

Dimitri Gielis

Real Application Security (RAS) in APEX



www.apexRnD.be



dgielis.blogspot.com



@dgielis



dgielis@apexRnD.be

Dimitri Gielis

- ❖ Founder & CEO of APEX R&D
- ❖ 18+ years of Oracle Experience (OCP & APEX Certified)
- ❖ Oracle ACE Director
- ❖ “APEX Developer of the year 2009” by Oracle Magazine
- ❖ “Oracle Developer Choice award (ORDS)” in 2015
- ❖ Author Expert Oracle Application Express
- ❖ Presenter at Oracle Conferences (OOW, ODTUG, OGh, UKOUG, ...)





<https://www.apexofficeprint.com>

http://dgielis.blogspot.com

@dgielis

Dimitri Gielis Blog (Oracle Application Express - APEX)
I created this Blog to share my knowledge especially in Oracle Application Express (APEX) and my feelings ...

FRIDAY, SEPTEMBER 26, 2014

APEX 4.2.6 patch available

Oracle released [APEX 4.2.6](#) yesterday, it's also available from My Oracle Support as a patch set 19595896.

Here's the table of bug fixes.

Table 6 Bugs Fixed in the Oracle Application Express 4.2.6.00.03 Patch Set

Bug Number	Description
18393429	Importing pre-4.2 application with data loading results in runtime error
18609856	APEX_WEB_SERVICE.CLOBBASE642BLOB converts incorrectly
18658967	Corrupted HTML mail messages are created from APEX_MAIL.SEND
18719750	ORA-01858 during application import
18733989	Errors picking up session with cookie when TOP CALL is not F, SHOW, or ACCEPT
19021052	Oracle Application Express 4.2.4 throwing error while generating check boxes
19313700	Check box fails with ORA-06502 after upgrade from release 4.0 to 4.2.4
19482775	ORA-06502 when importing application containing translations

Applying the patch took less than 7 minutes.

```
Session altered.
...Validating Application Express
...Database user "SYS", database schema "APEX_040200", user# "106" 20:48:40
...Compiled 0 out of 3014 objects considered, 0 failed compilation 20:48:40
...271 packages
...263 package bodies
...452 tables
...11 functions
...16 procedures
...3 sequences
...457 triggers
...1320 indexes
...211 views
...0 libraries
...6 types
...0 type bodies
...0 operators
...0 index types
```

My next public appearances:

- [Oracle Open World: 27-SEP/2-OCT-2014](#)
- [ORCLAPEX-BE Meetup: 19-NOV-2014](#)
- [ODTUG KScope: 21/25-JUN-2015](#)

About Me

[Dimitri Gielis](#)

Passionate about Oracle and especially Oracle Application Express (APEX). Building applications with love @ APEX R&D.

[View my complete profile](#)

 **ORACLE**
ACE Director

Need APEX consulting, training, development, then visit:



Twitter

 Follow @dgielis

A blue cartoon bird, resembling a Twitter logo, standing on a reflective surface. The bird is facing right, with its beak open as if chirping. It has yellow feet and a yellow beak. The background is a light blue gradient.

Agenda

- ❖ Security in an APEX app
- ❖ Introduction to Real Application Security (RAS)
- ❖ Using RAS in Oracle Application Express (APEX)
- ❖ Live demo implementing RAS in APEX app

A blue 3D padlock is centered in the image, set against a dark blue background filled with glowing binary code (0s and 1s). The padlock is open, with its shackle raised. The text "Security in APEX" is overlaid in white, centered horizontally and partially covering the padlock.

Security in APEX

Oracle APEX Security

- ❖ Authentication schemes
 - ❖ Can I go in? - Users
 - ❖ SSO, Custom table, APEX, DB...
- ❖ Authorization schemes
 - ❖ What can I do? - Roles
 - ❖ Defined on APEX components (page, item, navigation, ...)

Security



Security Attributes

Authentication Schemes

Authorization Schemes

Session State Protection

Build Options

Access Control

- ❖ Easy wizard
- ❖ Creation of Authorization schemes & Admin screen
 - ❖ Assign roles to users
- ❖ Targeted for UI, not for Data



Access Control

Access Control wizard

Application	325
Page	2
Page Name	Access Control Administration Page
Page Title	Access Control Administration Page
Create Table	APEX_ACCESS_SETUP
Create Table	APEX_ACCESS_CONTROL
Create Authorization Scheme	access control - administrator
Create Authorization Scheme	access control - edit
Create Authorization Scheme	access control - view

Access Control admin screen

Application Administration

Application Mode

☒ **Full access to all, access control list not used.**

☐ Restricted access. Only users defined in the access control list are allowed.

