153

DBMS_PRIVILEGE_CAPTURE

The `DBMS_PRIVILEGE_CAPTURE` package provides an interface to database privilege analysis.

> **See Also:**
>
> Oracle® Database Security Guide regarding on how to analyze the use of privilege grants

This chapter contains the following topics:

DBMS_PRIVILEGE_CAPTURE Overview

Database privilege analysis enables you to create a policy that records the usage of system and object privileges that have been granted to users. You then can determine the privileges that your users are using and not using. From there, you can revoke any unused privileges, thereby reducing the number of excess privilege grants for users.

By analyzing the privileges that users must have to perform specific tasks, privilege analysis policies help you to achieve a least privilege model for your users.

DBMS_PRIVILEGE_CAPTURE Security Model

The privilege analysis administrator role, `CAPTURE_ADMIN`, is granted `EXECUTE` permission on the `DBMS_PRIVILEGE_CAPTURE` package by default.

The `CAPTURE_ADMIN` role is granted to the `DBA` role during database installation.

DBMS_PRIVILEGE_CAPTURE Constants

The `DBMS_PRIVILEGE_CAPTURE` package defines several enumerated constants for specifying parameter values.

Table 153-1 DBMS_PRIVILEGE_CAPTURE Constants

Constant	Value	Type	Description
G_DATABASE	1	NUMBER	Analyzes all privilege use, except privileges used by the SYS user.
G_ROLE	2	NUMBER	Analyzes privilege use for the specified roles.
G_CONTEXT	3	NUMBER	Analyzes privilege use when the condition parameter evaluates to true.
G_ROLE_AND_CONTEXT	4	NUMBER	Analyzes privilege use for the specified roles when the condition parameter evaluates to true.

DBMS_PRIVILEGE_CAPTURE Examples

These examples illustrate using the DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE procedure to create various types of privilege analysis, like database analysis, role analysis, and context-specific analysis. The examples also illustrate combining different conditions in context-specific analysis.

```
--Create a database privilege analysis policy
BEGIN
DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
        name         => 'all_priv_analysis_pol',
        description  => 'database-wide policy to analyze all privileges',
        type         => DBMS_PRIVILEGE_CAPTURE.G_DATABASE);
END;

--Create a privilege analysis policy to analyze privileges from the role PUBLIC
BEGIN
DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
       name         => 'pub_analysis_pol',
       description  => 'Policy to record privilege use by PUBLIC',
       type         => DBMS_PRIVILEGE_CAPTURE.G_ROLE,
       roles        => role_name_list('PUBLIC'));
END;

-- Create a policy to analyze privileges from the application module, "Account
-- Payable"
BEGIN
DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
  name         => 'acc_pay_analysis_pol',
  type         => DBMS_PRIVILEGE_CAPTURE.G_CONTEXT,
  condition    => 'SYS_CONTEXT(''USERENV'', ''MODULE'') = ''Account Payable''');
END;

-- Create a policy that records privileges for session user APPS when running the
-- application module "Account Payable"
BEGIN
DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
  name         => 'acc_pay_analysis_pol',
  type         => DBMS_PRIVILEGE_CAPTURE.G_CONTEXT,
  condition    => 'SYS_CONTEXT(''USERENV'', ''MODULE'') = ''Account Payable'' AND
                   SYS_CONTEXT(''USERENV'', ''SESSION_USER'') = ''APPS''');
END;
```

Summary of DBMS_PRIVILEGE_CAPTURE Subprograms

This table lists and briefly describes the `DBMS_PRIVILEGE_CAPTURE` package subprograms.

