Impersonation
3. Authentication Services
4. Introduction to LDAP
5. Resources

Program Agenda

1. Rdb Authentication
2. Impersonation
3. Authentication Services
4. Introduction to LDAP
5. Resources

Program Agenda

1. Rdb Authentication
2. Impersonation
3. Authentication Services
4. Introduction to LDAP
5. Resources

Program Agenda

1. Rdb Authentication
2. Impersonation
3. Authentication Services
4. Introduction to LDAP
5. Resources

Program Agenda

1. Rdb Authentication
2. Impersonation
3. Authentication Services
4. Introduction to LDAP
5. Resources

Program Agenda

1. Rdb Authentication
2. Impersonation
3. Authentication Services
4. Introduction to LDAP
5. Resources

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.

Rdb Authentication

Attach, Connect and Declare Alias

Traditional

- Login through OpenVMS with **username** and **password**
- Rdb uses your process attributes as your credentials
- UIC is very important
  - Stored in object ACL (access control list)
  - Used as ID for **create user**
  - Function result of **current_uid**, **session_uid** and **system_uid**
- Assume 1-to-1 mapping of USERNAME to UIC
  - SHOW PROTECTION and SHOW PRIVILEGES will format the UIC
  - If LEE and JONES share a UIC might login as one but act as the other

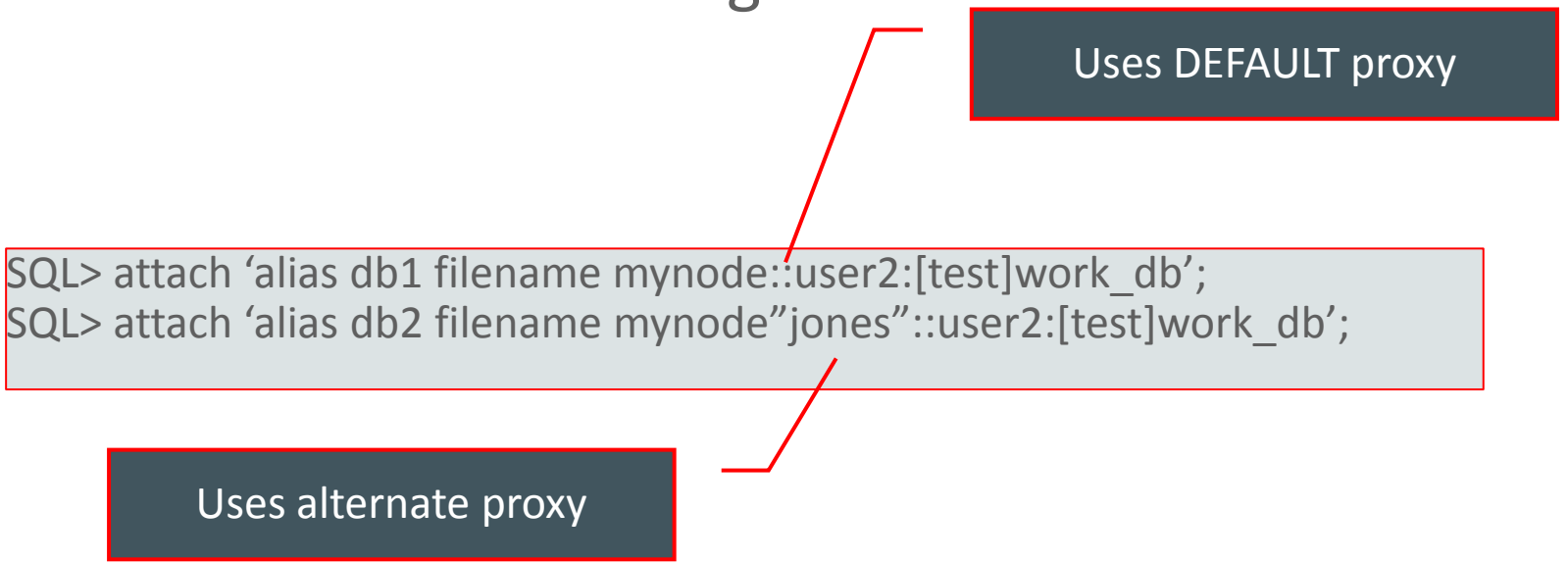
Remote Access - DECnet

- To access a remote database **username** and **password** can be supplied on the file specification
- This is handled by RMS (Record Management Services) as part of the DECnet interface
- Remote process is created with correct credentials and runs the RDBSERVER image

```
SQL> attach ‘filename mynode”smith blake7washere”::user2:[test]work_db’;
```

