Fine-Grained Access Control in Banner 7

Presenters:

Shelly Wingfield  SkyBridge Global
Amanda Marshall  Board of Regents
Agenda

Introduction
Glossary

Fine-Grained Access Control (FGAC)
Related terms and concepts

FGAC in Banner 7

Value-Based Security (VBS)
Personally Identifiable Information (PII)
Glossary

- **Fine-Grained Access Control (FGAC)**
  - An ORACLE feature new in release 8i
  - Used to provide row-level security (RLS)
  - Once security policies and functions are created and applied, the database server automatically enforces these security policies, no matter how the data is accessed
  - VBS and PII are applications of the FGAC feature
  - PII and VBS do not require each other; you can implement together or separately
  - SCT Banner’s FGAC features require a minimum release of General 7.0 and are designed to function with Oracle 9.2i
Glossary

**Domain**

- A functional area or functional set of information in Banner such as Course Catalog, Schedule, Admissions, Test Scores, etc.
- There are two types – one for VBS and one for PII

**Domain Driver**

- The table that is designated as the driver for the business logic associated with a VBS or PII domain.
- Usually the parent table of a module
Glossary

- **Predicate**
  - SQL clause for a domain and group that defines the access restriction

- **Policy**
  - Oracle object on a table that makes FGAC work
  - Must create policy before PII and VBS will work
  - Policy created by process the DBA runs after users define domain and its tables
  - One policy per table in the GOKFGAC FGAC schema
Glossary

- **Business Profile**
  - Group of users that have the same access restrictions
  - Reduces data entry of access restrictions
  - Different than BANSECR roles. Maintenance of Business Profiles is distributed and moved out of BANSECR schema.

- **CRUD**
  - An acronym for the four types of operations that can be performed on data: *Create, Retrieve, Update*, and *Delete* functions.
1. User inserts into saradap

Insert into saradap
(saradap_pidm, .....)
Values (1234, .....)

3. FGAC Appends Predicate to SQL statement

(new)saradap_coll_code = ‘AS’
and (new)saradap_resd_code = ‘M’

2. FGAC executes GOKFGAC predicate function and retrieves predicate

4. Row inserted or oracle error message displayed
Value-Based Security (VBS)

- Coded and applied as needed to individual users
- Uses the FGAC feature to apply business rules defined by your institution
- For Example, you can apply VBS rules to users in one department so that they can only see student records relevant to that department
These steps make up the VBS creation process.

- Perform analysis on where the VBS restriction should reside.
- Define the domain, which is the driver table for the VBS restrictions.
- Define all tables that are members of the domain and will be restricted by the VBS rule.
- Have the DBA create ORACLE policies on tables.
- Identify the users who need to be restricted by the VBS rule.
- Create the business profile and add restricted users to the business profile.
- Create the VBS rule for the domain
- Assign the business profile.
Define New Domain

- GTVFDMN - Domain Code Validation
- Preface each domain with the product abbreviation G(eneral), S(tudent), etc...and B(anner), followed by the entity name and VBS. Example: SB_CONTACT_VBS
**Assign Driver Table**

- **GORFDMN - Domain Driver Rules; assigns driver table to Domain**
Define Tables and Joins in Domain

- **GORFDPL - VBS Table Rules Form**
- **Assign other tables and joins to Domain**
Create Policy in Oracle

- Run: @gen$exe:gfvbsaddpol and/or gfgacdroppol as BANINST1

- Create policy on all tables defined in domain.
  - Will accept wildcards in the table name

- To view policy data from SQLPlus
  - select * from dba_policies where object_name = 'driver_table';
These steps make up the VBS creation process.

