Whitepaper

June, 2024

Omega DB Security Reporter ™

For Oracle Database

Security assessment and reporting

Introduction

The database is the central point of enterprise's most valuable informational assets, data on customers, partners, transactions, financial and much more. With the arrival of the information age, millions of such records owned by the company are being confronted with an ever increasing number of attacks from insider and/or outsider sources who are trying to gain unauthorized access to steal, destroy, compromise or retrieve industrial espionage data. Database security is one of the top concerning priorities of the information owners that needs to comply with more internal and external regulatory compliance practices and standards that require stronger information security controls.

The database remains today one of the less protected point of the enterprise's information, which traditionally has been focused mostly in protecting perimeter networks, or operating systems which do indeed create some barriers, but which are few effective against insider threats, especially from privileged account holders, who not only are within the internal network, but by nature of their jobs may access information bypassing application security, or own a high security clearance on it. Furthermore the traditional network and OS protection has been modeled with the concept in mind of the once "isolated" database within the internal network, but due to their increasing business services and interfaces, today's databases are much more open toward the external networks and internet, and the number and sophistication level of the attacks has since then increased.

In all of the recent studies performed by the authoritative bodies of the field, inside breaches account for more than 50% of data breaches, usually with higher impact than breaches from outside.

The Challenge

The first approach for a strong security on the database is to have a clear picture of everything related to security. This means an accurate process of security assessment and reporting. The security administrator must know how the privileges are granted, to whom are granted, how the audit policies are configured, especially related to the granted privileges, and many other things like passwords settings for users and important security-related initialization privileges.

The challenge consists not only in having a clear picture on the above, but also in tracing their change in time, as things like privileges and (consequently) their respective audit (or missing audit) are stuff that changes frequently in time – just consider new users and application schema owners created or deleted, or changing privileges according to application changes.

Consolidating, enhancing and formalizing these security requirements into a software solution, which must be accurate and practical are further steps in this challenge.

Introducing Omega DB Security Reporter

Omega DB Security Reporter is a security auditing, software-only, and out-of-box solution for Oracle databases. It implements quick reporting, visualization and documentation of the security posture of the Oracle database and addresses the internal and external security compliance requirements. Omega DB Security Reporter provides detailed, integrated, categorized and evaluated assessment of the Oracle Database, enabling the security personnel to dispense with this complex task in a few minutes.

Omega DB Security Reporter is a PL/SQL solution, fully client side, that is installed and configured in few minutes and is ready for instant security assessment of your Oracle database. It brings easiness to its users letting them focus only on the conceptual security tasks, without concentrating on complex technical security configurations, made easy and plainly presented to them via its rich user interface.

Omega DB Security Reporter assesses the following security areas of top importance:

Privileges	for system, objects, and roles
Audits	on system privileges, user statements, audited system actions, object privileges and operations audits
Others	User password profiles and Initialization (security) parameters

The inter-relations of Oracle security are presented to user in flexible application forms and assessed items visualized by user-friendly data-aware components.

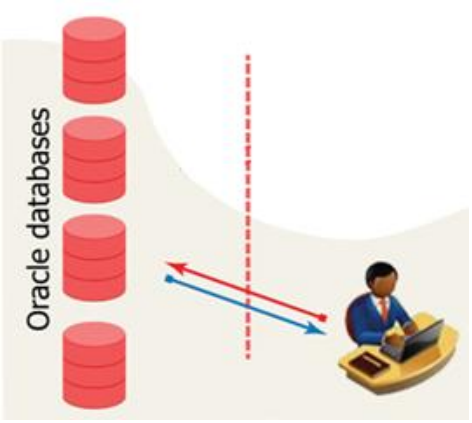
Reports Comparison of type Target vs Baseline pushes for cutting-edge Change Management of the assessed database security configuration items; and detection of security the slightest configuration differences between reports.

Ready-to-start predefined Checklists enable Security Compliance assessment with a few clicks.

Both Traditional and Unified Oracle audit are supported!

Solution Architecture

Omega DB Security Reporter features the simplest possible architecture regarding Oracle database.



(simplest) Architecture

A two-tier, Client-Server model, the Application directly connecting and assessing the target Oracle database. Fully client-side and standalone (can run from USB).

The security personnel assess and reports on multiple databases; all configurations and results are stored locally.

Quick Deployment and Run

1. Download and uncompress
2. Run the Application
3. Create scan account on DB
4. Create a DB entry and connect
5. Load the checklist templates and run the assessment

Security Assessment Report Classes

Reports are classified according to the type of the Oracle Security Item that is being assessed, which can be a privilege (system, object, role), an audit (of a system privilege, statement, shortcut, object privilege/statement), or a user password profile resource, … ; this logically determines the technical approach of the assessment and impacts the content of the report result.