Remote Access – DECnet using PROXY

- Most applications don’t want to include password in the access string
- OpenVMS DECnet supports a PROXY database
- Use AUTHORIZE to manage



Remote Access – DECnet using PROXY

- Simplifies access
- Rdb doesn't need your username or password
- DECnet handles the creation of a remote process with the credentials granted by the proxy definition

```
UAF> add/proxy SAMPLE::WALTER ROBIN/default
%UAF-I-NAFADDMSG, record successfully added to NETPROXY.DAT
```

Access from node SAMPLE by user WALTER can use the credentials of ROBIN on this node

Example

- **Walter** logs on to VMS
- Then uses SQL to attach to the database
  - SQL> attach ‘file SAMPLE::disk1:[db]acct.rdb’;
- The remote user will be **Robin**
- SYSTEM_USER, SESSION_USER and *probably* CURRENT_USER will reflect this state
  - Probably… can be changed by executing procedure

Simple Mapping

- Many systems use a simplified mapping for PROXY
- Allow same user to access any node
- UAF> add/proxy *::LEE LEE/default
- All nodes allowed but maps the username

Remote Access – TCP/IP

- Username/Password in the file specification is only used by DECnet
- For TCP/IP Rdb must perform the impersonation
  - Statements include keywords: USER and USING
- Accepted on various statements
  - Create, Alter, Drop, Import Database
  - Attach, Connect and Declare Alias
  - Set Session Authorization
- **attach** and **connect** are dynamic statements, so expect the password to be passed at runtime

Remote Access – TCP/IP

- Remote process (service) is run under RDB$REMOTExx user
- New user is impersonated by Rdb

Example

```
declare :usr,:pwd char(20);
accept :usr prompt 'Username: ';
accept :pwd prompt 'Password: ' hide;

attach 'alias db1 filename db$:personnel';

connect
   to 'alias db1 filename db$:personnel'
   as 'myatt'
   user :usr
   using :pwd;

show connection *;

disconnect all;
```

:usr and :pwd are parameters

Remote Access – TCP/IP

- Can also provide values for **user** and **using** in a configuration file
  - RDB$CLIENT_DEFAULTS.DAT
  - Opened via the logical name RDB$USER_DEFAULTS
  - Or, if found in SYS$LOGIN
- SQL_USERNAME and SQL_PASSWORD options
- Expect the .DAT file to be secured
- (Aside: Recommend defining SQL_NETWORK_TRANSPORT_TYPE as TCPIP if not using DECnet)

Remote Access – TCP/IP, with PROXY?

- To recap:
  - DECnet accepts the access string and creates the remote process
  - Or, DECnet contacts remote system and determines that a PROXY is defined and uses it
- Rdb has nothing to do with remote security
- TCP/IP doesn't have identical support

Remote Access – TCP/IP

- TCP/IP on OpenVMS has a PROXY database
- However, Rdb would have to get username to the remote system securely, and interface to that PROXY database
- Not done today
  - OpenVMS doesn't provide a public interface to the PROXY database
- Talking with HP and VMS to see if this can be done in a supported way… stay tuned

Impersonation

Persona

Servers perform user Impersonation

- SQL/Services
- OCI Services for Rdb
- ODBC
- JDBC
- ORDT (.NET)
- Use server architecture to share attaches between multiple users

User and Using

- Not restricted to remote access
- Servers use CONNECT to share attaches
- Or can use SET SESSION AUTHORIZATION
- Note:
  - SYSTEM_USER will be the server user
  - SESSION_USER will be the impersonated user
  - CURRENT_USER will match SESSION_USER unless overridden by procedure call

Persona is Enabled

- Database attribute controls the type of impersonation
  - Security checking is … (persona is enabled)
- For V7.3 **create database** or **import database** set this implicitly
- Databases from older versions stick with UIC (non-persona) impersonation
- Persona impersonation means that the full rights identifier credentials are used as well as the UIC

