New VBS Using Oracle Fine-Grained Access Control

John Morgan, SunGard SCT, Banner Architect

Rock Eagle 2004, Thu., Oct. 21, 11:30 AM
Introduction

- Introduce Oracle Fine-Grained Access (FGAC) as a working tool in SCT Banner for row level security
- When is this being implemented in Banner
  - Banner 7.0
- Scope of what FGAC will secure
  - Value Based Security (VBS)
  - Personally Identifiable Information (PII)
Definitions

- FGAC - Fine Grained Access Control
  - FGAC is meant for row level security
    - It works by dynamically modifying a SQL statement in a way transparent to users
    - Adds a condition (WHERE predicate clause) which restricts the rows shown to the user
Definitions

- Enabling technology used to implement VPD and other more flexible security
  - Used to achieve application security.
  - Users know of other users, and can possibly see data outside their area but be restricted from database modifications.

- Our project defines it as GOKFGAC FGAC
  - GOKFGAC is the package that owns all of the processing.
Definitions

- **VBS**
  - Value Based Security
  - Defined for individual users as needed

- **PII**
  - Personally Identifiable Information.
  - 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)
Definitions

- PII secures General Person identifiable information, and is only on the selection of data – delivering PII on SPRIDEN
- To have access to a SPRIDEN row, the PIDM must have a row in one of the PII Domains the user is assigned
- When turned on, affects all users of the system. Certain users and program objects can be exempt.
- PII and VBS do not require each other, can implement one or the other
Definitions

- Domain
  - Area in Banner that has a common driving table
    - Example of a VBS domain is Student Admissions
    - The driver is SARADAP
    - All lesser tables in Admissions are part of the domain and will follow restrictions based on the rules defined for the Admissions domain
  - PII domain determines where PIDM must exist
    - The domain driver for Admissions is SARADAP and the PIDM values must exist in this table for the user to have access.
Definitions

- **Predicate**
  - The 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
Definitions

- Business Profile
  - Lets you group users together that have the same access restrictions. Introduced to reduce data entry of access restrictions.
  - Different than BANSECR Roles. Maintenance of Business Profiles is meant to be distributed and moved out of the BANSECR schema.
Example of VBS

- The institution has two colleges: College of Arts and Sciences and College of Education.
- Each college has a separate Admissions Office.
- The Admissions Office can insert, update, delete and select all applications in their own college.
  - They can also admit their applicants into their college, but they cannot change the Student record.
  - In addition they can only query the applications in the other college.
Example of VBS (cont.)

- **Benefits of VBS**
  - Restrictions at the row level not the table or object
  - Security checking has to happen when rows are accessed
  - Restrict SARADAP tables access based on college code value
Example of PII

- Back to my institution with the Admissions Office
- Staff in Admissions Office can view people’s names/IDs only if the person has an application

Solution:

- Identify PII domain that is associated with User’s office (like Admissions)
- PII Policy on SPRIDEN will filter based on PII Domain assigned to individual users.
  - PIDM must have row in PII domain driver table for User to view SPRIDEN data
PII and Multiple PIDM prevention

- Can exempt USER from all PII processing
  - May be needed for users who create SPRIDEN rows
- Can exempt objects that perform searches from all PII and VBS restrictions
PII and protecting sensitive data

- Deliver limited masking rules for Forms
  - Turn visibility off on displayed fields on page
  - Change format of dates and numbers
    - To show only month/day of a date, use DD-MON
  - Conceal character data with ‘*’
  - Utilize on any Banner Form
  - Partial concealment of char data post 7.0 release
    - E.g.: show just the first three characters of the SSN like 123******
### How does FGAC work?

1. User selects from `saradap`
   
   ```sql
   Select * into saradap_c.rowtype from saradap
   Where saradap_pidm = :pidm and saradap_term_code_entry = :term_code
   ```

2. FGAC executes `GOKFGAC` predicate function and retrieves predicate

3. FGAC Appends Predicate to SQL statement

   ```sql
   saradap_coll_code = 'AS' and saradap_resd_code = 'M'
   ```

4. Row retrieved or no records found message
How does FGAC work?

1. User inserts into saradap
   Insert into saradap
   (saradap_pidm, .....)
   Values (1234, .....)

2. FGAC executes
   GOKFGAC predicate function and retrieves predicate

3. FGAC Appends Predicate to SQL statement
   (new)saradap_coll_code = ‘AS’
   and (new)saradap_resd_code = ‘M’

4. Row inserted or oracle error message displayed
Banner/GOKFGAC FGAC set up

Domain Driver Table
SARADAP

Domain Table
SARADAP

Domain Table
SARCHKL

Domain Table
SARQUAN

Oracle Table
SARADAP
Policy

Oracle Table
SARCHKL
Policy

Oracle Table
SARQUAN
Policy
New processes in Banner

- Setting up Policies using new GOKFGAC FGAC rules forms
  - Identify domain and its driver table
  - Define tables under each domain
  - Tables can be a part of multiple domains
  - Run gorfdpl.sql using BANINST1 ID to create the table policies in ORACLE
VBS Restrictions and Banner

