
ORACLE®

Domains, VPDs and Vendor Access Solution

OTM Domain and VPD Design

Program Agenda

1. Objective
2. OTM Domains
3. OTM VPDs
4. Vendor Based Security Scenario
5. Q&A

Domains and VPDs

Objective

Objective

- Review OTM Domain and VPD concepts
- Provide Domain and VPD Design Tips
- Review a Sample Vendor Based Security Scenario

Data Security vs. Data Filtering

Definition

Data Security vs. Data Filtering

Data Security:

- Protecting Data from destructive forces and the unwanted actions of unauthorized users

Data Filtering:

- A wide range of strategies or solutions for refining data sets. Data sets are refined into what a user (or a set of users) needs, without including other data that can be repetitive or irrelevant

Data Security vs. Data Filtering

OTM Data Security Tools:

- Domains
- VPD Profiles
- Access Control Lists
- User Roles
- User Configuration

OTM Data Filtering Tools:

- UI Screen Set Filters
- Manager Layouts
- Saved Queries
- Business Monitors
- Reports

Domains

Purpose

Purpose of Domains and VPDs

- Definition of Data Segregation for Security Reasons
- Workflow / Process Segregation
- Can be used for Data Segregation for Filtering purposes*

*Recommend evaluating other options

Domains

Types

Domain Types

- Peer Domains
- Hierarchical Domains
- PUBLIC Domain
- SERVPROV Domain
- Module Domains

Peer Domains

- They are Self Contained when created
- No implicit relationships with other Domains
- Relationship with other Domains is defined manually

Hierarchical Domains

- Hierarchical structure defined when created
- Implicit Top-Down security enforced. Users in the Parent Domain have implied access to all the Sub-domains.
- Additional relationships can be defined with other Domains.

PUBLIC Domain

- Contains the OTM System Parameters
- Contains configuration that is shared by all Domains
- Data in the PUBLIC Domain can only be updated by user DBA.ADMIN
- All Domains have implicit Read access to the PUBLIC Domain

SERVPROV Domain

- Used to configure Service Provider users
- Created with the necessary Carrier security configuration
- Users in this Domain are created automatically when a Service Provider is created in OTM
- Additional Carrier users can be created and associated manually with Service Providers

Module Specific Domains

- New Domains created to support new OTM modules
- Usage depends on the Module that uses them

Domains

Design

Domain Design

Domain and VPD design should be done as part of the full OTM Data Security Design.

Domain Design

- How is your Transportation data currently segregated in current systems? What is your target segregation? Is Consolidation an Implementation Objective?
  - Segregation by Client
  - Geographical or Sales Region
  - Order Source System
  - Data Type
    - Master Data
    - Transactional Data
    - Invoicing/Payment Data
- Users are configured by Domain. Consider what each configured user will have to see in OTM

Domain Design

How are your Transportation/Logistics and purchasing departments organized?

What objects (orders, shipments, invoices, etc.) is each department responsible for?

- Geographically: region? (APAC, NAM, EMEA), country?
- IT Group (using a specific Software instance)
- Previous company
- Product Line
- DC, Warehouse