The Report Classes available in this version are:

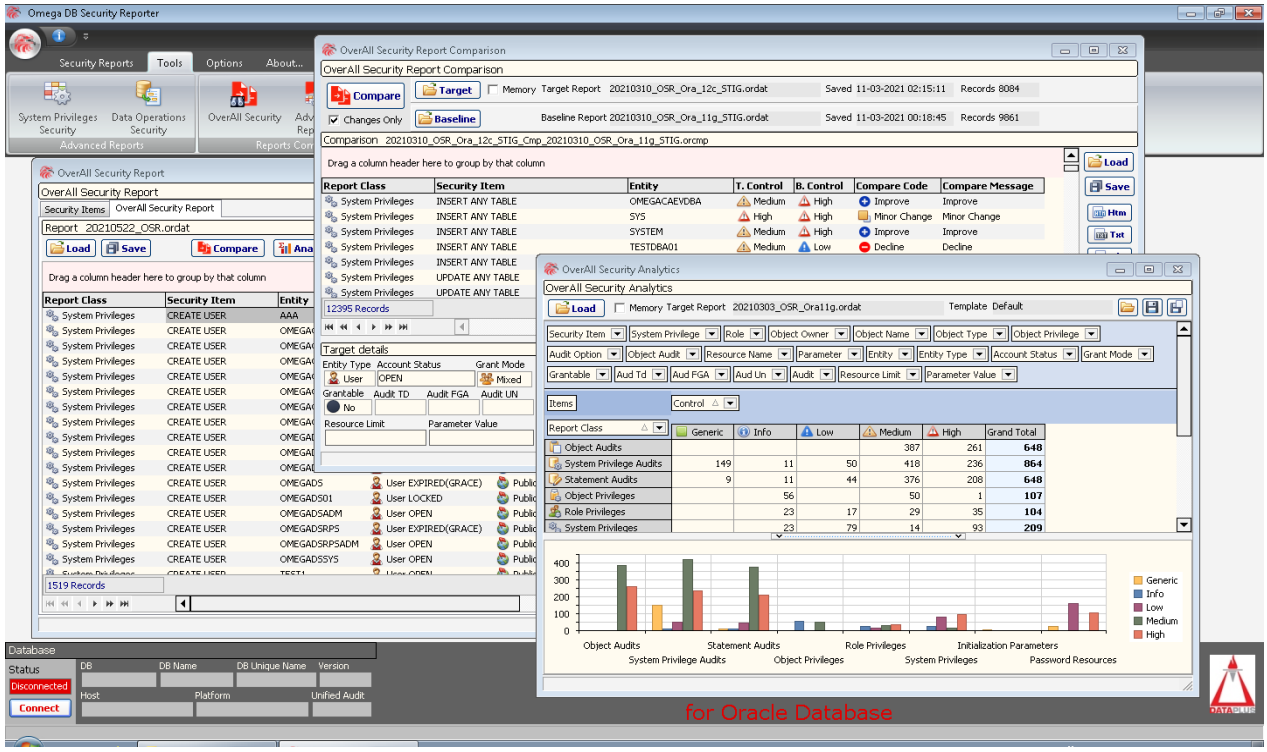
1. System Privileges – system privilege vs user
2. Object Privileges – object privilege vs user
3. Role Privileges – role privilege vs user
4. System Privileges Audits – system privilege traditional and unified audit vs user
5. Statements Audits – statement audit (traditional) vs user
6. Object Audits – object audit traditional and unified, plus FGA vs user
7. Audited System Actions – system actions audit (unified) vs user
8. Password Resources – Password Profile resource vs user
9. Initialization Parameters – security related parameters

Report classes are implemented:

* Individually - as Ad-Hoc Reports
* Combined by class-level - at Overall Security reports
* Combined at item level - at Advanced Reports

Rich and Intuitive Interface

The application uses best components on the market for grids, pivots, charts; and any other data-enabled presentation components.



Advanced Features

Effective privilege evaluation:

A system, object or role privilege that is directly granted to a grantee (user account or role) is easily verifiable in respective Oracle dictionary views, which is the simplest approach; however a grantee might have effectively (!) the same privilege not granted (and verified) directly, but through a Role, or more, hidden behind a "chain" of roles granted to each other and having the privilege granted to the last role at the end of this "chain".
The above feature ensures the evaluation considers not only a direct grant, but also an "indirect" – granted through roles hierarchy.