Table 153-2 DBMS_PRIVILEGE_CAPTURE Package Subprograms

Subprogram	Description
CAPTURE_DEPENDENCY_PRIVS Procedure	Captures the privileges that are used by definer's rights and invoker's rights PL/SQL program units for compilation.
CREATE_CAPTURE Procedure	Creates a policy that specifies the conditions for analyzing privilege use.
DELETE_RUN Procedure	Deletes a privilege analysis capture run
DISABLE_CAPTURE Procedure	Stops the recording of privilege use for a specified privilege analysis policy
DROP_CAPTURE Procedure	Removes a privilege analysis policy together with the data recorded
ENABLE_CAPTURE Procedure	Starts the recording of privilege analysis for a specified privilege analysis policy
GENERATE_RESULT Procedure	Populates the privilege analysis data dictionary views with data

CAPTURE_DEPENDENCY_PRIVS Procedure

This procedure captures the privileges that are used by definer's rights and invoker's rights PL/SQL program units for compilation.

Syntax

```
DBMS_PRIVILEGE_CAPTURE.CAPTURE_DEPENDENCY_PRIVS ();
```

Parameters

This procedure has no parameters.

Usage Notes

Every rerun of the `DBMS_PRIVILEGE_CAPTURE.CAPTURE_DEPENDENCY_PRIVS` procedure deletes any existing records from the privilege analysis data dictionary views. It then recaptures records based on the existing PL/SQL program units.

CREATE_CAPTURE Procedure

This procedure creates a privilege analysis policy that specifies the conditions for analyzing privilege use. It also optionally specifies the roles for which privilege use is to be analyzed, and the conditions under which privilege use is to be analyzed.

Syntax

```
DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE (
   name            IN  VARCHAR2,
   description     IN  VARCHAR2 DEFAULT NULL,
   type            IN  NUMBER DEFAULT G_DATABASE,
```

```
   roles           IN  ROLE_NAME_LIST DEFAULT ROLE_NAME_LIST(),
   condition       IN  VARCHAR2 DEFAULT NULL);
```

Parameters

Table 153-3 CREATE_CAPTURE Procedure Parameters

Parameter	Description
name	Name of the privilege analysis policy. A string of size up to 30 characters.
description	Description of the policy (up to 1024 characters)
type	Type of the privilege analysis policy. Possible values are: • G_DATABASE: Captures all privilege use in the database, except privileges used by the SYS user. • G_ROLE: Captures the use of a privilege if the privilege is part of a specified role or list of roles. • G_CONTEXT: Captures the use of a privilege if the context specified by the condition parameter evaluates to true. • G_ROLE_AND_CONTEXT: Captures the use of a privilege if the privilege is part of the specified list of roles and when the condition specified by the condition parameter is true.
roles	The roles whose privileges are to be analyzed. Required if the type is G_ROLE or G_ROLE_AND_CONTEXT.
condition	PL/SQL boolean expression containing up to 4000 characters. Required if type is G_CONTEXT or G_ROLE_AND_CONTEXT. Note that the boolean expression can only contain SYS_CONTEXT, but not other functions.

Usage Notes

- When using role-based analysis for the CREATE_CAPTURE procedure, privilege use is analyzed even if the privilege is indirectly granted to the specified role.

  For example, say role R2 contains role R1, and R1 contains privilege P1. If the privilege policy includes only role R2, any use of the P1 privilege is still analyzed, as privilege P1 is an indirect part of role R2.

- When using the condition parameter, use the following syntax for the PL/SQL expression:

  ```
  condition::= predicate | (predicate1) AND (predicate2)
  | (predicate1) OR (predicate2)
  ```

  Where,

  ```
  predicate::= sys_context(namespace, attribute) relop constant_value |
  sys_context(namespace, attribute) between constant_value and
   constant_value | sys_context(namespace, attribute) in {constant_value
  (,constant_value)* }
  ```

  Where,

  ```
  relop::= = | < | <= | > | >= | <>
  ```

- A privilege analysis policy cannot analyze the use of SYS user privileges.

DELETE_RUN Procedure

This procedure deletes a privilege analysis capture run.