Domain Design

What are your Data Security Segregation Concerns/Requirements by object type

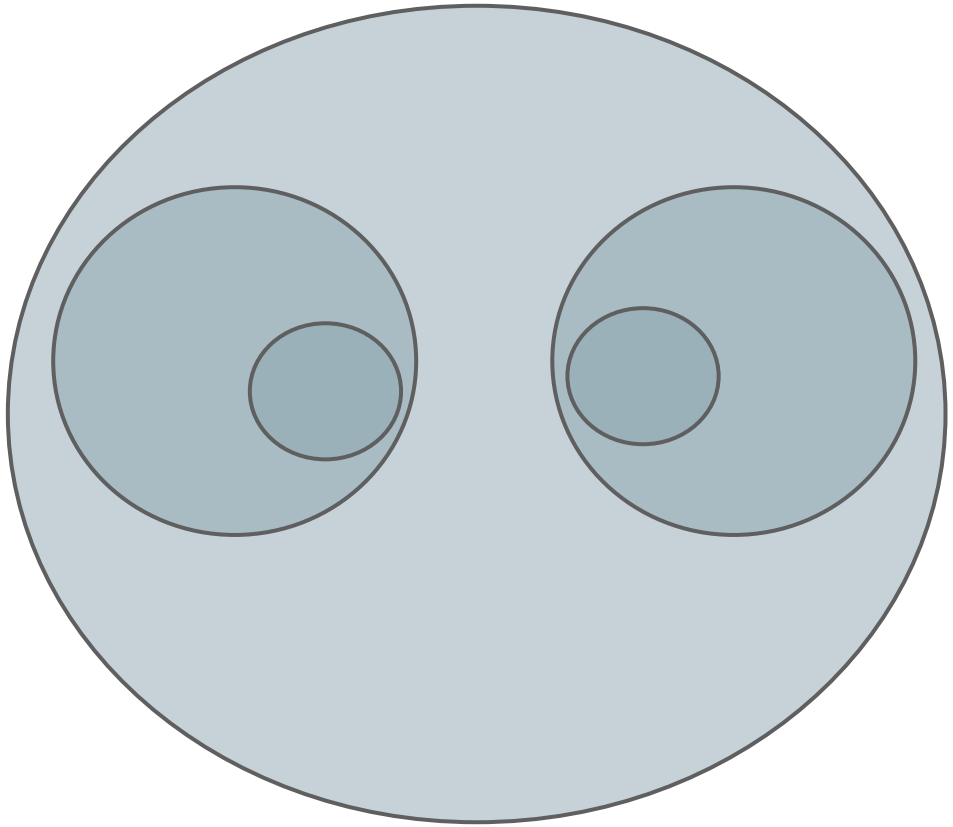
- Rates
- Orders
- Shipments
- Invoices
- Vouchers
- Locations*

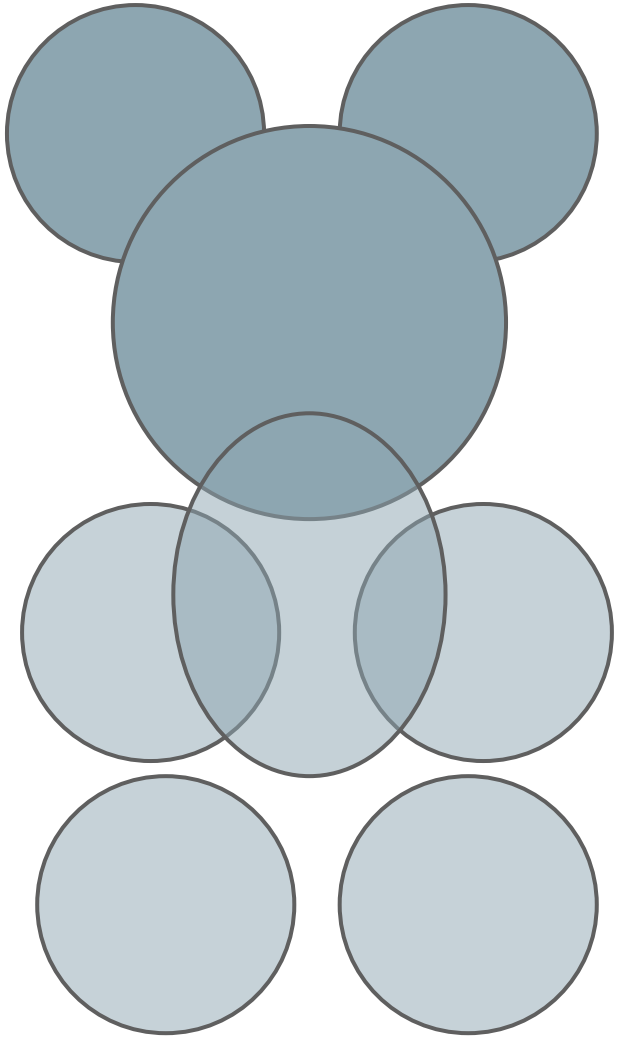
Domain Design

- From all the information gathered and any other current or Target Data Segregation (or Consolidation) Requirements:
- Identify (and exclude) Data Filtering Requirements
- Identify Data Security Requirements
- Identify which OTM Data security tools will address each Data Security Requirement
- Create an OTM Domain Design Document to meet the Data Security Requirements addressed by Domain Configuration

Hierarchical vs. Peer Domains

Hierarchical vs. Peer Domains





Peer Domains

Created as Stand-Alone Domains, the only Parent Domain is the PUBLIC Domain

Pros & Cons:

- Pros: More control, less potential complexity, more flexibility, easier debugging, easier maintenance
- Cons: Could cause some workflow duplication, less re-use, more maintenance

Peer Domains

Use when?