Effective audit evaluation:

As with privileges, the audit mode (level) is provided as a final result of all available audits that do apply to the security item and/or user entity.
At Traditional audit both statements and statements shortcuts for system privileges are supported.
At Unified audit "by granted Role" (clause *by_users_with_roles*), "audit role" (clause *role_audit*), and audit *by/except user* clauses are supported.
Top-level SQL audit is supported for *ALL STATEMENTS* clause at Traditional audit and for *ONLY TOPLEVEL* clause at Unified.
Difference is made on partial audit vs full audit depending on audit settings for Success and/or Failure on both Traditional and Unified Audit.
FGA - Fine-Grained audit - is assessed whenever object audit operations are involved.
Finally, cumulative audit for different settings (ex Success/Failure) is applied for a final audit result.

Account status evaluation:

The status of an Oracle user account is a factor in evaluation making the difference between *permanently* Locked statuses and others:

Locked:	LOCKED, EXPIRED & LOCKED, EXPIRED(GRACE) & LOCKED
Others:	OPEN, EXPIRED, EXPIRED(GRACE), LOCKED(TIMED), EXPIRED & LOCKED(TIMED), EXPIRED(GRACE) & LOCKED(TIMED)

Intelligent Assessment:

At privilege assessment, the ability to grant the received privilege (Grantable) is a factor in result.
At audit assessment, auditing for success and/or failure is a factor in result.

A detailed result per item/user is given with 5 levels: Generic, Info, Low, Medium, High, and not just a simple Correct/Finding.

Authorization of exceptions is featured at item and user (or role) level.

Advanced Reports

System Privileges Security

System Privilege Security Report combines system privilege grant status with audit status (combination of traditional and unified) for each assessed system privilege and user.

Objects Operations Security

Object Operations Security Report combines system/object privilege grants status with audit status (combination of system/statement/object audit for traditional and unified) for each assessed object operation and user.

Security Comparison for Change Management

Reporting alone is unable to provide a clear view on the next most important issue after report itself: Change Management of the security posture. Reports can involve thousands of records. A visual-only comparison would find it impossible (even with hundreds) to distinguish with clarity and precision the changes performed between the two reports.

Report Comparison, a feature available to all Reports, highlights and categorizes the changes between two different reports - Target and Baseline. Comparison consists in matching individual items per user/role between the compared reports and making an evaluated and categorized decision on the quality and scope of the changes – from the most important to the slightest – at assessed security item and user (or role) level.

Comparison highlights changes in details: Improvements, Declines and Minor Changes.

Visualizations and Analytics

Pivot-style analytics are available for Overall and Advanced Security Reports.

Predefined checklists

Pre-defined checklists are provided for Overall Reports and Advanced Reports, in three compilations:

DATAPLUS (recommended)
CIS
STIG-DISA

User can edit existing templates or create new ones, not being limited to predefined items for assessment only.

Compliance

Performs and exceeds most SQL-PL/SQL assessable controls of Oracle security checklists CIS and STIGDISA. Features special compliance forms for Overall Security and advanced Reports. Addresses requirements of IT Security Frameworks and Standards, like: ISO 27001/2, ISACA, PCI-DSS and HIPAA.

Persistence and Integration

Reports can be saved in XML format and re-loaded. They can be exported to Xls, Rtf, Txt and Html. Overall and Advanced Security Reports can also be printed (or previewed) and exported to Pdf.

Compatibility

Database	Oracle Database 10g - 21c
Application	All Win NT-based systems

About DATAPLUS

DATAPLUS is an information security consulting and solution provider company, founded in October 2007 in Tirana, Albania. We provide Oracle database security software only solutions and services.

Contact us

For more information about Omega DB Security Reporter please visit www.dataplus-al.com, or contact us at:

DATAPLUS

Tirana, Albania
Street Address: Bul. Zog I, P. "Edicom", 8F.
E-Mail: info@dataplus-al.com
Tel: +355 67 5045551

For product documentation, forum and knowledge base, visit our site:

https://www.dataplus-al.com/omega-db-security-reporter

For technical issues, comments, ideas and impressions, e-mail us at:

support@dataplus-al.com

For pricing and licensing information, contact our Sale specialists at:

sales@dataplus-al.com

Also follow us on the next social media sites where DATAPLUS is present:

YouTube https://www.youtube.com/channel/UCa59qQuGg5tvd2vIe1MsMOw
LinkedIn https://www.linkedin.com/company/dataplus-al