☐ Public read only. Edit and administrative privileges controlled by access control list.

☐ Administrative access only.

?

Set Application Mode

Access Control List

Identify usernames which correspond to this application's authentication scheme.

Find

?

Go

☐	Username	Privilege	Last Changed By	Date
☐	DGIELIS	Edit	dimi	Now

1 - 1

Add User

Delete

Apply Changes

Challenges on Data Access Control

What about
data?



Challenges on Data Access Control

- ❖ Code executed under privileged user
- ❖ Database unaware of end users
- ❖ Data access policy (data security) is hard coded in
 - ❖ Where-clause - application level
 - ❖ Views - database level
 - ❖ Virtual Private Database (VPD) - database level



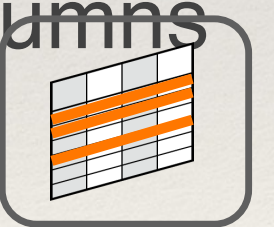
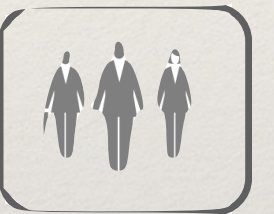
Real Application Security (RAS)

Real Application Security (RAS)

A database authorisation solution for end-to-end
application security

RAS Key features

- ❖ Support Application Users and Sessions
 - ❖ Schema-less user, security and application context in DB
- ❖ Support Application Privileges and Roles
- ❖ Support fine-grained data access control on rows and columns
 - ❖ Based on user operation execution context
 - ❖ Enforce security close to data

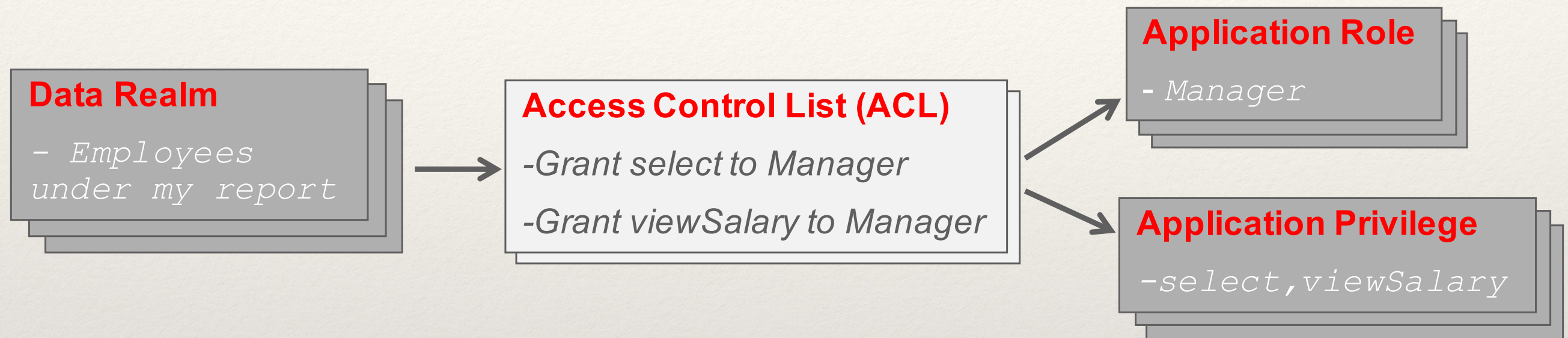


Example Application Security

- ❖ All employees can view public information
- ❖ An employee can view own record, update contact information
- ❖ Manager can view salary of his/her reports

Name	Manager	SSN	Salary	Phone Number
Adam	Steven			515.123.4567
Neena	Steven			515.123.4568
Nancy	Neena	108-51-4569	12030	650.111.3300
Luis	Nancy		6900	515.124.4567
John	Nancy		8200	515.124.4269
Daniel	Nancy		9000	515.124.4469

RAS Concepts: Policy components



- ❖ Data Security policy is a collection of Data Realms and ACLs
- ❖ Each Data Realm has an associated ACL with grants

RAS: setup with PL/SQL API

```
xs_principal.create_role(name => 'emp_role', enabled => true);
```

```
xs_security_class.create_security_class(  
    name          => 'hr.hrprivs',  
    parent_list   => xs$name_list('sys.dml'),  
    priv_list     => xs$privilege_list(xs$privilege('view_salary')));
```

