Top 5 Oracle Database Incidents You Need Visibility Into

Table of Contents

#1: Table and Record Deletions

Because Oracle database tables store important information used by critical enterprise applications, they must be monitored constantly to detect harmful activity and prevent system downtime. You need to know quickly if someone deletes a table or some of its elements, either maliciously or by mistake. Netwrix Auditor reports on dropped tables and removed records, providing answers to the following questions:

- **Who** removed a table or record from any of your Oracle databases?
- **What is the name** of each removed object?
- **From which workstation** was each deletion made?
- **Where** was the object stored before it was deleted?
- **When** was each deletion made?

Data Deletions

Lists dropped tables and table where data was removed. Use this report to promptly react to data deletion and prevent its loss.

Action	Object Type	What	Who	When
■ **Removed**	**Table**	ENT.AUDIT_LOG. VALUE	ENTERPRISE\J.Carter	9/19/2016 3:54:21 AM
Where: orcl/orcl.enterprise.com **Workstation:** 192.168.1.47 **Session ID:** 35436277 **Container name:** CDB$ROOT **Action name:** DROP TABLE **Database user:** C##J.Carter				
■ **Removed**	**Data**	ENT.AUDIT_LOG	ENTERPRISE\J.Carter	9/19/2016 3:50:04 AM
Where: orcl/orcl.enterprise.com **Workstation:** 192.168.1.47 **Action name:** DELETE **Database user:** C##J.Carter **Session ID:** 35436277				

#2: Role and Privilege Escalation

A user's database roles and privileges control which types of SQL statement they can run and whether they have administrative rights to manipulate the database. Good security practice involves granting users only the minimum privileges needed to accomplish their work. Netwrix Auditor helps control unwarranted role assignments and modifications, and provides answers to the following questions:

⁂ **Who** made a privilege or role assignment?

⁂ **Which user account** received a new role or privilege?

⁂ **From which workstation** was each change made?

⁂ **When** did each modification occur?

Privilege Management

Shows changes to roles and privileges. Use this report to detect unwarranted role assignments or modifications and ensure Oracle Database security.

Action	Object Type	What	Who	When
■ **Added**	**Role**	CDB_DBA	ENTERPRISE\T.Simpson	9/19/2016 3:22:01 PM

Where: orcl/orcl.enterprise.com

Workstation: 192.168.1.47
Action name: GRANT
Container name: CDB$ROOT
Database user: C##J.Carter
Privilege for action: CDB_LOCAL_ADMIN_PRIVS, PDB_ALERTS, PDB_PLUG_IN_VIOLATIONS
Program name: SQL Developer
Session ID: 1790914
Unified policy name: ORA_SECURECONFIG

#3: Failed Activity by User

Multiple failed attempts to access, add, read, modify or remove objects in Oracle Database can be the first sign of a malicious attack. Netwrix Auditor shows details about every failed action made by a user and helps answer the following questions:

- **Which users** attempted actions that failed across Oracle Database?
- **How many** failed actions were attempted by each user?
- **What actions** did each user fail to perform?
- **What was the cause** of each failed action?
- **When** was each failed action attempted?

Failed Activity

Shows failed actions, including failed read attempts, failed modification attempts, failed logons, etc., grouped by user.

Who: ENTERPRISE\J.Parker   **Total Count: 8**

Action	Object Type	What	When
■ Add (Failed Attempt)	Audit Policy	ENT.ACTIONS_POL	9/19/2016 3:54:21 AM

Where: orcl/orcl.enterprise.com
Workstation: 192.168.1.47
Action name: CREATE AUDIT POLICY
Cause: ORA-01905: no privileges on SYS table
Container name: CDB$ROOT
Database user: C##T.Simpson
Privilege for action: AUDIT_VIEWER
Program name: SQL Developer
Session ID: 67348947
Unified policy name: ENT.ORA_SECURECONFIG

#4: Account Changes

Complete visibility into successful and failed attempts to create, modify, delete, enable or disable Oracle Database accounts ensures timely detection of attacks and can help prevent a data breach. Netwrix Auditor gives you control over user account changes and provides detailed answers to the following questions:

⋗ **Who** made or tried to make user account changes?

⋗ **What user accounts** were affected or targeted by a failed change attempt?

⋗ **What changes** were applied or attempted to be applied to each user account?

⋗ **What SQL statement** was submitted by a user to make a modification?

⋗ **When** was each change made or attempted?

Account Management

Shows successful and failed attempts to create, modify, delete, enable, or disable Oracle Database accounts. Use this report to detect suspicious activity and exercise security control over your data.

Action	Object Type	What	Who	When
■ **Modified**	**User**	C##J.Carter	ENTERPRISE\T.Simpson	9/21/2016 8:21:15 AM

Where: orcl/orcl.enterprise.com

Workstation: 192.168.1.49
Action name: ALTER USER
Captured SQL statement: ALTER USER "C##J.Carter" TABLESPACE "SYSAUX" TEMPORARY TABLESPACE "TEMP" PASSWORD EXPIRE ACCOUNT UNLOCK
Container name: CDB$ROOT
Database user: C##J.Carter
Privilege for action: SYSDBA, ALTER USER
Program name: SQL Developer
Session ID: 224769
Unified policy name: ORA_SECURECONFIG

#5: Trigger Changes

Maintaining the integrity of the information stored in your Oracle Database requires control over all changes made to database triggers. Netwrix Auditor tracks every successful and failed attempt to change the procedural code and gives answers to the following questions:

- **What trigger** was changed or attempted to be changed?
- **Who** changed or tried to change a trigger?
- **What action** did each user perform or attempt to perform?
- **From which workstation** was each modification made?
- **When** did each change attempt take place?

Trigger Management

Shows successful and failed attempts to create, modify, or delete triggers. Run this report regularly to promptly identify changes to your workflows and exercise security control over your data.

Action	Object Type	What	Who	When
■ Removed	Trigger	BackupTrigger	ENTERPRISE\J.Carter	9/2/2016 2:45:12 PM

Where: orcl/orcl.enterprise.com

Workstation: 192.168.1.78
Action name: DROP TRIGGER
Container name: CDB$ROOT
Database user: C##J.Carter
Program name: SQL Developer
Session ID: 3647276957
Unified policy name: ORA_SECURECONFIG

About Netwrix Auditor

Netwrix Auditor is a **visibility and governance platform** that enables control over changes, configurations and access in hybrid cloud IT environments to protect data regardless of its location. The unified platform provides security analytics for detecting anomalies in user behavior and investigating threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Microsoft Entra ID (formerly Azure AD), Exchange, Office 365, Windows file servers, Dell data storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with a RESTful API, Netwrix Auditor provides **endless integration, auditing and reporting capabilities** for security and compliance.

Unlike other vendors, Netwrix focuses exclusively on providing complete visibility and governance for hybrid cloud security. The sharp focus enables us to offer much more robust functionality than legacy change auditing solutions. Netwrix Auditor has been already honored with more than **100 awards** and recognized by almost **160,000 IT departments** worldwide.

Deploy Netwrix Auditor Wherever You Need It

🏠 Free 20-Day Trial for On-Premises Deployment: netwrix.com/freetrial

🛢 Free Virtual Appliance for Hyper-V and VMware Hypervisors: netwrix.com/go/appliance

netwrix.com/social

Toll-free: 888-638-9749

Int'l: +1 (949) 407-5125

EMEA: +44 (0) 203-318-0261

Netwrix Corporation, 6160 Warren Parkway, Suite 100, Frisco, TX, US 75034