Oracle Database Vault

Under the Covers

Vipin Samar
Vice President, Database Security, Oracle
Data Security: Oracle Products

**User Management**
- Oracle Identity Management
- Enterprise User Security

**Access Control**
- Oracle Database Vault
- Oracle Label Security

**Monitoring**
- Oracle Audit Vault
- EM Configuration Pack

**Data Protection**
- Oracle Advanced Security
- Transparent Data Encryption
- Oracle Secure Backup

Core Platform Security
Agenda

• Current Techniques to Control Access
• High-level Goals for Database Vault
• Database Vault Architecture
• Database Vault Components
• Operating with Database Vault
• Case Studies
• For More Information
Controlling Access to Oracle Database

Current Techniques

- Controlling Network Access
  - Configure SQL-Net to control connection from specific addresses

- Controlling User Login
  - Define login trigger to control who can access the database

- Controlling Access and changes
  - Define DML triggers to control row level access
  - Create VPD and OLS policies per table and view
  - Define system triggers to control DDL commands

- Controlling access to sensitive roles
  - Integrate Application Roles to control privilege escalations

- Auditing to monitor access (if nothing else)
Limitations of Current Techniques

- Collection of security techniques
  - Lacks underlying common framework and management
  - Per object control required; Manageability issues
  - Lacks flexibility and may require application changes
  - Operational complexity with multiple components
- No protection from users with DBA privileges
  - DBA role with full access to user and business data
  - Only few apps built with least-privilege model
  - Various utilities require powerful administrator privileges
- Cannot meet new compliance requirements
  - Separation of Duty not enforced
  - Cannot control user creation, role assignment, etc.
  - No way to specify additional security policies on top of exiting apps
- Performance impact due to triggers or SQL modification
Oracle Database Vault Goals

Defense in Depth

- Integrated security framework to provide full control
  - Network, users, DBA, data, roles, SQL
  - Multi-factor Authorization and Policies across various checks
  - Protect and share data assets using environmental factors
- Compliance requirements
  - Built-in Separation of Duty (User mgmt, data mgmt, apps mgmt)
  - Group business data into individual administration units
  - Prevent misuse of powerful privileges
  - Support Database consolidation
- Operational requirements
  - No application changes
  - Minimal Performance impact
  - Easy-to-use PLUS customization flexibility
  - Hardened Database with seeded rules to lock down
  - Audit security relevant events
Oracle Database Vault

- Controls on privileged users
  - Restrict DBA access to application data
  - Provide Separation of Duty
  - Security for database and information consolidation
- Enforce data access security policies
  - Control who, when, where and how is data accessed
  - Make decision based on IP address, time, auth…
- Available on Oracle 10gR2 and 9iR2
- Validated with PeopleSoft
- E-Biz & other Apps validation underway, including 3rd party
Oracle Database Vault
Protection Realms

• Database DBA views HR data
  Compliance and protection from insiders

• HR DBA views Fin. data
  Eliminates security risks from server consolidation

Realms can be easily applied to existing applications with minimal performance impact
Oracle Database Vault
Custom Policies: Multi-factor Authorization

SELECT ....
Unexpected IP address
HR account

CREATE ...
Business hours
FIN DBA

HR
FIN
Database Vault – Under the Covers
Database Vault System Overview

Oracle Database Vault (DV)

Oracle User/Session (SQL)

Oracle Label Security
Application Roles

Realm Checks
Command Check
Role Checks

HR Realm
Fin Realm
Dictionary Realm

HR
Fin
SYS

Management UI
Protected Schema
Security Config
DV Factors
Rules & Rule Sets
DV Audit
Key Components

- Protection Realms
- Decision Factors
- SQL Command Rules
- Usage Reports
Protection Realms

- Collections of schemas, objects and roles to be secured
- Controls SELECT, DML, DDL, EXECUTE on protected objects
- Prevents super user (ANY) access to security sensitive data
  - Does not impact direct object priv.
- Rule sets and factors for more control (introduced later)
- Realm owner determines:
  - Who can access the realm using system privileges
  - Grants/revokes applicable roles
- Authorization enforced at every data object access during SQL execution
Benefits of Data Protection with Realms