Persona

- OpenVMS provides a set of Impersonation system services
- Rdb uses a small subset
  - sys$persona_create
  - sys$persona_assume
  - sys$persona_delete

Authentication Services

RDB$COSIP.EXE Image

Authentication Services

- Used by SQL/Services
- Rdb Remote access
- Set Session Authorization

Authentication Services

- Privileged image supplied with Oracle Rdb
- Calls system services such as SYS$GETJPIW, SYS$GETUAI, SYS$SCAN_INTRUSION, etc.
  - Enforced password check
  - Hourly and daily limits
  - Disabled users
  - Expired passwords
  - Reported access to VMS intrusion system
  - And so on

Changes in Rdb V7.3

- V7.3 replaced most of Oracle Rdb code with a call to **sys$acmw** system service
- ACM - Authentication and Credential Management
- Rdb no longer needs to maintain our authentication code
- Rdb automatically inherits any OpenVMS security upgrades and features

Advantages

- Allows interface to extra services such as the ACME LDAP Agent
- Setting UAF flag causes OpenVMS as well as Rdb to use LDAP to perform authentication
- Note that RDB$COSIP is not versioned; once V7.3 has been installed (multi-version mode) then V7.2 users can also use LDAP

Introduction to LDAP

Lightweight Directory Access Protocol

What is it?

- LDAP - Lightweight Directory Access Protocol
  - open,
  - vendor-neutral,
  - industry standard protocol
  - for accessing and maintaining distributed directory information services
- Commonly used to provide “single-signon” password
- Stored in a central repository
  - Oracle Internet Directory, Microsoft Active Directory, HP-UX LDAP-UX Integration Software, OpenLDAP, etc.

Usage

- When LDAP is setup you can enable specific users to be externally validated
- This means login to VMS, Rdb authentication, and so on all obey this mapping

Setup

Brief and incomplete

Setup

- Must install optional OpenVMS software
  - See documentation referenced later
  - Details beyond the scope of this talk
- Must configure VMS to use your existing LDAP server
  - Will examine briefly
- Or install and configure one of those listed previously
- Configure the user accounts in the UAF (AUTHORIZE)

Setup the ACME/LDAP agent on the OpenVMS nodes

- SYS$STARTUP:LDAPACME$CONFIG-STD.INI
- This LDAP configuration file is required
- It defines where the LDAP server resides and how to connect to it

SYS$STARTUP:LDAPACME$CONFIG-STD.INI

- It should have, as a bare minimum, the following items
  - server = ldapsys01.mycompany.com
  - port = 389
  - bind_dn =
  - bind_password =
  - base_dn =
  - login_attribute = samaccountname
  - scope = sub
  - port_security = none
- See also SYS$STARTUP:LDAPACME$CONFIG-STD.INI_TEMPLATE

SYS$MANAGER:ACME$START.COM

- The startup procedure comes with lines commented out
- Make sure they are active

```
$! The LDAPACME$INIT logical MUST contain the path name to the initialization
$! for the LDAP ACME Agent Server
$ DEFINE/SYSTEM/EXECUTIVE LDAPACME$INIT SYS$STARTUP:LDAPACME$CONFIG-STD.INI
$ @SYS$STARTUP:LDAPACME$STARTUP-STD                    ! LDAP_STD
```

Mapping LDAP users to OpenVMS users

- To activate LDAP to OpenVMS mapping a local mapping file must be created
- SYS$STARTUP:LDAPACME$CONFIG-STD.INI
- Towards the end of the supplied sample uncomment these lines

```
mapping = local
mapping_file=SYS$STARTUP:LDAP_LOCALUSER_DATABASE.TXT
```

Mapping LDAP users to OpenVMS users

- Each line is an ldapname,uafname pair
- The ldapname is not case sensitive on the LDAP server

```
“jenny.p.jones”,”J_JONES”
“marvin.t.robot”,”MTR”
“james.t.kirk”,”CAPTAIN”
```

Start the ACME/LDAP agent

- The ACME server must be started
  - $ SET SERVER ACME/RESTART
- or:
  - $ SET SERVER ACME/EXIT/WAIT
  - $ SET SERVER ACME/LOG/START=AUTO