RAS Administration Tool

Home Policies Privileges Namespaces Users Roles Settings

Home > Policies > Policy Definition

Policy Cancel Delete Apply Changes

Policy Name * HRM.EMPLOYEE_POLICY

Description

Protected Objects +

Data Realm Authorization Delete Add

	Realm Description	SQL Predicate	ACL	Reorder
☐	ALL RECORDS	1=1	HRM.ALL_EMP_ACL	△ ▽
☐	MY RECORD	EMPLOYEE_ID IN (SELECT EMPLOYEE_ID FROM HRM.USER_PROFILE WHERE LOGON_NAME = XS_SYS_CONTEXT('XS\$SESSION','USERNAME'))	HRM.MY_EMP_ACL	△ ▽
☐	MY REPORTS	EMPLOYEE_ID IN (SELECT EMPLOYEE_ID FROM (SELECT EMPLOYEE_ID, level l FROM HRM.MANAGERS M START WITH M.EMPLOYEE_ID IN (SELECT ...	HRM.MY_REPORT_ACL	△ ▽

1 - 3

Column Authorization Delete Add

	Column	Privilege	Description
☐	SALARY	VIEW_SALARY	To view Salary column
☐	SSN	VIEW_SSN	To view SSN column

1 - 2

Employees
Table

1. All records
2. My record
3. My reports

Restricted
Salary & SSN
Columns

Privilege
Grants

Note: the RASADM (RAS Administration Tool) is written in APEX :)

RAS Administration Tool: ACLs

Grants on all records

Principal	All Except	Privilege	Start Date	End Date	Reorder
EMPLOYEE	NO	SELECT	-	-	△ ▽
HRREP	NO	VIEW_SSN	-	-	△ ▽

Grants on my record

Principal	All Except	Privilege	Start Date	End Date	Reorder
EMPLOYEE	NO	UPDATE	-	-	△ ▽
EMPLOYEE	NO	VIEW_SSN	-	-	△ ▽
EMPLOYEE	NO	VIEW_SALARY	-	-	△ ▽

Grants on my reports

Principal	All Except	Privilege	Start Date	End Date	Reorder
MANAGER	NO	VIEW_SALARY	-	-	△ ▽

RAS Administration Tool: Application Roles

Employees can view and update their own records

HR Representatives can view SSN

Managers can view salaries of their reports

ORACLE® RAS Administration					
Home	Policies	Privileges	Namespaces	Users	Roles
Home > Roles					
Q Go Reports 1. Primary Report ▼					
Role Type in 'REGULAR, DYNAMIC' ☒ ☐					
Role	Description	Privilege	Object	Data Realm	Role Type
EMPLOYEE	Regular employees	SELECT	HRM.EMPLOYEES	ALL_RECORDS	REGULAR
EMPLOYEE	Regular employees	UPDATE	HRM.EMPLOYEES	MY_RECORD	REGULAR
EMPLOYEE	Regular employees	VIEW_SALARY	HRM.EMPLOYEES	MY_RECORD	REGULAR
EMPLOYEE	Regular employees	VIEW_SSN	HRM.EMPLOYEES	MY_RECORD	REGULAR
HRREP	HR representatives	VIEW_SSN	HRM.EMPLOYEES	ALL_RECORDS	REGULAR
MANAGER	Managers	VIEW_SALARY	HRM.EMPLOYEES	MY_REPORTS	REGULAR

