19c ORACLE Database

# Privilege Analysis

Privilege Analysis (PA), a feature of Oracle Database Enterprise Edition, dynamically analyzes privilege and role usage for database users and application service accounts.   PA generates reports on which privileges were used as well as those that were not used.  Reports generated by PA are more informative than those produced by static based role/privilege analysis tools, which can only show you which roles and privileges are granted to users.  Understanding actual usage of roles and privilege is essential to implementing a least privilege model for all database accounts and reducing your application attack surface.

## GENERAL

### When was Privilege Analysis introduced?

Privilege Analysis was initially released as part of Oracle Database Enterprise Edition 12c (12.1.0.1) as a licensed feature of Oracle Database Vault.

### What Oracle Database version, edition, and/or option do I need to purchase to use Privilege Analysis?

PA is a feature of Oracle Database Enterprise Edition.  This is available in all supported versions of the database.  No additional options are required.

### Why has Privilege Analysis been included with Oracle Database Enterprise Edition?

In today's environment, you need tools to assess your security before hackers do it for you.  To support this, Oracle created the Database Security Assessment Tool and made it available for all customers to help them analyze their database security configuration.  Privilege Analysis complements this functionality by enabling customers to implement a least privileges policy for their database user accounts. These tools are security tools all customers should use to assess their security configuration and manage their risk profile.

## LEAST PRIVILEGE

### What is least privilege and why is it important?

Least privilege is a security model that limits the privileges of any account (user, application, utility) to only what is required for their normal tasks.  This applies to any system – not just databases.  Extraordinarily powerful privileges that are only used for troubleshooting should be requested and checked out as required, and not granted as part of a user's everyday set of roles and privileges.  Least privileges also requires continuous management with granting additional privileges as required/approved and revocation of privileges when they are no longer required.

Bad actors target privileged user accounts since many are over-privileged and provide unfettered access to all the sensitive data.  Forrester estimates 80% of breaches use privileged accounts.  Least privilege is an important security component of a strong security environment.

### Do I need to install anything to run Privilege Analysis?

PA is built into the Oracle Database core starting with Oracle Database 12c, and nothing else is required to install it.

### Why should I use Privilege Analysis?

Static tools exist to show the privileges and roles granted to an account, but these tools don't show which privileges get used and which don't get used.  PA collects role and privilege use over time and reports on what was used and unused.  Unlike static tools, there is no guessing of which privileges are required by an user..

### Does Privilege Analysis automatically give me least privileges?

No – but it gets you much closer than using other methods.  As a next step, you can create audit alerts when the unused privileges and roles are used instead of just revoking them.  This way you can catch unusual use of the account, but it won't be block authorized use.  After a period of time, when you have enough confidence the unused privileges and roles aren't needed, you can revoke them.

You'll also need to review the used privileges and roles report.  Look at what system privileges were used and see which one's could be replaced by direct object grants.

### I can easily generate a list of privileges and roles that are granted to each of my database users – why do I need Privilege Analysis?

The list of privileges and roles you get is a static list and doesn't show if these granted privileges and roles were used.  Unused privileges violate the least privileges model and allow bad actors using stolen privileged user credentials to steal more data.

## USING PRIVILEGE ANALYSIS

### Do I need to configure and enable Database Vault to run Privilege Analysis?

No – Database Vault does not need to be configured or enabled to run PA.  PA collects and reports independently of Database Vault.

### How can I run Privilege Analysis?

The user first needs the CAPTURE_ADMIN role. The user creates a PA policy, and then enables the policy for a period of time. After disabling the PA policy, the user generates the report of used and unused privileges.

### Won’t Privilege Analysis slow down my applications if I run it on my production database?

No, Privilege Analysis is built into the kernel of the Oracle Database, and it was designed to work in production databases. Accurate user privilege use is best captured in production environments. However, application privilege use can be captured in production or test. Running a full regression test on an application may be equivalent to running an application for an extended period of time on the production server.

### How long does it take to run Privilege Analysis?

You need to determine how long you need to capture all the tasks that are normally done. This might be one day or three months. If you’re evaluating task-based privileges, it will be as long as you need to complete the task.

### What role do I need to run Privilege Analysis?

The CAPTURE_ADMIN role is required to create and run PA policies.

### I’ve got my list of Privilege Analysis report of unused privileges and roles – should I just revoke them from the user?

The list of unused privileges is a good starting point. You could analyze each unused privilege and consider if it should be revoked. However, you run the risk of revoking a privilege the user really needed but wasn’t used during the Privilege Analysis policy capture window. Depending on the user or application, this could lead to a minor inconvenience up to and including application downtime. An alternative to this post-PA analysis is to create audit/alerts on the unused privileges. That way, users or applications can continue to function. Any alerts that are generated would signal one of two things: 1) The privilege use is valid and the privilege use can be dropped from audit/alert or 2) The alert indicates unauthorized privilege use and additional investigation is required. This might result in revoking the privilege to prevent additional unauthorized activities.

### Why should I care about the used privileges/roles report?

A key item to review with this report is how system privileges are used. System privileges will show up as being used, but they may be used inappropriately. System privileges are frequently granted to users and applications because it’s easy to do and too hard to figure out exactly what direct object grants are needed. PA makes it easy to figure this out. Under the DBA_USED_PRIVILEGES view, you can see what system privilege was used to access which objects. If the user/application doesn’t need access to other objects, replace the system privilege with direct object grants. Replacing system privileges with direct object grants greatly reduces security risk.

### Does Privilege Analysis just capture runtime privileges and roles?

PA captures runtime privilege and role use, but it also captures other privileges and roles that are often overlooked but critical for that user. PA can capture the privileges required to 1) compile PL/SQL packages, procedures, and functions and 2) run Oracle Database Java programs. PA can also capture roles associated with code-based access control (CBAC) and secure application roles (SAR).

### Can I run PA on SYS?

No.  PA cannot capture privilege use by SYS.  SYS (and the SYSDBA privilege) is the equivalent to OS root and should be managed through a ‘break glass’ process or a privilege account management system.  SYS should only be used for specific tasks like patching and upgrades and not for daily administrative tasks.  Therefore, there is no need to run PA on SYS.

## COMPATIBILITY

### How does Privilege Analysis work in a multitenant database?

(from documentation) If you are using a multitenant environment, then you can create privilege analysis policies in either the CDB root or in individual PDBs. The privilege analysis policy applies only to the container in which it is created, either to the privileges used within the CDB root or the application root or to the privileges used within a PDB. It cannot be applied globally throughout the multitenant environment. You can grant the CAPTURE_ADMIN role locally to a local user or a common user. You can grant the CAPTURE_ADMIN role commonly to common users.

### Does PA work with RAC Databases?

Yes – PA does work on RAC databases.  Just run it on a node and it will capture privilege usage across all the RAC nodes.

## CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/cloudsecurity/db-sec facebook.com/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services

Oracle is committed to developing practices and products that help protect the environment

ORACLE