- Ability to restrict access to privileged users based upon a collection of objects
- Separation of Duty regarding user administration, and role management
- Ability to define additional realm authorization rules based upon requirements
- Limit damage even if privileges escalate to DBA
- Minimize risks associated with an army of DBAs for 7 * 24 operation whether in-house, outsourced
- No changes required to applications
Decision Factors

- Including additional operational and other application factors in controlling access to realm-data or other SQL commands
- User attributes (USERENV values)
  - Date/Time
  - IP Address, Machine
  - Proxy user name, …etc
- Application/Custom Attributes
  - Can be any other PL/SQL expressions
  - Define using application context
- Transparent to the Application
- Trusted environment attributes
  - Instantiated during user logon
  - Cached in user session (UGA)
  - Session or Access

Customer-controlled variables
Additional Built-In Factors

- **User Factors**
  - Name
  - Authentication type
  - Session User
  - Proxy Enterprise Identity

- **Network Factors**
  - Machine name
  - Client IP
  - Network Protocols

- **Database Factors**
  - Database IP
  - Database Instance
  - Database Hostname
  - Database SID

- **Runtime Factors**
  - Language
  - Date
  - Time
SQL Command Rules

In order to perform this SQL command . . .

On this object . . .

owned by this user . . .

this rule set must evaluate to TRUE.
SQL Command Rules Mechanics

- Works very similar to DDL event triggers
- Built into the SQL engine for optimization and security
- Can reference USERENV or Factors for authorization decisions
- Ultimate Veto power
- Cover all basic DDL and DML commands

<table>
<thead>
<tr>
<th>Alter Function</th>
<th>Audit/Noaudit</th>
<th>Alter Tablespace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alter Package Body</td>
<td>Alter Procedure</td>
<td>Alter Profile</td>
</tr>
<tr>
<td>Alter System</td>
<td>Alter Synonym</td>
<td>Alter Table</td>
</tr>
<tr>
<td>Alter Trigger</td>
<td>Alter User</td>
<td>Alter View</td>
</tr>
<tr>
<td>Connect</td>
<td>Create Function</td>
<td>Create Index</td>
</tr>
<tr>
<td>Create Package</td>
<td>Create Database Link</td>
<td>Create Procedure</td>
</tr>
<tr>
<td>Create Role</td>
<td>Create Package Body</td>
<td>Create User</td>
</tr>
<tr>
<td>Create View</td>
<td>Create Table</td>
<td>Grant</td>
</tr>
<tr>
<td>Insert</td>
<td>Create Tablespace</td>
<td>Create Trigger</td>
</tr>
<tr>
<td>Truncate Table</td>
<td>Update</td>
<td>Delete</td>
</tr>
<tr>
<td>Execute</td>
<td>Select</td>
<td></td>
</tr>
</tbody>
</table>
Rules and Rule Set
Additional controls on Realms and SQL Commands

Rule 1 → TRUE or FALSE
AND / OR
Rule 2 → TRUE or FALSE
AND / OR
 Rule n → TRUE or FALSE
AND / OR

Rule Set Result → TRUE or FALSE
Examples of Security Policies

- IP address based policy
  - Allow access from intranet IP addresses
  - Allow access only from application servers
  - Data loading from intranet, but transactions only from middle-tier
- DBA policies
  - Allow updates to the database structure only on the weekend
  - Allow DBA access only with PKI/Kerberos authentication
  - Allow DDL but only with strong authentication
  - Permit DDL (CREATE INDEX) but not SELECT
  - Implement a different set of policies for different types of DBAs
  - Two-key actions
- Time/date based policies
- Disallow access from adhoc tools (SQL*plus)
Database Vault Reports

- Over 3 dozen security reports
- Useful for initial priv. maps
- System and Public Privileges
- Audit violation/use attempts
Protecting Database Vault and Database
Protecting Database Vault Schema

Security configuration needs full protection

- Protected Schema: Special built-in schema that is not accessible to DBAs, including SYSDBA
- Stores Database Vault security relevant objects and metadata
- Enforcement integrated into database security layer
  - Access only through DV roles
  - Database Vault schemas are protected schema
  - No creation or dropping of Database Vault schemas allowed
  - SYSDBA cannot modify/query Database Vault schemas
  - Protection not bypass-able by DBAs
- Stops privileged users from tampering DV meta-data
Oracle Database Vault Roles
Administration Model