- Perform analysis on where the VBS restriction should reside.
- Define the domain, which is the driver table for the VBS restrictions.
- Define all tables that are members of the domain and will be restricted by the VBS rule.
- Have the DBA create ORACLE policies on tables.
- Identify the users who need to be restricted by the VBS rule.
- Create the business profile and add restricted users to the business profile.
- Create the VBS rules for the domain
- Assign the business profile.
Create New Group Code

- **GTVFGAC - Group Code Validation**: establish a new group code (Recommend ending group code with _GRP)

![Table and Diagram]

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Activity Date</th>
<th>User ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEOGRAPHIC DIVISION</td>
<td>Restrict access based on Geographic Division</td>
<td>12 SEP 2004</td>
<td>BANNER_GUEST</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14 SEP 2004</td>
<td>BANNER_GUEST</td>
</tr>
</tbody>
</table>
Create Business Profiles and Assign Users

- GTVFBPR - Business Profile Validation: create business profile based on line of business or functions (Recommend ending profile code with _PRF)
- GOAFBPR - Business Profile Assignments Form: assign users to profiles created
Create Rule for Each Group

Group: GEOGRAPHIC_DIVISION
Restrict access based on Geographic Division

Active
Effective date: 12-SEP-2004

Domain: GB_GEO_VBS
Restrict Access by Geographic Division

Predicate:

gorpged_good_code = 'UNDERGRAD'

Table: GORPGED
Column: 
Operator: 
Edit: 

Copy Domain
Validate SQL
Define Access to Predicate

Group Attributes/Predicate

Business Profile Access to Predicate

Profile | Description |
--- | --- |
GRADUATE_OFFICE | Graduate Office Users |

User Access to Predicate

User | Select | Insert | Update | Delete |
--- | --- | --- | --- | --- |
SYSTEST01 | | | | |
Be Aware

- **Must exit and reenter Banner after saving to enable new VBS**
- **Can not modify policies.**
  - Must delete (run gfgacdroppol.sql) and recreate (run gfvbsaddpol)
- **Oracle Error 28113 refers to VBS predicate syntax error**
- **User GOIFGAC and GOVFGAC (view) to report on VBS structure**
- **Functions in predicate clauses can slow performance, especially if predicate is against a big table**
Be Aware

- **Parameter _DYN_RLS_POLICIES must be set to TRUE in init.ora if using VBS FGAC in Banner**
- **FGAC is turned off for all Banner jobs/processes excluding GLBDATA.**
  - Use `Gokfgac.p_turn_fgac_off` and `Gokfgac.p_turn_fgac_on` to turn off and back on FGAC on custom jobs/processes
  - Any object can be made exempt by inserting it on the FGAC Excluded Objects Form (GORFEOB)
**Personally Identifiable Information (PII)**

- Philosophy of PII: User can access PII for records in their processing area (you can only view PII for Student Applicants if you work in Admissions)

- PII is implemented system-wide. All users of the system are restricted by PII except when specifically exempted.

- PII restrictions are PIDM based and only on one or two tables in the database. The purpose of PII is to restrict access to records based on the existence of data in key locations.
Define PII domain User assignments

- PII Domains define where the PIDM must exist for the User to have access.
- Use Business Profiles to minimize data entry

Assigning PII domains has to be done for all users of the system

Exempt system type users, and those used for student self service

Work with DBA to create Oracle policy
These steps make up the VBS creation process.

- Define & enable PII domains
- Define PII tables
- Have DBA Create policy on PII table and turn PII on
- Define Business Profiles and PII assignments
- Set up individual user’s exempt, cross domain search status. Repeat until all users of the system are entered.
- Check the active indicator on the entry in GORFDPI to activate PII.
Define PII Domain

- GTVFDMN – PII Domain Code Validation
- Preface each domain with the product abbreviation G(eneral), S(tudent), etc...and B(anner), followed by the entity name and PII. Example: SB_OUTCOME_PII
Enable PII Domain

- Enable PII Domain in GORFDMN
Define Tables in the PII Domain

- Enter the PII tables in GORFDPI
  - PII function delivered: GOKFGAC.F_FIND_PII_DOMAIN.
Create Policies

- Execute the BANINST1 db trigger GOTVBSI0.SQL to turn PII on
- Run: @gen$exe:gfvbsaddpol and/or gfgacdroppol as BANINST1
These steps make up the VBS creation process.