- Data is independent
- Data sharing needs to be more flexible
- Process flows in OTM are different

Hierarchical Domains

Implicit Top-Down security enforced. Users in Parent Domain have implied access to all the Sub-domains.

Pros & Cons

- Pros: automatic pre-established relationships, security and control. Less initial setup required
- Cons: less flexibility, exceptions harder to manage, difficult to override parent/domain implicit relationship for exceptions

Hierarchical Domains

Use when?

- Data relationship between domains is mostly hierarchical (Top down)
- Objects exist where their process is the same across all Sub-Domains
- No need to control processes in Parent and Sub-Domain for the same object types

PUBLIC Domain

- Avoid doing any application configuration there
- Avoid using the workflows in this domain, if you need one, copy it to your domain
- Do not use it to for any kind of transactional processing
- Lock it down!

Domains and Workflows

Where do I create my workflows? For Peer Domains? For Hierarchical Domains? In the Parent Domain? Sub-domains?

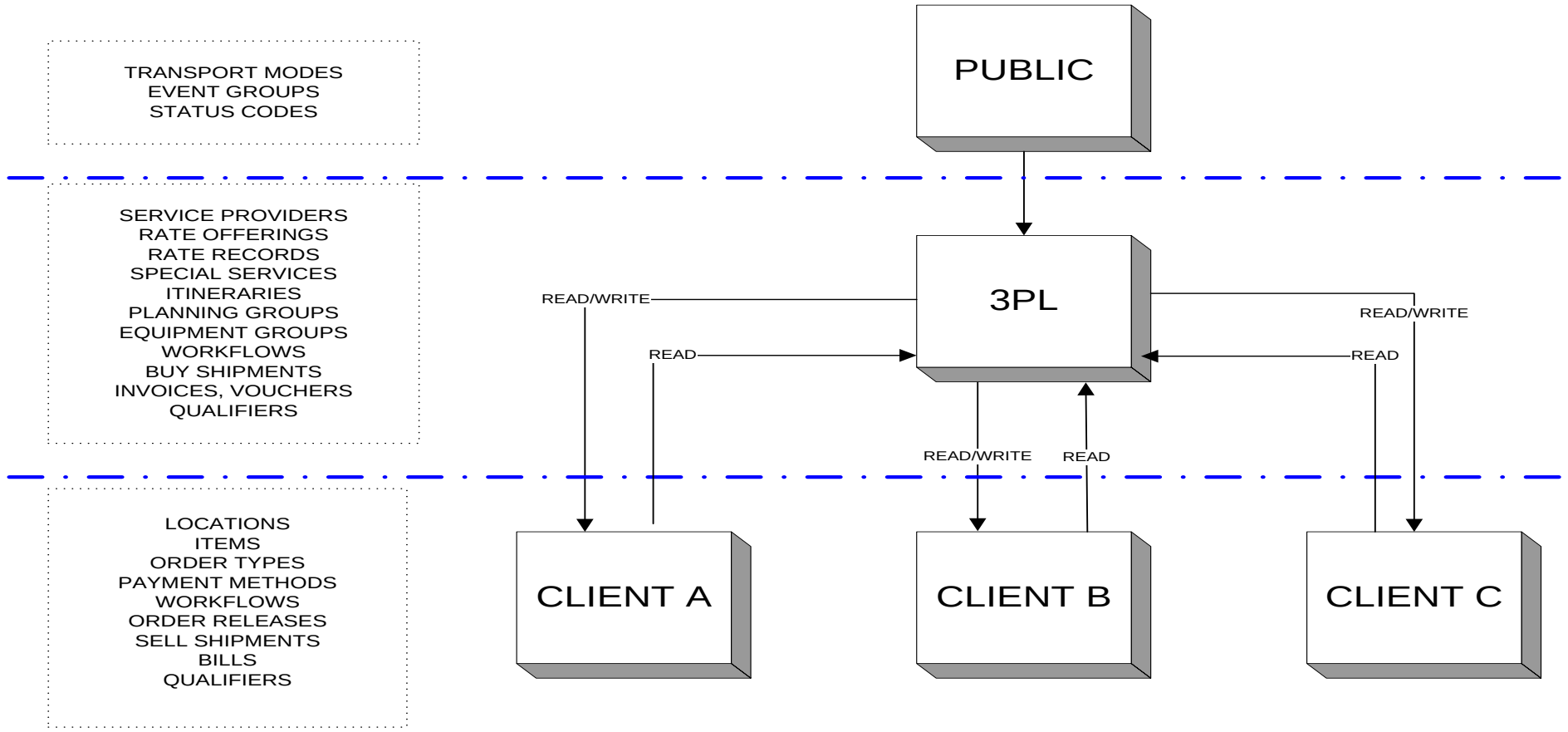
Domains and Workflows

- For Peer Domains, create Workflows in the Domains where their object types are stored
- For Hierarchical Domains, create Workflows in the highest level that will be common for all Sub-Domains