Enable your users

- Use AUTHORIZE to set some user flags

```
UAF> modify j_jones/flags=(extauth,pwdmix)
%UAF-I-EXTAUTH, ExtAuth set for J_JONES; field modification may have no effect
%UAF-I-MDFYMSG, user record(s) updated
```

Some flags don't make sense

User flags in SYSUAF file (from HELP)

- EXTAUTH
- Considers user to be authenticated by an external user name and password, not by the SYSUAF user name and password
- The system still uses the SYSUAF record to check a users login restrictions and quotas and to create the users process profile

User flags in SYSUAF file (from HELP)

- DISPWDSYNCH
- Suppresses synchronization of the external password for this account. See bit 9 in the SECURITY_POLICY system parameter for system wide password synchronization control

User flags in SYSUAF file (from HELP)

- PWDMIX
- Enables case-sensitive and extended-character password. After PWDMIX is specified, you can then use mixed-case and extended characters in passwords

Example

- Use LDAP to login to OpenVMS

```
Username: jenny.p.jones
Password:
TRIBLE - Property of Oracle Corporation
   Last interactive login on Tuesday, 23-SEP-2014 01:19:29.87
**** Logon authenticated by LDAP ****
$ @sys$share:rdb$setver 73
Current PROCESS Oracle Rdb environment is version V7.3-111 (MULTIVERSION)
Current PROCESS SQL environment is version V7.3-111 (MULTIVERSION)
Current PROCESS Rdb/Dispatch environment is version X7.3-01 (MULTIVERSION)
$ sql$
SQL> attach 'filename abc';
SQL> select system_user from rdb$database;

 J_JONES
1 row selected
```

Example

- Trying remote access…

```
$ sql$
SQL> attach 'f 0"jenny.p.jones …"::COSI_USER1:[JJONES]abc';
SQL> show version
Current version of SQL is: Oracle Rdb SQL V7.3-111
Underlying versions are:
   Database with filename 0"jenny.p.jones password"::COSI_USER1:[JJONES]abc
            Oracle Rdb V7.3-111
            Rdb/Dispatch V7.3-01 (OpenVMS Alpha)
            Remote Server V7.3-111 (OpenVMS Alpha)
            Remote Client V7.3-01 (OpenVMS Alpha)
            Rdb/Dispatch V7.3-01 (OpenVMS Alpha)
SQL> select system_user, session_user, current_user from rdb$database;

 J_JONES                J_JONES                J_JONES
1 row selected
```

Resources

HP and Other Sources

Just skimming the surface

- Did you attend the OpenVMS Bootcamp?
- ACME/LDAP setup and troubleshooting
  Speaker: Dan Buckley, HP

HP Documentation

- **Security Features in OpenVMS Version 8.4**
  - http://h71000.www7.hp.com/openvms/security.html#acme_ldap_changes
- HP OpenVMS ACME LDAP Installation and Configuration Guide
  - SYS$HELP:ACMELDAP_STD_CONFIG_INSTALL.PDF
- HP OpenVMS Guide to System Security
  - http://h71000.www7.hp.com/doc/84FINAL/ba554_90015/ba554_90015.pdf

More Documentation

- HP OpenVMS – External Authentication using ACMELDAP
  - http://www.openvms.org/stories.php?story=12/12/14/4832565
- ACME Developers Readme
  - SYS$HELP:ACME_DEV_README.TXT
- Some useful notes from Hoffman Labs
  - http://labs.hoffmanlabs.com/index.php?q=node/619