Banner Object, or other activity against table

Oracle Table SARCHKL Policy

VBS Rules page GOAFIGAC

GOKFGAC Package predicate functions
New processes in Banner

- Defining VBS restrictions
  - Add new group rule and activate on page GOAFGAC
  - Enter predicate (SQL) statement for each domain you want restrictions defined
  - Add Business Profiles or User IDs that are restricted by rule
New VBS rules page in Banner
New VBS rules page in Banner

| Domain: | SB_CONTACTS_VBS | Student Contacts VBS |
| Predicate | sorcont_ctyp_cade in ('CMP','CNN') | Copy Domain |
| Table: | | Column: | Operator: | Edit: |

Validate SQL
**New VBS rules page in Banner**

### Business Profile Access to Group

<table>
<thead>
<tr>
<th>Profile</th>
<th>Description</th>
<th>Select</th>
<th>Insert</th>
<th>Update</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schooled</td>
<td>School of Education</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### User Access to Group

<table>
<thead>
<tr>
<th>User</th>
<th>Select</th>
<th>Insert</th>
<th>Update</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFriend</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MHockett</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
GOKFGAC FGAC Internal Processing

- GOKFGAC package contains context variables and functions called by VBS/PII FGAC policies
  - Centralized functions defined in the GOKFGAC package to construct the predicate
    - f_insert_fnc, f_update_fnc, f_select_fnc, f_delete_fnc
  - ALL GOKFGAC Table Policies use the same predicate functions
  - No coding required in Banner object to implement VBS using FGAC, ORACLE and GOKFGAC processing covers it all!
GOKFGAC FGAC Internal Processing

- GOKFGAC construction of the predicate

\[
\begin{align*}
&[\text{driver table link AND}] \\
&(\text{Predicate SQL 1 from GOAFGAC OR} \\
&\text{Predicate SQL 2 from GOAFGAC}) \\
\end{align*}
\]

- Above constructed for each domain and ‘AND’ed
- ORACLE automatically ‘AND’s the entire predicate to the executing SQL statement
- Page to view constructed predicate per user or business profile and table
GOKFGAC FGAC and performance

- Performance
  - Store constructed predicate statements in context variables
  - Previous version of VBS was based on secured views, not always returning the best performance
  - Testing on production sized database (PII is being tested at McGill)
  - Largest component of performance will be the SQL statement coded on GOAFGAC predicate rule
GOKFGAC FGAC and the Self Service

- Oracle Fine Grained Access works across the entire Oracle Database, including the Self Service
- There are ways to exempt self service from FGAC processing
- Still in Research
  - Requires Oracle ID if FGAC is needed for parts of the self service (SS Faculty)
  - Uses GOAEACC to cross reference the SS login ID and the Oracle ID
Turning GOKFGAC off for processes

- New page to identify objects that are excluded from GOKFGAC FGAC processing
  - Prevent data corruption
- All JOBS in GUBOBJS delivered as ‘exempt’.
- GOKFGAC FGAC has function to turn restrictions off
  - Can be coded in dbprocs, like the ones for Registration and new Common Matching
- Exemptions include both PII and VBS
GOKFGAC FGAC and VPD

- VBS and VPD can co-exist
  - Oracle ANDs multiple predicates together at runtime

```
Select * into saradap_c.rowtype
from saradap where
saradap_pidm = :pidm and
saradap_term_code_entry = :term_code
&
saradap_coll_code = ‘AS’
&
saradap_vpdi_code = ‘X’
```
GOKFGAC FGAC vs VPD

- VPD advantages
  - New column to secure data
    - Works for any group of related tables
  - Best for large-scale segmentation of data
    - E.g.: shared Student DB with Financial Aid VPDs
GOKFGAC FGAC vs VPD

- **VBS advantages**
  - Uses existing columns to secure data
    - Appropriate for sets of tables that contain the data necessary for security
  - Best for securing small sets of data
    - E.g.: in-state and out-of-state admissions officers
Which to Use?

- VBS and VPD on a continuum
  - Choice of which to use made after analysis of institutional needs
Replacing Old VBS with New VBS

- New VBS using FGAC will replace all existing Banner VBS implementations in release 7.0
- Secured views, table triggers and Form triggers removed from the following modules, replaced with Seed data to define domains and domain tables
  - Banner Student
    - Admissions, Recruiting, General Student, Test Scores, GPA, Courses, Schedule
  - Banner Financial Aid
    - RORSTAT
Summary

- Expandable, does not require modification to existing Banner objects to implement new policy.
- Predicate is SQL based and does not have a preset data dictionary
- Expecting wide adoption of the New VBS using FGAC because it is easier to manage
Thank You!

John Morgan
jmorgan@sungardsct.com
Thank you

SunGard, the SunGard logo, SCT, the SCT logo, and Banner, Campus Pipeline, Luminis, PowerCAMPUS, SCT Matrix, SCT Plus, SCT OnSite and SCT PocketRecruiter are trademarks or registered trademarks of SunGard Data Systems Inc. or its subsidiaries in the U.S. and other countries. All other trade names are trademarks or registered trademarks of their respective holders.

© SunGard 2003 - 2004