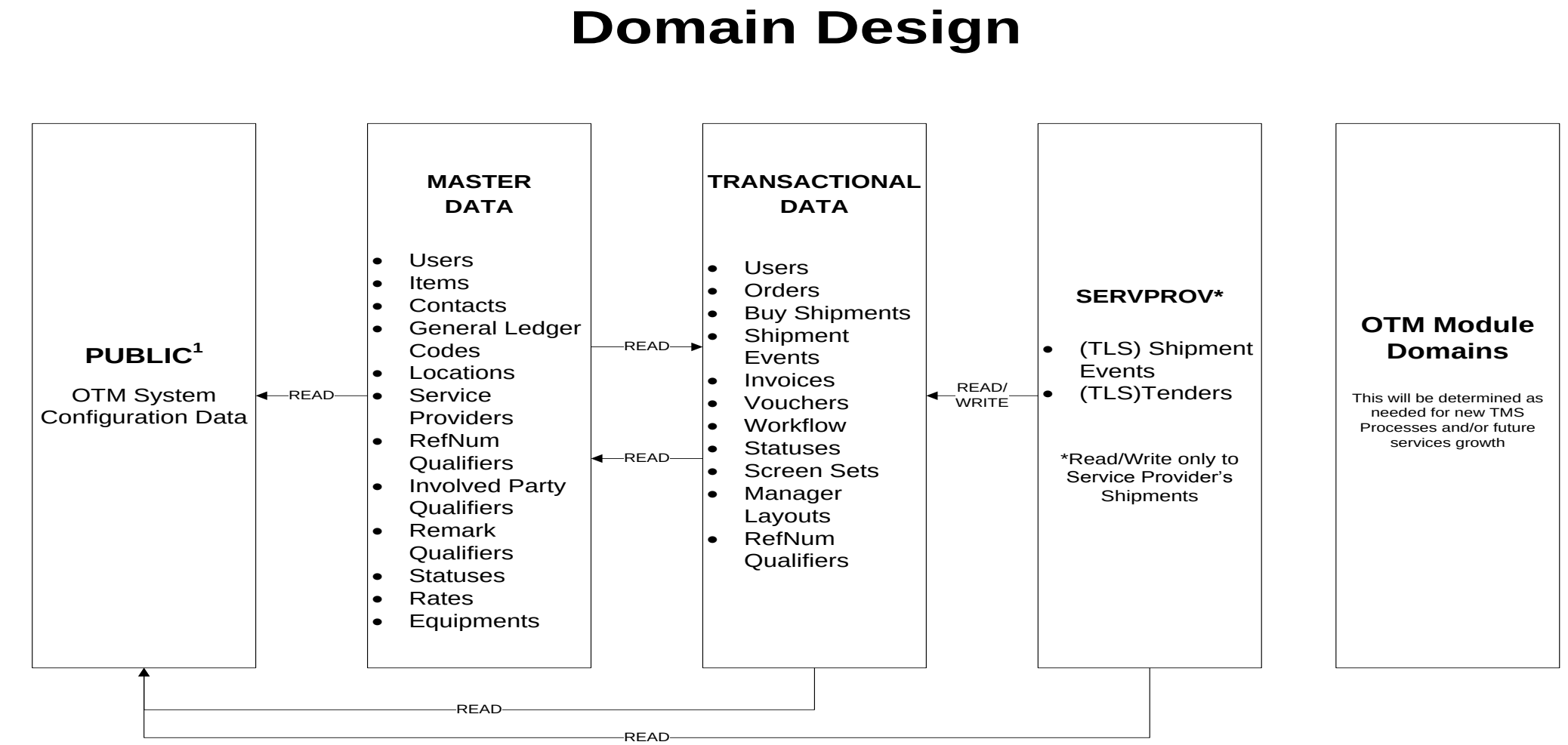
Domain Design

- Define List of Domains to be created
- Define List of objects in each domain:
  - Try to keep all of each object type at the same level if using Hierarchical, in one Domain if using Peer Domains with grants
    - Transactional data: Orders, shipments, invoices, vouchers, etc.
    - Master data: Items, Locations, Service providers, Rate Information
- Define Domain Relationships/Grants:
  - Read
  - Read/Write
  - Include Grantor Sub-domains (option) *
  - All Table Sets/Some Table Sets

Typical 3PL Scenario



Typical Corporate Scenario



[1] By Default all Domains have Read Access to the Public Domain

Domains

Configuration

OTM Domain Configuration