- DV Administrative roles
  - DV_SECANALYST: Reporting only
  - DV_ACCTMGR: Maintain db accounts/profiles (but no roles)
  - DV_OWNER: Big boss but cannot grant any direct access rights

- DV Realm Roles
  - DV_REALM_OWNER: Manages realm and associated roles

- Security
  - Provide separation of duties with different admin roles
  - sys, system, sysdba and sysoper cannot grant DV_OWNER, DV_ADMIN roles

Please refer to the documentation for complete details.
# DB Hardening

<table>
<thead>
<tr>
<th>Initialization Parameter</th>
<th>Default Value in DB 10g R2</th>
<th>New Value specified by Database Vault</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUDIT_SYS_OPERATIONS</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>AUDIT_TRAIL</td>
<td>NONE</td>
<td>DB</td>
</tr>
<tr>
<td>LOCAL_LISTENER</td>
<td>Not configured</td>
<td>LISTENER &lt;SID&gt;</td>
</tr>
<tr>
<td>OS_AUTHENT_PREFIX</td>
<td>ops$</td>
<td>(null string)</td>
</tr>
<tr>
<td>RESOURCE_LIMIT</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>SQL92_SECURITY</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>RECYCLEBIN</td>
<td>ON</td>
<td>OFF</td>
</tr>
</tbody>
</table>
After Installing Database Vault

- Re-links Oracle Kernel
  - Replaces objects in kernel library; New Oracle executable
- Hardens the database
- Creates new Database Vault security metadata repository in protected schema to prevent from DBA tampering
  - Defines protected schema DVSYS
  - Stores security tables, functions and views in DVSYS
  - Locks DVSYS account
- Creates realms for major area of admin. responsibilities
  - Account Management
  - Data Dictionary
  - Enterprise Manager
  - Database Vault
Account Management Default Realm

- Protects user accounts and profile
  - Create/Alter/Drop User command
  - Session Connect role
  - Create/Alter/Drop Profile command
- Protects Account Management role
- Granted Access: Only user account managers
Data Dictionary Default Realm

- Protects all DBMS meta-data
  - All objects owned by SYS
  - All objects owned by SYSTEM
  - All objects owned by seeded schemas like:
    - CTXSYS
    - MDSYS
    - OLAPSYS, …etc
  - All Seeded Administration Roles like:
    - DBA
    - SCHEDULER_ADMIN
    - HS_ADMIN_ROLE, …etc
- Granted Access: Only during DB maintenance and on exception
Enterprise Manager Default Realm

- Protects all objects required by Enterprise Manager
  - All objects owned by SYSMAN
  - All objects owned by DBSNMP
  - All Enterprise Manager related Roles:
    - OEM_MONITOR
    - MGMT_USER
    - MGMT_VIEW
- Granted Access: Operators of Enterprise Manager to monitor health of DBMS
Database Vault Default Realm

- Protects all Database Vault meta-data, including:
  - All object owned by Database Vault schemas
  - All objects owned by LBACSYS
  - DBMS_RLS package
  - All Security Administration Roles
    - DV_ADMIN
    - DV_OWNER
- Granted Access: Only the security officer
Operating with Database Vault
### Post Installation Oracle Environment

#### Separation of Duty

<table>
<thead>
<tr>
<th>Key roles</th>
<th>Roles</th>
<th>Description</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Management</td>
<td>DV_ACCTMGR</td>
<td>User account management responsibility that can create, drop, or modify database users.</td>
<td>DBA can no longer manage users</td>
</tr>
<tr>
<td>Security Administrator</td>
<td>DV_OWNER DV_ADMIN</td>
<td>Setup Database Vault Realms, Command Rules, authorize others users to use them, and execute various Database Vault specific security reports.</td>
<td>DBA can not longer grant/revoke DBA roles nor access DVSYS schema</td>
</tr>
<tr>
<td>Resource Administrator</td>
<td>SYSDBA</td>
<td>Traditional DBA tasks</td>
<td>None</td>
</tr>
</tbody>
</table>
Other Impact On Operations

- Separation of Duties may require review of security operation procedures and responsibilities
  - Define data owner and system administrators
  - Identify sensitive data and access policies
- Administration affected
  - User and application administration
  - Privilege administration
  - Ad-hoc program in place that rely on DBA or SYSDBA being all powerful
Performance