- Define & enable PII domains
- Define PII tables
- Have DBA Create policy on PII table and turn PII on
- Define Business Profiles and PII assignments
- Set up individual user’s exempt, cross domain search status. Repeat until all users of the system are entered.
- Check the active indicator on the entry in GORFDPI to activate PII.
Assigning PII domains

- GOAFPUD – Assign PII domain to users individually
Business Profiles for PII

- GTVFBR, GOAFBPR – Define PII Business Profiles
Assigning PII domains

- GOAFPUD – Assign PII domain to users by Business Profile
Turning GOKFGAC FGAC off for processes

- New page to identify objects that are excluded from GOKFGAC FGAC processing
  - Prevent data corruption
- All JOBS defined in GUBOBJJS are delivered as ‘exempt’.
- Exemptions includes PII and VBS
- Option not available on the Self Service yet
Turning GOKFGAC FGAC off for processes

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
<th>Activity Date</th>
<th>User ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>AADACKS</td>
<td>Dues Acknowledgement Rules</td>
<td>27-FEB-2004</td>
<td>WGALE</td>
</tr>
<tr>
<td>AAPACKN</td>
<td>Membership Acknow Process</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>AAPADJS</td>
<td>Dues Adjustment Report</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>AAPCARD</td>
<td>Membership Card Process</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>AAPFEED</td>
<td>Advancement Dues-Finance Feed</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>AAPREMD</td>
<td>Membership Reminders Process</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>AAPRNEW</td>
<td>Membership Renewal Process</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>AAPSTAT</td>
<td>Membership Status Update</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>ADPACTC</td>
<td>Designation Accounting Report</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>ADPCFAE</td>
<td>CFAE Report</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>ADPEXPD</td>
<td>Expired Designations Report</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>ADPEXED</td>
<td>Advancement - Finance Feed</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>ADPFED</td>
<td>Pledge Feed to Finance Report</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>ADPVGER</td>
<td>Volunteer Support of Education Report</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>APPCAMR</td>
<td>Campaign History/Results</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>APPDCRN</td>
<td>Campaign Donor Report</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>APPSOLA</td>
<td>Campaign Solicitor Assignments</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>APPSOLB</td>
<td>Campaign Unassigned Solicitors</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>APPSOLC</td>
<td>Campaign Unassigned Cons.</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
<tr>
<td>APPTELF</td>
<td>Campaign Telefund Prospects</td>
<td>01-DEC-2003</td>
<td>MHOCKETT</td>
</tr>
</tbody>
</table>
### Oracle Developer Forms Runtime - Web

#### FGAC Policy and Predicate Query

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>HHOCKETT</td>
</tr>
<tr>
<td>Table Name</td>
<td>GORPGEO</td>
</tr>
<tr>
<td>Comments</td>
<td>Geographic Regions/Divisions for persons</td>
</tr>
</tbody>
</table>

#### Select

**Policy Status:** Policy is enabled on GORPGEO and FGAC restrictions will be applied.

**SQL Predicate:** 
```sql
(SELECT GB_GEO_VBS */ (/* GEOGRAPHIC_DIVISION*/ (gorpgeo_good_code = 'GRADUATE')))```

#### Insert

**Policy Status:** Policy is enabled on GORPGEO and FGAC restrictions will be applied.

**SQL Predicate:** 
```sql
(SELECT GB_GEO_VBS */ (/* GEOGRAPHIC_DIVISION*/ (gorpgeo_good_code = 'GRADUATE')))```

#### Update

**Policy Status:** Policy is enabled on GORPGEO and FGAC restrictions will be applied.

**SQL Predicate:** 
```sql
(SELECT GB_GEO_VBS */ (/* GEOGRAPHIC_DIVISION*/ (gorpgeo_good_code = 'GRADUATE')))```

#### Delete

**Policy Status:** Policy is enabled on GORPGEO and FGAC restrictions will be applied.

**SQL Predicate:** 
```sql
(SELECT GB_GEO_VBS */ (/* GEOGRAPHIC_DIVISION*/ (gorpgeo_good_code = 'GRADUATE')))```
Error Reporting

- Banner Forms show message on hint line. Open display error to see Oracle error.
Error reporting

- **Reports show Oracle Error (ORA 28113 Predicate Syntax Error)**
- **Self Service show error on new error page**
- **Oracle Bug**
  - Error with Update and Delete are not reported. Oracle does not note the access restriction and returns record updated successfully.
  - APIs are programmed to show an error when this happens (However, not all tables have API’s)
API message for failed update, delete
Questions and Answers
Thank you for your participation

Shelly Wingfield
swingfield@skybridgeglobal.com