- A Domain defines the Data that a User and his processes have access to
- By Default, a User can only access data in his Domain + PUBLIC data + data in its Sub-domains
- Additional access can be provided using Grants
- Grants are given from one Domain to another:

Domain Grants

- **Tableset:** List of tables created so that grants can be made in terms of table sets rather than individual tables. The ALL_TS table set contains all the “normal” OTM tables.
- **Domain Grant:** A Domain Grant allows access from one domain to another to all the tables in the domain or to a subset of tables (table set). A user logged in one domain can see data in the other domain to which they have been granted access.

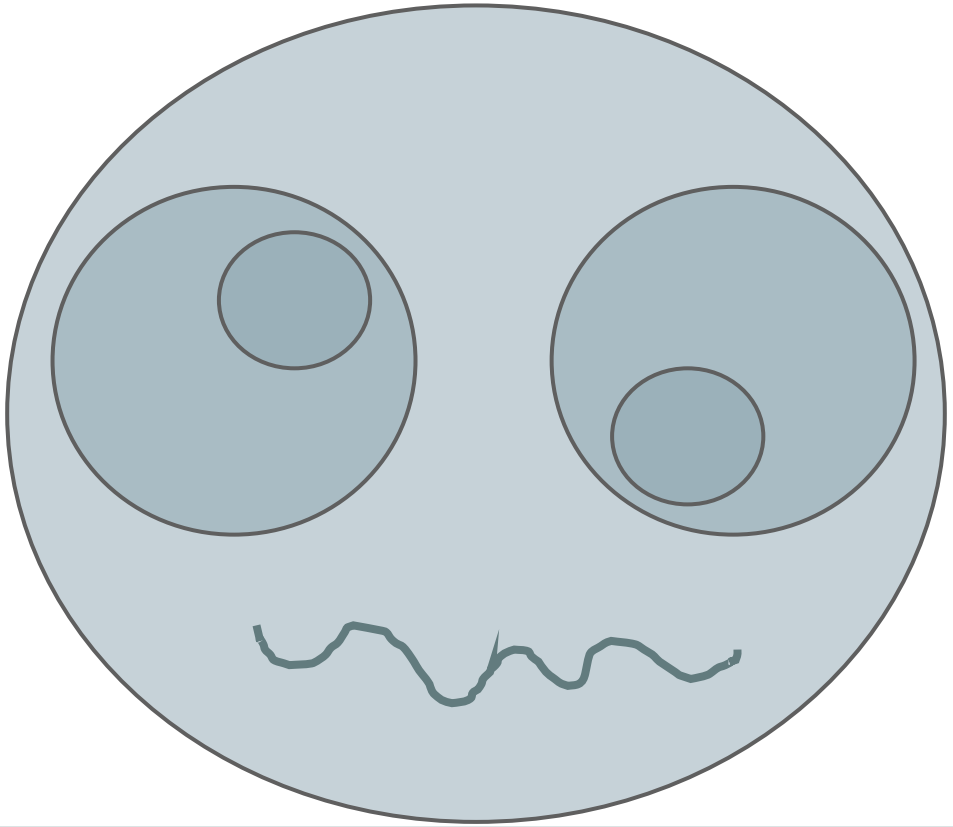
Domain grants

Recommendations:

- Use Grant access to ALL_TS if possible
- Limit use of Read/Write permissions
- Use Include Grantor Sub-Domains option with care if needed
- Use appropriate Domain Names (Search, Integration, Reporting Impact)

Domain Grants

- Note on “Include Grantor Subdomains” option:
  - Be Careful if you are using Hierarchical Domains and granting read access to the parent domain



VPDs

(Virtual Private Databases)

VPD Definition

- Virtual Private Databases provide fine-tuned Data Access Control to Users
- A Virtual Private Database (VPD) is an Oracle feature that provides Fine-Tuned Access Control, down to the level of Table Rows
- Similar to adding a SQL “Where” clause to every Query executed by the User

VPD Benefits

- Maintenance: Applied at the Database Level once, no need to manage at the App Layer
- Flexibility. VPDs provide different Policies (Read, Insert, Update, etc), at the Table Row level
- Data is secure no matter how the user accesses the data (UI, Operational Reports*, etc)

VPD Profile Cautions

- External Predicates need to be designed by someone with good DB and SQL knowledge
- An External Predicate with erroneous or inefficient SQL can bring down OTM

VPD Profiles

Design

VPD Profile Design

- VPD Profiles should be used to address Data Security Requirements NOT Data Filtering Requirements
- A thorough OTM User Configuration review is needed to identify the Tables that require External Predicates (Menus, Screen Sets, etc)
- It may not always be possible to completely exclude Visibility to certain Table Rows
- VPD's are not the only Data Security tool in OTM, ensure the requirement is met by the appropriate OTM Tool
- Review and test the Operations to the Objects a User will execute

VPD Profile Design (Domain vs. VPD)

The Main objective of a VPD Profile is: To further section out access to Data at a more granular level

The Domain level should be fairly general, because creating a new domain impacts:

- Data Keys (Master Data: Items, Locations, Transactional Data: Orders, Shipments)
- Integration
- User Configuration
- Workflows

VPD Design (Domain vs. VPD)

When to use VPDs?

When there is a need to segregate some of the data at a lower level for users that otherwise would be able to use almost the same OTM configuration, i.e. :

- - UI configuration (Menus, Screen Sets, etc)
- - Master Data
- - Integration
- - Workflows
- - Messages