More…

OCI

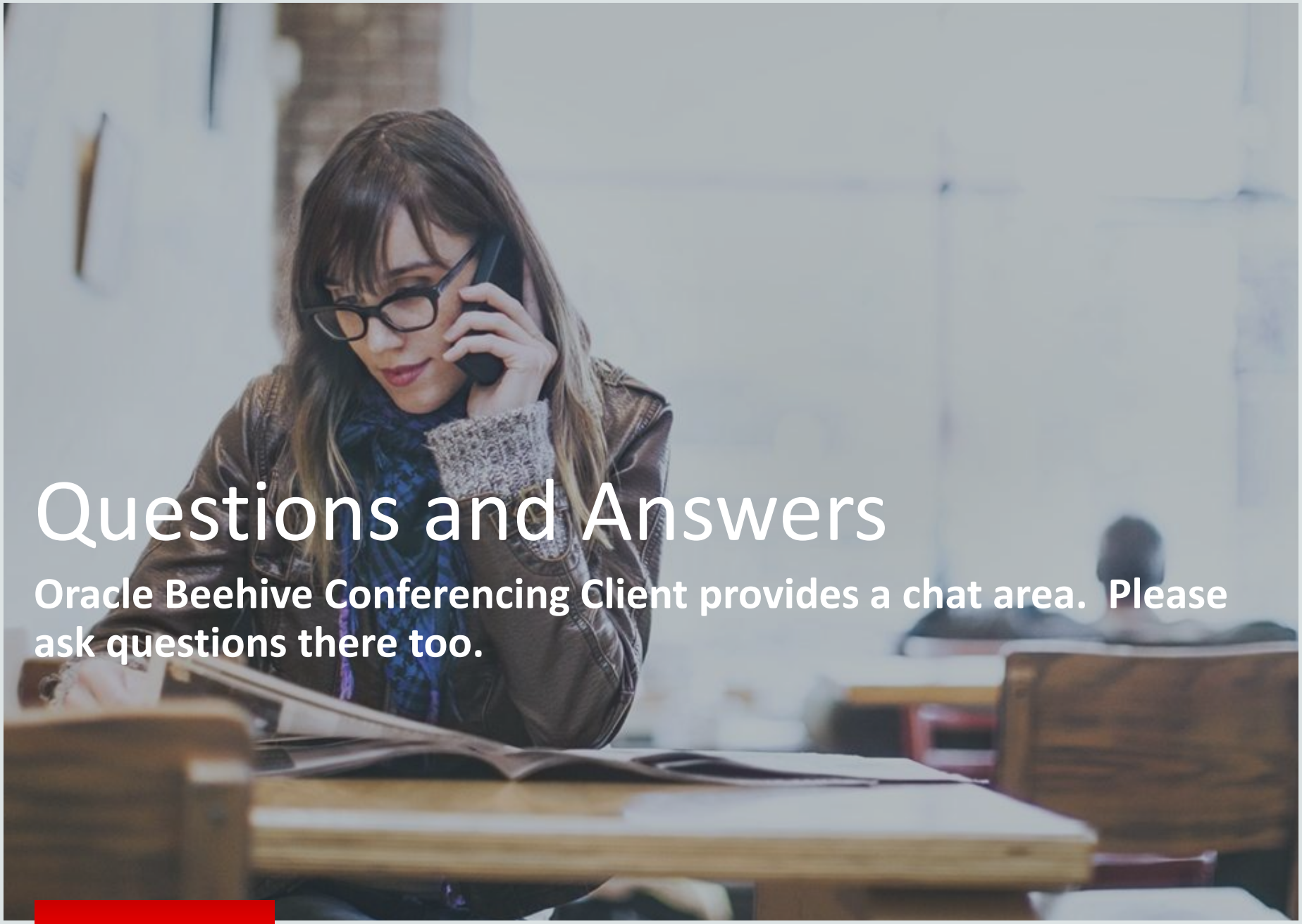
- What about OCI Services for Rdb?
  - Currently users are defined in the USER$ table
  - We store an encoded password (different encoding to that used by OpenVMS and LDAP servers)
  - This password is used to authenticate with the Oracle server
- Looking at a project to use the LDAP environment but must be able to fetch this special encoded password
- Use LDAPACME$INIT logical so OCI shares the same LDAP server

Is this ready for production use?

- ACMELDAP support has been around for several years on OpenVMS (8.3 originally)
- Original implementation using SYS$ACMW in RDB$COSIP was in V7.3.1
- Used in-house for a few years
  - 7.3.1.2 allows longer LDAP user names
  - 7.3.1.x will further improve the interface
- Plan to document the support for our next kit
- Talk to us

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.



Questions and Answers

Oracle Beehive Conferencing Client provides a chat area. Please ask questions there too.

Hardware and Software
Engineered to Work Together


ORACLE®