- Tested
  - TPCC: ~1% with realm-protection
  - SQL Command Rules protection overhead depends on rule complexity

- Techniques used for improving performance
  - Caching of realm objects, realm membership, realm authorization result
  - Kernel row-cache for DV policies and meta-data
  - No PL/SQL VPD policy
  - No logon triggers for evaluation of factors
PL/SQL API to Database Vault

• PL/SQL interface for scriptable administration and tools
• API includes
  • Create, modify, and delete Database Vault components
  • Allow a session to define their security environment
  • Query the state and values of components
  • Administer and configure system-wide Database Vault parameters
• Supports for bulk policies loading
Database Vault Trust Profile

- Trusted Accounts
  - DV_ACCTMGR: Manages users/profiles, but cannot grant
  - DV_OWNER: Creates realms, Command Rules, Factors, etc.
- Trusted Roles: SYSDBA
  - But operations are audited
  - And they cannot modify DV schema, or grant DV roles
  - Can be blocked (if needed)
- Trusted Operating System users
  - Oracle software owner
  - OS Root
  - Members of DBA and OINSTALL OS groups with direct file access
- Data in backed up media can be accessed unless encrypted

Refer to the Protection Profile section of the Database Vault documentation for further details.
Deployment Flow

1. Define Realms (Block Highly Privileged Users)
   2. Add Command Rules (Optional)
   3. Add customized Factors, Rule Sets, or other security policies (Optional)
   4. PL/SQL scripts to deploy security policies (Optional)
   5. Test your application and measure performance
   6. Consider application maintenance
Case Studies
## Case Study 1

**Financial Services**

<table>
<thead>
<tr>
<th>Business Requirements</th>
<th>Database Vault Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent DBAs from accessing sensitive data</td>
<td>Put sensitive data/schema in a Realm</td>
</tr>
<tr>
<td>Control DBA’s use of ad-hoc query tools</td>
<td>Restrict connections by ad-hoc query tools to maintenance times</td>
</tr>
<tr>
<td>Enforce maintenance periods</td>
<td>Use DV to enforce another monitoring user to be logged in while patching</td>
</tr>
<tr>
<td>Restrict hostnames authorized to access the DB</td>
<td>Add rules to specify trusted middle tier systems</td>
</tr>
<tr>
<td>Control access based on geography</td>
<td>Restrict system access by geography using subnet Factor</td>
</tr>
</tbody>
</table>
## Case Study 2
### Hosting Services

<table>
<thead>
<tr>
<th>Business Requirements</th>
<th>Database Vault Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide assurance to customers their data is protected</td>
<td>Define Realms for customer-specific sensitive data</td>
</tr>
<tr>
<td>Reduce liability for data breach by limiting access to</td>
<td>Define realms around each hosting data to enforce separation of duty</td>
</tr>
<tr>
<td>customer data by hosting services staff</td>
<td></td>
</tr>
<tr>
<td>Provide backend operations to customers, among other</td>
<td>Define command rules to allow multiple level of DBAs in order to protect data from</td>
</tr>
<tr>
<td>services</td>
<td>backend operations</td>
</tr>
<tr>
<td>Comply with regulations such as SOX and PCI</td>
<td>Use DV role to enforce operations. DBAs are not allowed to see business data</td>
</tr>
</tbody>
</table>
Summary
Oracle Database Vault Summary

Defense in Depth

• Integrated security framework to provide full control
  • Control access based upon Network, users, DBA, data, roles, SQL access
  • Multi-factor Authorization and Policies across various checks
  • Baked-in Security controls

• Compliance requirements
  • Built-in Separation of Duty (Users mgmt, data mgmt, apps mgmt)
  • Prevent misuse of powerful privileges

• Operational requirements
  • No application changes required
  • Minimal Performance impact
  • Easy-to-use PLUS customization flexibility
  • Support Database consolidation
Learn More

Learn the Technology

- Visit: oracle.com/goto/DatabaseVault
  View whitepapers, buyer’s guides, and webinars

Try the Software

- Visit OTN: otn.oracle.com (9.2 and 10gR2) OR
  Download software, get technical information

Ask Our Experts

- Speak with an Oracle Security specialist