Real Application Security Features

Controlled Delegation

- VP delegating calendar management function to an Assistant

Effective-date support

- Contractor getting access for a specific duration

Negative grants

- Access to certain reports allowed only on intranet

Code-based security

- Batch programs with elevated privileges to summarize data

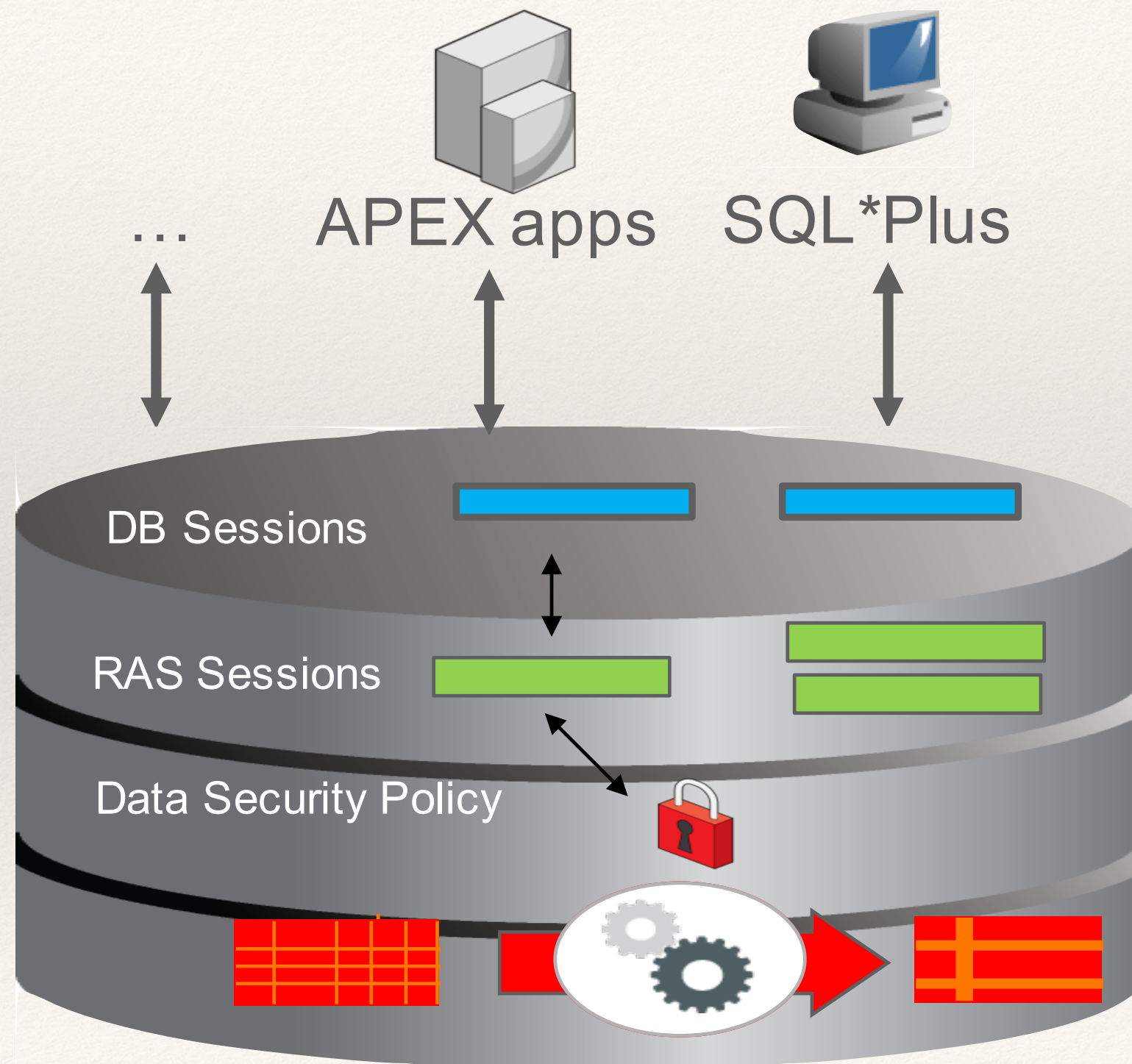
Function Security

- Conditional rendering of User Interface

Auditing

- Application users, privileges, roles are known to database

Real Application Security Architecture

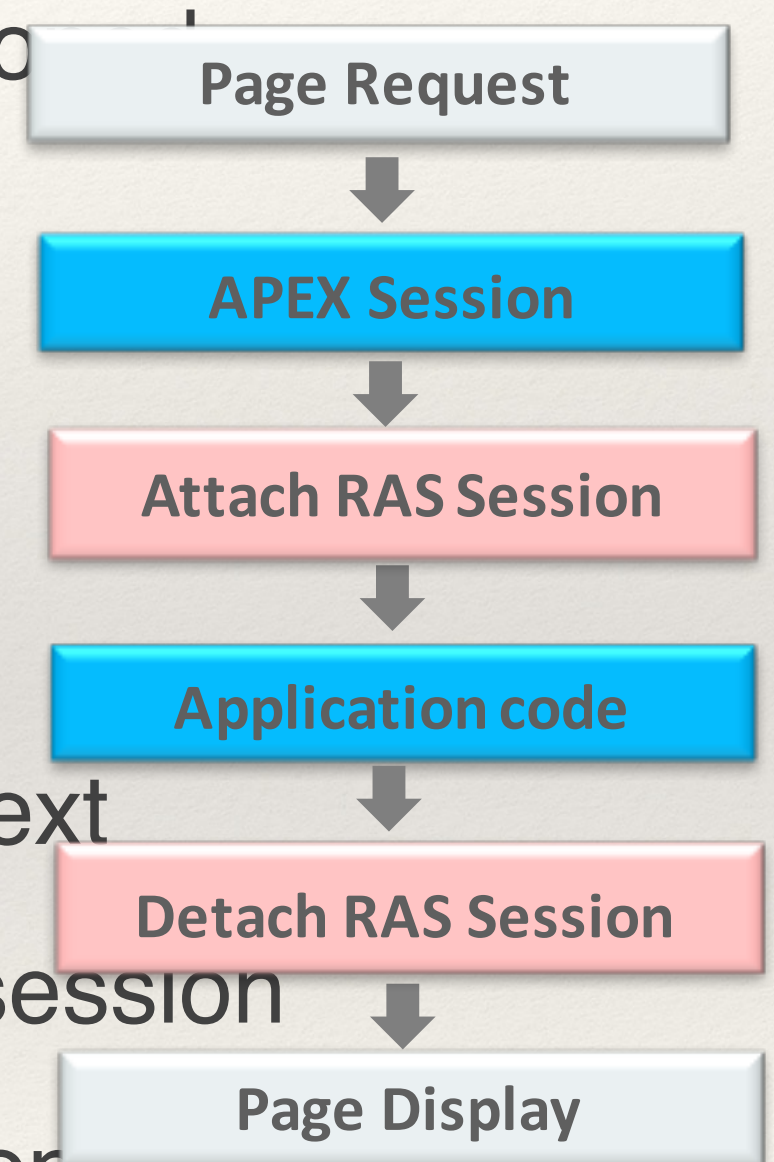


RAS in APEX



RAS Integration with APEX

- ❖ Application users continue to be provisioned in the database or identity stores
- ❖ User authentication remains in APEX
- ❖ RAS session contains application user, its roles, and session context
- ❖ Based on APEX user's security context
- ❖ Application code executes within RAS session
- ❖ Attached and detached to a db session



RAS Integration with APEX 5

- ❖ APEX can use RAS users, roles, and data security policy
 - ❖ Instead of custom authorization using VPD
- ❖ RAS Session is transparently created based on APEX session
- ❖ For APEX authorization schemes, use RAS ACL check operators

Authentication Scheme

Cookie Path

Cookie Domain

Show All

Name	Subscription	Source	Source
------	--------------	--------	--------

Real Application Security

RAS Mode

Authorization Scheme

* Scheme Type

* PL/SQL Function Body

```
declare
result pls_integer;
begin
select ORA_CHECK_ACL(:UPD_CHECK_ACLIDS, 'UPDATE') into re
if result = 1 then
return true;
```