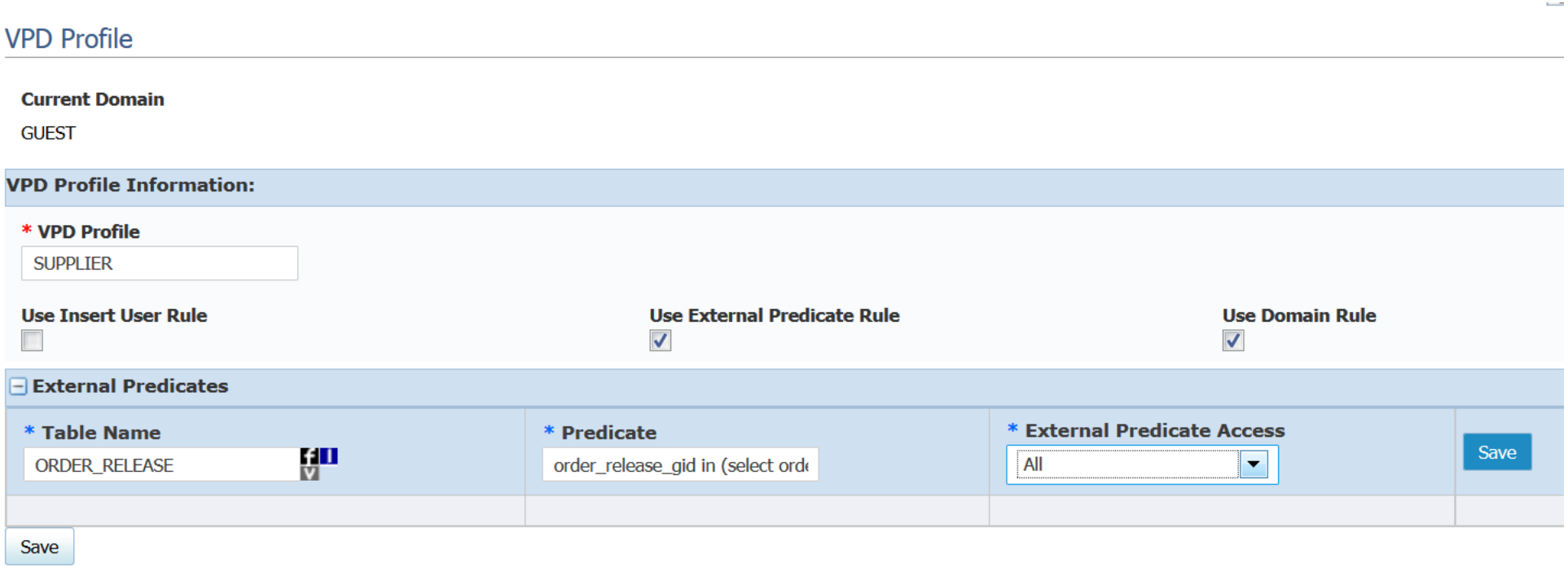
VPD Profiles

Configuration

VPD Profile Configuration

- A VPD Profile is a set of Virtual Private Database (VPD) Rules
- VPD Rules provides fine-grained Access Control to Users, across or within Domains
- VPD Profiles are assigned to User Roles
- User Roles are assigned to Users

VPD Profile Configuration



VPD Profile Configuration

VPD Profile General Information:

- Use Insert User Rule to limit access to data that the current user entered
- Select Use External Predicate Rule to limit user access to Database Tables and Rows specified by the statements in the External Predicates defined in the VPD Profile
- Clear the Use Domain Rule check box to disable Domain Level Security for a given VPD profile*

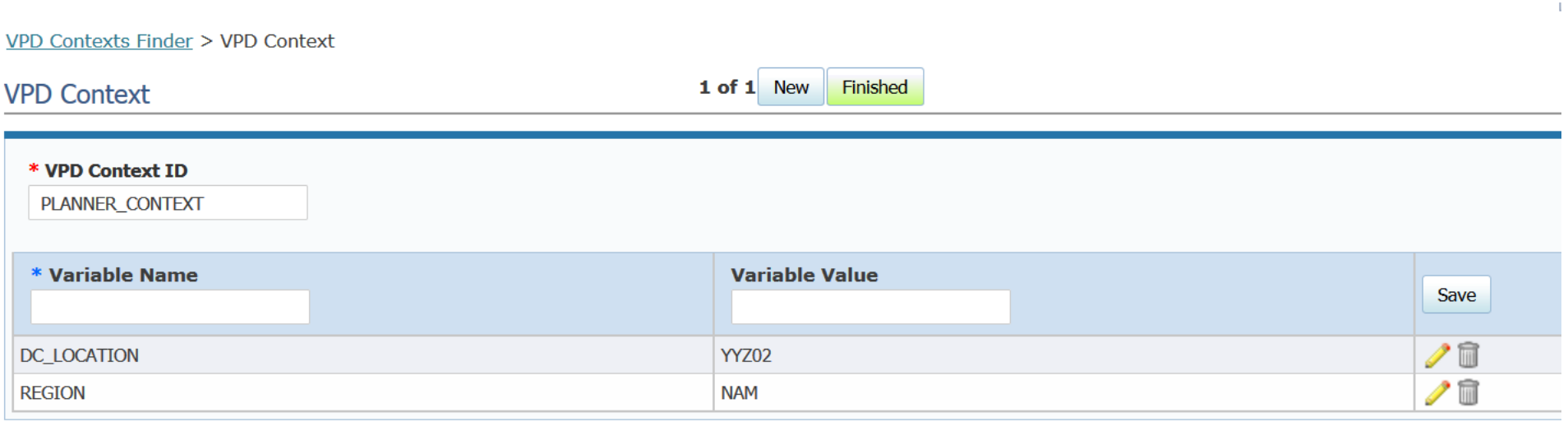
VPD Profile Configuration

VPD Rules with External Predicates:

- Table Name: Table for which this rule will apply
- Predicate: SQL where clause that will be applied to the table. This will be an additional “data filter” applied any time the user queries this table
- External Predicate Access. Appropriate access rights that should apply to the table and predicate:
  - ALL, Read, Insert, Update, Delete, Insert/Update/Delete

Context Variables

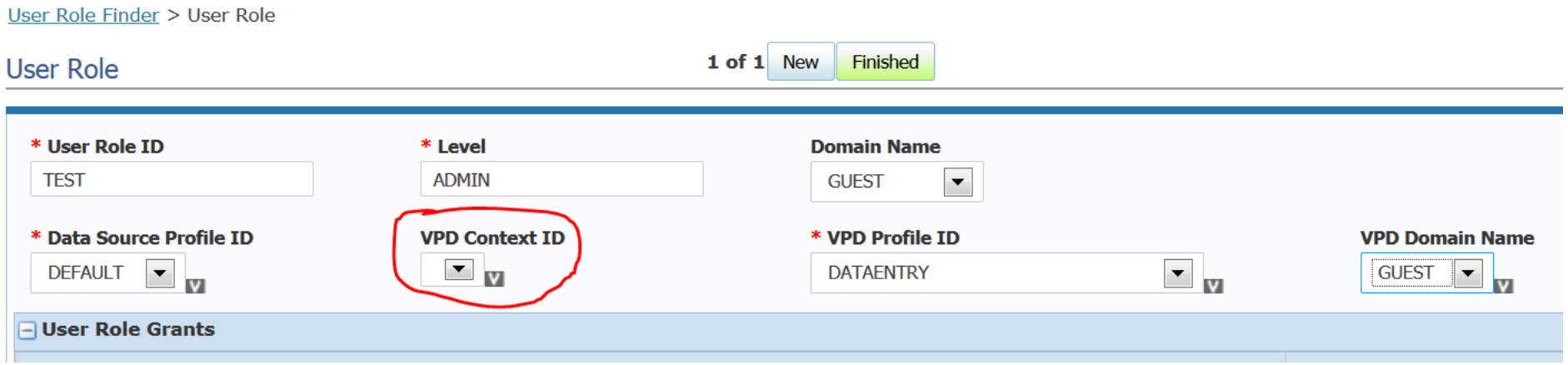
- Definition



Context Variables

Assigned to a Role

- Function sys_context(context, variable) available for use in VPD Rules



Context Variables

Standard Context Variables:

- sys_context('GL_USER_CTX','log_in_user_gid')
- sys_context('GL_USER_CTX',‘gl_user_gid')

Configured Context Variables:

- sys_context('GL_USER_CTX','LOCATION_GROUP'

Vendor VPD

Example

Vendor VPD Example

VPD Scenario: Vendors

Assumption is that all Vendors can use:

- Same UI configuration
- Master Data
- Interfaces
- Workflows
- Message notifications

VPD Vendor Example

- Objective: Vendors must not see other Vendors Orders or Shipments

Vendor VPD Example

Step 1. Identify the Tables involved

Considerations:

- Be careful to not miss related tables
- Be careful to consider all the UI menu options that users have access to
- -Shipment
- - Shipment Stop
- - Ship Units
- - Order Bases
- - Order Base Lines
- - Order Releases

Vendor VPD Example

- Step 2. Identify the Criteria used to segregate the Orders and shipments
- Source Location? *
- Destination Location?
- Involved Party?

Vendor VPD Example

- Step 3. Design the Structure to link the Criteria to the User or User Role
- Step 4. Write External predicates
- Step 5. Test Predicates
- Step 6. Create VPD Profile
- Step 7. Test VPD Profile

Vendor VPD Example

- Sample Docs

Q & A

Hardware and Software
Engineered to Work Together


ORACLE®