Syntax

```
DBMS_PRIVILEGE_CAPTURE.DELETE_RUN (
   name      IN VARCHAR2,
   run_name  IN VARCHAR2);
```

Parameters

Table 153-4 *DELETE_RUN Procedure Parameters*

Parameter	Description
name	Name of the privilege analysis policy with which the capture run is associated
run_name	Name of the capture run

Usage Notes

- You can find the names of existing privilege capture policies by querying the DBA_PRIV_CAPTURES data dictionary view.
- Another way to delete a capture run is to drop the policy with which the capture run is associated. Dropping the policy automatically drops its associated capture runs.
- When you drop a capture run it is no longer accessible through the privilege capture data dictionary views.

DISABLE_CAPTURE Procedure

This procedure stops the recording of privilege use for a specified privilege analysis policy. When a policy is disabled, privilege use meeting the policy condition is no longer recorded.

Syntax

```
DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE (
   name        IN VARCHAR2);
```

Parameters

Table 153-5 DISABLE_CAPTURE Procedure Parameters

Parameter	Description
name	Name of the privilege analysis policy to be disabled

Usage Notes

When a privilege analysis policy is first created, it is disabled by default.

DROP_CAPTURE Procedure

This procedure removes a privilege analysis policy together with the data recorded. When a policy is removed, all previously recorded privilege use data associated with the policy is deleted.

Syntax

```
DBMS_PRIVILEGE_CAPTURE.DROP_CAPTURE (
   name      IN VARCHAR2);
```

Parameters

Table 153-6 *DROP_CAPTURE Procedure Parameters*

Parameter	Description
name	Name of the privilege analysis policy to be removed

Usage Notes

- You must disable a privilege analysis policy before removing it. An enabled policy cannot be removed.
- If there are capture runs associated with this policy, then they are automatically dropped when you drop the policy.

ENABLE_CAPTURE Procedure

This procedure starts the recording of privilege analysis for a specified privilege analysis policy and optionally provides a capture run for this policy. After a policy is enabled, all privilege use under the policy condition is recorded.

Syntax

```
DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE (
   name      IN VARCHAR2,
   run_name  IN VARCHAR2 DEFAULT NULL);
```

Parameters

Table 153-7 *ENABLE_CAPTURE Procedure Parameters*

Parameter	Description
name	Name of the privilege analysis policy to be enabled
run_name	Name of the capture run to associate with this policy, less than 128 characters. Enclose exotic characters in double quotation marks.

Usage Notes

The following usage notes apply:

- When a privilege analysis policy is first created, it is disabled by default. You must run `ENABLE_CAPTURE` to enable the privilege analysis policy.

- You can enable only one privilege analysis policy at a time. However, a database-wide privilege analysis of the `G_DATABASE` type can be enabled together with another non `G_DATABASE` privilege analysis.
- You cannot enable the same run multiple times. For example, `run_01` cannot be used again if you want to re-enable the capture for `run_01`. Instead, create a new run.

GENERATE_RESULT Procedure

This procedure populates the privilege analysis data dictionary views with data.

> **See Also:**
>
> Oracle® Database Security Guide for more information about privilege analysis views.

Syntax

```
DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT (
   name        IN VARCHAR2,
   run_name    IN VARCHAR2 DEFAULT NULL,
   DEPENDENCY  IN BOOLEAN DEFAULT NULL);
```

Parameters

Table 153-8 *GENERATE_RESULT Procedure Parameters*

Parameter	Description
`name`	Name of the privilege analysis policy for which views are populated
`run_name`	Name of the capture run that is associated with the privilege analysis policy. If you omit this parameter, then the records of all created runs will be analyzed. When you specify the `run_name` parameter, only the records of that run are analyzed and all other runs are unaffected.
`dependency`	Enter `Y` (yes) or `N` (no) to indicate if PL/SQL compilation privileges, set by the `DBMS_PRIVILEGE_CAPTURE.CAPTURE_DEPENDENCY_PRIVS` procedure, should be included in the report.

Usage Notes

You must disable a privilege analysis policy before populating the privilege analysis views for the policy. You cannot invoke this subprogram on an enabled privilege analysis policy.