Demo RAS in APEX

RAS Benefits

- ❖ Stronger security
 - ❖ Enforced regardless of entry points: direct, APEX, or middleware
 - ❖ Audit end-user activity in database audit trail
- ❖ Simpler development
 - ❖ Declarative policy, relieves writing authorization code
 - ❖ Native support for application roles, application privileges, application users
- ❖ High Performance Access Control
 - ❖ Optimized for typical data access patterns within core database
- ❖ Simpler administration
 - ❖ Centralized management, end-to-end uniform security across mid-tier and database

RAS - to know...

- ❖ One RAS repository for the whole database
- ❖ Takes a bit of time to get used to the implementation and naming
- ❖ RASADM can help, but ...
 - ❖ RASADM doesn't expose all features
 - ❖ RASADM app didn't always behave as expected (had to patch it to get some things working)
- ❖ Once you enable RAS make sure to test your app (!)
APEX Advisor can't check for the correct grants (yet).

References

- ❖ Oracle RAS Developer Guide

docs.oracle.com/database/121

- ❖ Oracle RAS Papers

www.oracle.com/technetwork/database/security/real-application-security

- ❖ Presentation by Vikram Pesati

- ❖ Presentation by Joel Kallman & Tanvir Ahmed

www.slideserve.com/odele/oracle-database-12c-real-application-security-for-oracle-application-express

Q&A

APEX RD
research & development



www.apexRnD.be



dgielis.blogspot.com



@dgielis



dgielis@apexRnD.be

Consulting, Development, Training

- ❖ Looking for consulting, training and development in Oracle Application Express (APEX)?
- ❖ Contact : www.apexRnD.be
- ❖ Mail : info@apexRnD.be